

# CURSO DE CIBERSEGURIDAD EN LAS FLOTAS DE VEHÍCULOS

EN COLABORACIÓN CON EL EQUIPO TÉCNICO DE



## — DOCUMENTACIÓN ALUMNO —

**Fecha actualización**  
**18 de abril de 2024**

# ÍNDICE DOCUMENTOS

|                                                                                                                                                                                                                                                                  |         |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| <b>1. INFORME EUROCYBCAR SOBRE NORMATIVA UNECE/R155</b>                                                                                                                                                                                                          | PÁG 4   |
| <b>2. DOCUMENTO UNECE/R155 – ORIGINAL - UNECE/R155: UNIFORM PROVISIONS CONCERNING THE APPROVAL OF VEHICLES WITH REDARDS TO CYBER SECURITY AND CYBER SECURITY MANAGEMENT</b>                                                                                      | PÁG 31  |
| <b>3. DOCUMENTO UNECE/R155 – APÉNDICES A LA NORMATIVA R155 DESDE 2021 A 2024</b>                                                                                                                                                                                 | PÁG 61  |
| <b>4. LA ONU AMPLÍA LA NORMATIVA A LAS MOTOCICLETAS, SCOOTERS Y BICICLETAS</b>                                                                                                                                                                                   | PÁG 66  |
| <b>5. DOCUMENTO UNECE/R156 – UNIFORM PROVISIONS CONCERNING THE APPROVAL OF VEHICLES WITH REDARDS TO SOFTWARE UPDATE AND SOFTWARE UPDATES MANAGEMENT SYSTEM</b>                                                                                                   | PÁG 69  |
| <b>6. REGLAMENTO UNECE/R155 DE LA ONU SOBRE CIBERSEGURIDAD Y SU IMPACTO EN LOS VEHÍCULOS ELÉCTRICOS</b>                                                                                                                                                          | PÁG 85  |
| <b>7. REGLAMENTO Nº155 DE LA COMISIÓN ECONÓMICA PARA EUROPA (CEPE) DE LAS NACIONES UNIDAS // DISPOSICIONES UNIFORMES RELATIVAS A LA HOMOLOGACIÓN DE LOS VEHÍCULOS DE MOTOR EN LO QUE RESPECTA A LA CIBERSEGURIDAD Y AL SISTEMA DE GESTIÓN DE ESTA [2021/387]</b> | PÁG 103 |
| <b>8. PROPOSAL FOR THE INTERPRETATION DOCUMENT FOR UN REGULATION Nº [155] ON UNIFORM PROVISIONS CONCERNING THE APPROVAL OF VEHICLES WITH REGARDS TO CYBER SECURITY AND CYBER SECURITY MANAGEMENT SYSTEM</b>                                                      | PÁG 134 |
| <b>9. NORMALIZACIÓN EN CIBERSEGURIDAD PARA LA MOVILIDAD CONECTADA Y AUTOMATIZADA DE VEHÍCULOS Y SU ENTORNO</b>                                                                                                                                                   | PÁG 173 |
| <b>10. CONTROL Y SEGUIMIENTO DE LOS COSTES DE LA FLOTA DE VEHÍCULOS</b>                                                                                                                                                                                          | PÁG 222 |
| <b>11. DESARROLLO DE UNA HERRAMIENTA DE GESTIÓN DE FLOTAS DE VEHÍCULOS ELÉCTRICOS</b>                                                                                                                                                                            | PÁG 337 |

# ÍNDICE DOCUMENTOS

|                                                                                                                                                 |                |
|-------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| <b>13. UNIFORM PROVISIONS CONCERNING THE APPROVAL OF MOTOR VEHICLES WITH REGARD TO THE EVENT DATA RECORDER</b>                                  | <b>PÁG 348</b> |
| <b>14. CASOS REALES DE CIBERATAQUES A FLOTAS Y SISTEMAS DE TRANSPORTE</b>                                                                       | <b>PÁG 376</b> |
| <b>15. MÉTODO PARA LA GESTIÓN EFICIENTE DEL COMBUSTIBLE EN FLOTAS DE VEHÍCULOS CON RUTAS FIJAS. APLICACIÓN A UNA EMPRESA DE CONSTRUCCIÓN</b>    | <b>PÁG 400</b> |
| <b>16. GESTIÓN DE FLOTAS EN EUROPA. IMPORTANCIA CRECIENTE EN UN MUNDO DE MOVILIDAD CAMBIANTE</b>                                                | <b>PÁG 435</b> |
| <b>17. EL FUTURO DE LA MOVILIDAD. CÓMO LA TECNOLOGÍA DEL TRANSPORTE Y LAS TENDENCIAS SOCIALES ESTAN CREANDO UN NUEVO ECOSISTEMA DE NEGOCIOS</b> | <b>PÁG 511</b> |
| <b>18. TENDENCIAS EN LA FLOTA MUNDIAL DE VEHÍCULOS 2023. GESTIÓN DEL CAMBIO A LOS SUV Y LA TRANSICIÓN A LOS VEHÍCULOS ELÉCTRICOS</b>            | <b>PÁG 553</b> |
| <b>19. LAS MEJORES PRÁCTICAS DE CIBERSEGURIDAD PARA VEHÍCULOS MODERNOS</b>                                                                      | <b>PÁG 737</b> |

# NUEVA NORMATIVA DE SEGURIDAD UNECE/R155 **LOS VEHÍCULOS DEBERÁN TENER UN CERTIFICADO DE CIBERSEGURIDAD**



- De obligado cumplimiento desde julio de 2024 para todos los vehículos nuevos a la venta
- Afecta a coches, autobuses, camiones, autocaravanas y remolques; pero también se ha ampliado a motos, scooter y bicicletas eléctricas de más de 25 km/h
- Multas económicas por unidad para los modelos que no cumplan la normativa



# ÍNDICE

|                                                                                                                                          |               |
|------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| <b>POR QUÉ ES NECESARIO CREAR UN REGLAMENTO DE CIBERSEGURIDAD PARA VEHÍCULOS</b>                                                         | <b>PAG 3</b>  |
| <b>- ALGUNAS DE LAS TECNOLOGÍAS QUE EQUIPAN LOS VEHÍCULOS</b>                                                                            |               |
| <b>QUÉ REQUISITOS DEBE CUMPLIR UN COCHE PARA VENDERSE EN LA UNIÓN EUROPEA</b>                                                            | <b>PAG 5</b>  |
| <b>- PRINCIPALES NORMATIVAS DE SEGURIDAD EN VEHÍCULOS GENERADAS POR LA UE DESDE EL AÑO 2000 HASTA EL PRESENTE</b>                        |               |
| <b>- LAS NORMATIVAS QUE LA UNIÓN EUROPEA TOMA DE NACIONES UNIDAS</b>                                                                     |               |
| <b>- LA NUEVA NORMATIVA DE LA UE: LA UNECE/R155</b>                                                                                      |               |
| <b>INICIATIVAS PREVIAS A LA NORMATIVA UNECE/R155</b>                                                                                     | <b>PAG 7</b>  |
| <b>- EN ESPAÑA, EN EUROPA Y EN EL MUNDO</b>                                                                                              |               |
| <b>TODO SOBRE LA NORMATIVA UNECE/R155</b>                                                                                                | <b>PAG 10</b> |
| <b>- QUÉ DICE EL REGLAMENTO</b>                                                                                                          |               |
| <b>- FASES DEL DESARROLLO DE LA NORMA</b>                                                                                                |               |
| <b>- ÍNDICE DEL DOCUMENTO ORIGINAL DEL REGLAMENTO</b>                                                                                    |               |
| <b>- LOS 70 REQUISITOS QUE DEBE CUMPLIR UN VEHÍCULO PARA OBTENER EL CERTIFICADO DE CIBERSEGURIDAD</b>                                    |               |
| <b>- CÓMO ES EL PROCESO PARA OBTENER EL CERTIFICADO</b>                                                                                  |               |
| <b>- ASÍ ES LA ETIQUETA DE "VEHÍCULO CIBERSEGURO"</b>                                                                                    |               |
| <b>- PAÍSES QUE LO APLICARÁN</b>                                                                                                         |               |
| <b>- A QUÉ MARCAS Y VEHÍCULOS AFECTARÁ MÁS</b>                                                                                           |               |
| <b>- LAS SANCIONES SI NO SE CUMPLE LA NORMATIVA UNECE/R155</b>                                                                           |               |
| <b>UNA SOLUCIÓN PARA CUMPLIR EL REGLAMENTO</b>                                                                                           | <b>PAG 21</b> |
| <b>- EL TEST EUROCYBCAR</b>                                                                                                              |               |
| <b>QUÉ OPINAN LOS EXPERTOS</b>                                                                                                           | <b>PAG 22</b> |
| <b>- PABLO ESCAPA, CTO DE EUROCYBCAR. INGENIERO Y MIEMBRO DE PETEC</b>                                                                   |               |
| <b>- AZUCENA HERNÁNDEZ, CEO DE EUROCYBCAR</b>                                                                                            |               |
| <b>- NURIA ROMÁN, EX-JEFA DE ÁREA DE LA SUBD. GRAL DE CALIDAD Y SEGURIDAD INDUSTRIAL DEL MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO</b> |               |

# POR QUÉ ERA NECESARIO CREAR UN REGLAMENTO DE CIBERSEGURIDAD PARA VEHÍCULOS

## EN VIGOR DESDE EL 22 DE ENERO DE 2021

**DURANTE LOS ÚLTIMOS AÑOS** los vehículos se han ido haciendo más complejos desde el punto de vista tecnológico. De hecho, se calcula que el software que equipa un coche moderno de gama media se compone de unos 100 millones de líneas de código. Eso significa que los sistemas informáticos que equipa un automóvil actual son más complejos que los de un caza de combate F35 -con 24 millones de líneas de código-, que el sistema operativo Windows Vista -50 millones- o, incluso, que todo el software que emplea Facebook -62 millones-.

Esa ‘informatización’ de los vehículos ha posibilitado que equipen tecnologías que permiten conectarlos con otros dispositivos. Por ejemplo, con un smartphone -a través del Bluetooth, de un cable USB o de una aplicación móvil-, o a Internet -a través de un punto Wifi instalado en el interior del propio coche-. Todo esto ha dado paso al concepto de ‘coche conectado’, que la Sociedad de Tecnología Vehicular -VTS, por sus siglas en inglés- define como aquel que equipa aplicaciones, servicios y

tecnologías que lo conectan con su entorno.

Pero esa creciente complejidad tecnológica de los automóviles ha hecho que los vehículos empiecen a sufrir ciberataques. Según datos de EUROCYBCAR, desde el año 2012 se han documentado ataques a modelos de más de 60 marcas en todo el mundo, que comprometieron la privacidad de las personas que viajaban a bordo de esos vehículos e, incluso, supusieron un peligro para su vida.

Uno de los casos más divulgados fue la demostración ‘en vivo’ que le hicieron los hackers Charlie Miller y Chris Valasek a un periodista estadounidense en 2015. En concreto, le invitaron a conducir un Jeep Cherokee y, mientras el reportero circulaba, Miller y Valasek se quedaron en la casa del primero para, desde la distancia, manipular el aire acondicionado, los limpiaparabrisas y el equipo de audio. También lograron interferir en elementos implicados en el movimiento del coche, como los frenos, la transmisión y el motor.

**Según EUROCYBCAR, desde 2012 se han documentado más de 550 ciberataques que afectan a modelos de 60 marcas diferentes**

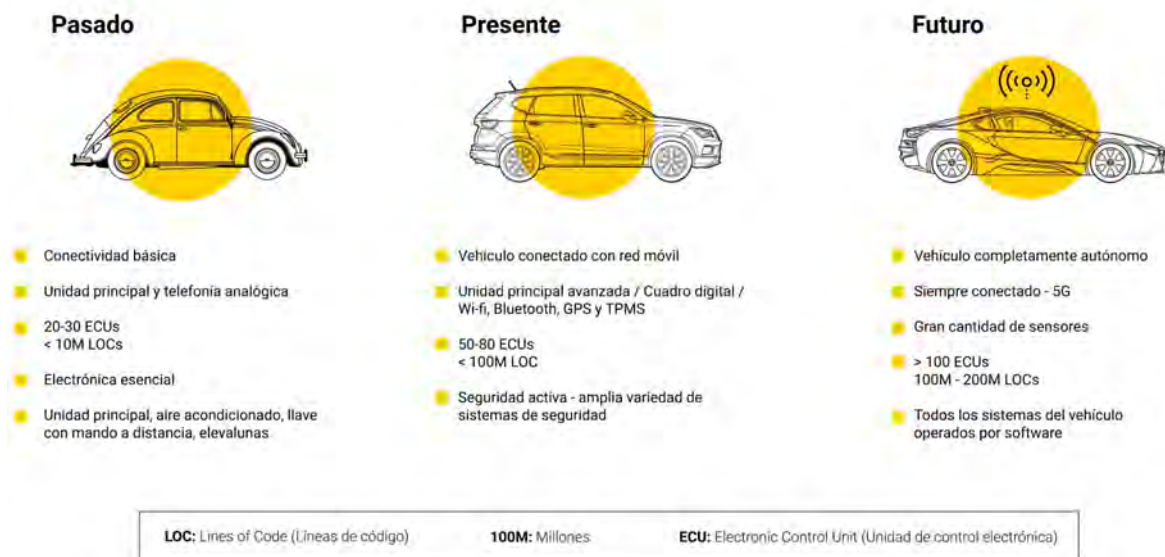
• **ALGUNAS DE LAS TECNOLOGÍAS QUE EQUIPAN LOS VEHÍCULOS... -y lo que podrían hacer los ciberdelincuentes con ellas- son:**

- ▶ **Bluetooth:** chantajearte, suplantar tu identidad o acosarte.
- ▶ **Llamada de emergencia E-Call:** impedir que te asistan en un accidente.
- ▶ **Airbags:** activarlo o desactivarlo a distancia.
- ▶ **Llave inteligente:** robarte el coche o "encerrarte" dentro de él.
- ▶ **WiFi:** espiarte, chantajearte o suplantar tu identidad.
- ▶ **GPS:** con el objetivo de secuestrarte, espiarte o chantajearte.
- ▶ **Radio-RDS:** dar información falsa.

Y, en el futuro, esta tendencia irá a más.

**Cabe recordar que desde 2023 ya circulan por el mundo 775 millones de coches conectados**. Los vehículos autónomos, que equipan un software más complejo, también van a ir en aumento: se estima que en 2026 **circularán** 50 millones de automóviles sin conductor.

Hasta ahora, los diversos gobiernos y organismos reguladores de todo el mundo habían creado normativas que garantizasen la seguridad física de los vehículos y sus pasajeros, pero la ciberseguridad había quedado fuera de esos marcos reguladores.



<https://www.informationisbeautiful.net/visualizations/million-lines-of-code/>

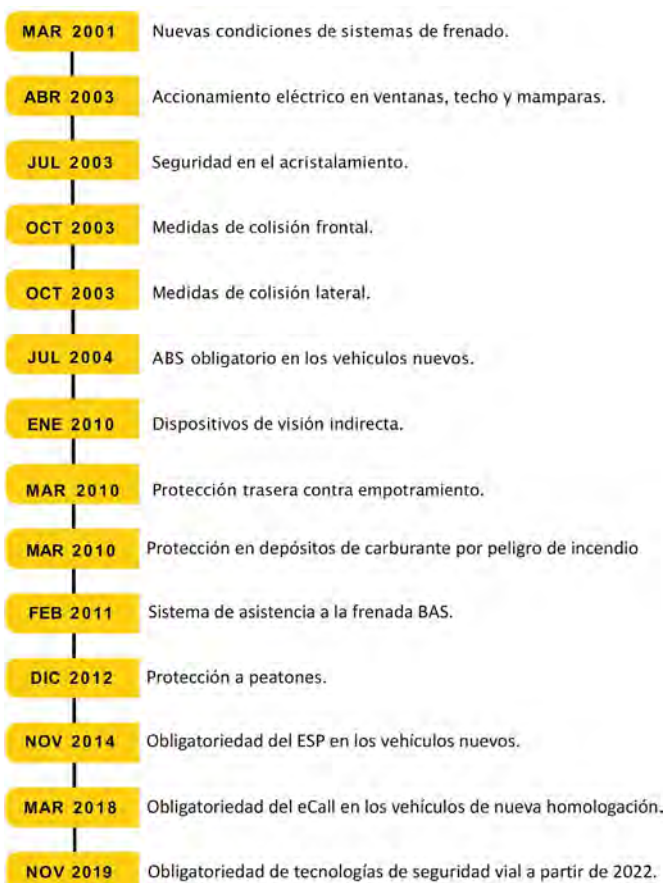
<https://site.ieee.org/connected-vehicles/ieee-connected-vehicles/connected-vehicles/>

Fuente EUROCYBCAR: están registrados, analizados y documentados más de 600 ataques a modelos de 60 marcas diferentes. Se confirma que, desde el año 2012 hasta el primer trimestre de 2024, los ciberataques contra vehículos e infraestructuras relacionadas con los coches han aumentado un 1.600%. Todo parece apuntar que el número real de casos es muy superior; el problema es que, debido al desconocimiento de este tipo de fallos de ciberseguridad entre la población, seguramente hay mucha gente que ha sufrido un ciberataque, pero no lo han considerado un crackeo al no tener evidencias que así lo demostrasen.

# QUÉ REQUISITOS DEBE CUMPLIR UN VEHÍCULO PARA VENDERSE EN LA UNIÓN EUROPEA

**PARA QUE LOS COCHES SE PUEDAN COMERCIALIZAR** en Europa, la Unión Europea exige a los fabricantes que sus modelos cumplan determinados requisitos de homologación, sobre todo, en lo que se refiere a su seguridad. Desde el año 2000 hasta el día de hoy, la Unión Europea ha hecho obligatorios en el equipamiento de los coches los siguientes sistemas de seguridad:

## PRINCIPALES NORMATIVAS DE SEGURIDAD EN VEHÍCULOS GENERADAS POR LA UE DESDE EL 2000



**JUNIO 2020 - OBLIGATORIEDAD DE UN CERTIFICADO DE CIBERSEGURIDAD PARA LOS VEHÍCULOS.**  
**ENTRADA EN VIGOR: 22 DE ENERO DE 2021**

## LAS NORMATIVAS QUE LA UNIÓN EUROPEA TOMA DE NACIONES UNIDAS

Y la última normativa que la UE ha implementado es la UNECE/R155

Además de generar normativas propias, la Unión Europea debe adherirse a las normativas que aprueba el Foro Mundial de UNECE para la Armonización de las Regulaciones de Vehículos -conocido como UNECE WP29-.

La Comisión Económica de las Naciones Unidas para Europa, o en inglés United Nations Economic Commission for Europe -UNECE-, fue creada en 1947 como una "comisión regional" de las Naciones Unidas, en la cual están incluidos 56 países miembros de Europa, Norteamérica y Asia.

Con sede en Ginebra, la UNECE tiene como propósito principal promover la integración económica y la cooperación entre los países miembros, así como promover el desarrollo sostenible y la prosperidad económica.

UNECE también establece normas, estándares y convenciones para facilitar la cooperación internacional tanto dentro como fuera de la región y, por ello, numerosos países fuera de la región utilizan los mismos estándares y normativa de la UNECE.

Dentro de UNECE existe el citado **Foro Mundial para la Armonización de las Regulaciones de Vehículos -WP29-**.

UNECE WP29 tiene el objetivo de crear, actualizar y mantener las regulaciones de los vehículos relacionadas con su tecnología, su seguridad y su protección del medio ambiente. Este es el sistema internacional de regulación de

vehículos más grande del mundo, porque 54 de sus países miembros -todos, salvo Estados Unidos y Canadá- tienen firmado un acuerdo desde 1958 por el cual se comprometen a reconocer y a aplicar dentro de sus fronteras las normativas aprobadas por UNECE WP29.

### ALGUNAS DE LAS NORMATIVAS QUE LA UNIÓN EUROPEA HA ADOPTADO DE UNECE WP29 SON:

•**Reglamento nº 151.** - Disposiciones uniformes relativas a la homologación de vehículos de motor con respecto al sistema de información de puntos ciegos para la detección de bicicletas.

•**Reglamento nº 44.** - Disposiciones uniformes relativas a la homologación de dispositivos de retención para niños ocupantes de vehículos de motor -Sistemas de retención infantil-.



## A ESTOS REGLAMENTOS HAY QUE SUMAR EL MÁS RECIENTE Y COMPLETO: EL WP29/2020/79

**Esta nueva normativa obligará a que los coches que se comercialicen en el espacio de la UE tengan un certificado de ciberseguridad.**

Consciente de los riesgos de ciberseguridad de los vehículos, UNECE WP29 aprobó, el 23 de junio de 2020, el reglamento ECE/TRANS/WP29/2020/79. Esta normativa exigirá que los vehículos cuenten con un certificado que acredite que están protegidos frente a ciberataques. Y la Unión Europea, entre otras regiones, hará obligatorio este reglamento en todo su territorio para los vehículos -coches, autobuses, camiones, furgonetas y remolques- de nueva homologación a partir de julio de 2022 y para todos los nuevos a la venta desde el 1 de julio del 2024.

Se trata, por tanto, de una normativa muy ambiciosa para la Unión Europea, que cierra el mercado a vehículos que no sean ciberseguros mucho antes, incluso, que aquellos con motores de combustión. Y es que lo máximo que, por el momento, propone la UE en materia de contaminación es multar a los fabricantes cuya media de emisiones de los vehículos que vendan exceda los 95 gramos de CO2 por kilómetro.

Los países miembros de UNECE son Albania, Alemania, Andorra, Armenia, Austria, Azerbaiyán, Bielorrusia, Bélgica, Bosnia y Herzegovina, Bulgaria, Canadá, Croacia, República Checa, Chipre, Dinamarca, Eslovaquia, Eslovenia, España, Estados Unidos, Estonia, Finlandia, Francia, Georgia, Grecia, Hungría, Islandia, Irlanda, Israel, Italia, Kazajistán, Kirguistán, Letonia, Liechtenstein, Lituania, Luxemburgo, Macedonia del Norte, Malta, Moldavia, Mónaco, Montenegro, Noruega, Países Bajos, Polonia, Portugal, Reino Unido, Rumanía, Rusia, San Marino, Serbia, Suecia, Suiza, Tayikistán, Turquía, Turkmenistán, Ucrania y Uzbekistán.

Texto completo disponible en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:42020X1596&from=EN>

La Unión Europea está formada por los siguientes países: Alemania, Austria, Bélgica, Bulgaria, Chipre, Croacia, Dinamarca, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Polonia, Portugal, República Checa, República Eslovaca, Rumanía y Suecia.

# INICIATIVAS PREVIAS A LA NORMATIVA UNECE/R155 EN ESPAÑA, EN EUROPA Y EN EL MUNDO

## A ESTOS REGLAMENTOS -151 Y 44- SE HA SUMADO UNO MÁS: EL UNECE/R155... PERO, ¿QUÉ ANTECEDENTES HAY PREVIOS A ESTE NUEVA NORMATIVA?

Los documentos previos a la llegada de la normativa UNECE/R155 eran simplemente recomendaciones, no normas vinculantes. Llama la atención que no es hasta el 2016 -aunque un medio de comunicación español alertó en el año 2013 que los vehículos que circulaban por las carreteras podrían no estar suficientemente ciberprotegidos, lo que facilitaría un ciberataque- cuando empiezan a surgir esas primeras recomendaciones de ciberseguridad aplicadas a los automóviles. Es llamativo porque hay registrados ciberataques a vehículos desde el año 2012 -ver introducción-. Una hipótesis podría ser que en 2015 tuvo lugar el ya citado hackeo de Charlie Miller y Chris Valasek a un Jeep Cherokee, el más 'popular' de los que se han producido sobre un vehículo. Lo mediático del suceso pudo haber hecho crecer la preocupación institucional con respecto a las vulnerabilidades de ciberseguridad de los vehículos.

Con esos antecedentes -ver gráfico de siguiente página-, la ONU inició el proceso de desarrollo de una norma que unificase los criterios y los requisitos, y que implante las bases mínimas de ciberseguridad para todos los vehículos. Todo esto se ha traducido en un reglamento en el que han trabajado expertos de todo el mundo y cuyos detalles se explicarán más adelante en este informe.

## ISO/SAE 21434, UN VISTAZO A LO ÚLTIMO

De forma paralela a la norma aprobada por la ONU/ UNECE WP29, la Organización Internacional de Normalización (ISO) y la Sociedad de Ingenieros Automotrices (SAE Internacional) ha desarrollado un texto que busca implementar la ciberseguridad en los vehículos durante todo su ciclo de vida. Se trata del estándar ISO/SAE 21434.

Este documento es similar a la norma de la UNECE/R155 porque especifica unos requisitos para gestionar los riesgos de ciberseguridad durante todo el ciclo de vida de los vehículos, desde sus primeras fases de su diseño hasta su desguace. LA ISO/SAE 21434 también define un lenguaje común para comunicar y gestionar el riesgo de ciberseguridad.

Ambos textos son compatibles, y presentan aspectos comunes, de forma que cumplir con uno hace sencillo cumplir con el otro. La diferencia fundamental entre el texto de la ONU y el de ISO/SAE radica en que mientras que el primero es vinculante para los países miembros de UNECE, el texto de ISO/SAE es un estándar que no es de obligado cumplimiento.

**La ISO/SAE 21434 también define un lenguaje común para comunicar y gestionar el riesgo de ciberseguridad**

El texto completo disponible en [https://www.sae.org/standards/content/j3061\\_201601/](https://www.sae.org/standards/content/j3061_201601/)

El texto completo disponible en <https://www.ic3.gov/Media/Y2016/PSA160317>

El texto completo está disponible en [https://www.nhtsa.gov/staticfiles/nvs/pdf/812333\\_CybersecurityForModernVehicles.pdf](https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf)

El texto completo está disponible en <https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars>

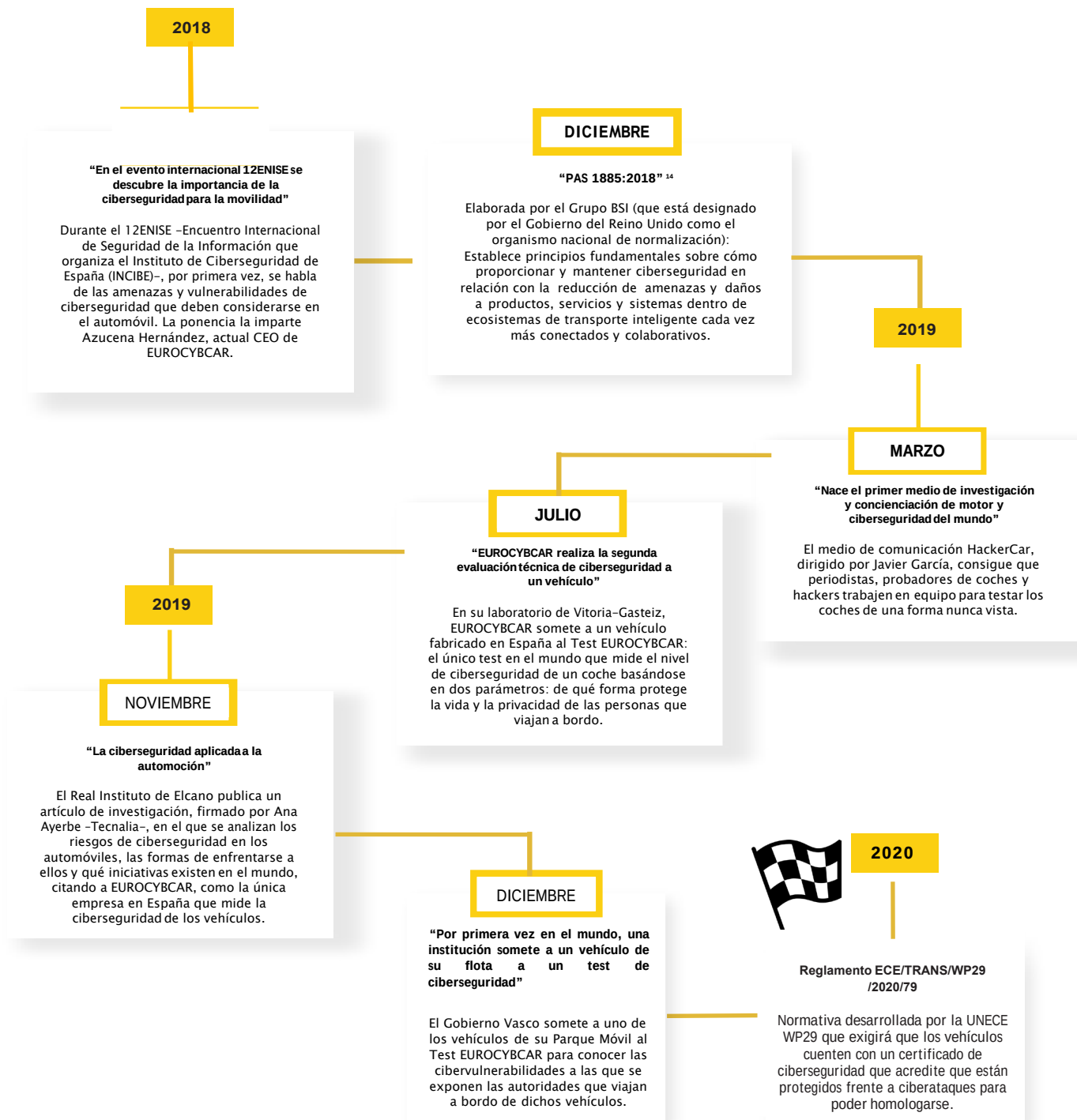
El texto completo está disponible en <https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles> y en [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/661135/cyber-security-connected-automated-vehicles-key-principles.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/661135/cyber-security-connected-automated-vehicles-key-principles.pdf)

El texto completo está disponible en <https://shop.bsigroup.com/ProductDetail/?pid=000000000030365446&ga=2.267667464.704902458.1545217114-2008390051.1545217114> Caso publicado en Wired. Disponible en <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>



## INICIATIVAS PREVIAS A LA NORMATIVA UNECE/R155





El texto completo disponible en <https://www.autofacil.es/usuario/2013/11/17/hacker-matarte-conduces/16435.html>

Grabación de la conferencia disponible en [https://www.youtube.com/watch?v=oFi8QxdK\\_AQ&t=3s](https://www.youtube.com/watch?v=oFi8QxdK_AQ&t=3s)  
<https://hacker-car.com/>

Los vídeos de sus conferencias se pueden visionar en <https://www.youtube.com/watch?v=nu3mHMuXlOw>

El texto completo disponible en [http://www.realinstitutoelcano.org/wps/portal/rielcano\\_es/contenido?WCM\\_GLOBAL\\_CONTEXT=/elcano/elcano\\_es/zonas\\_es/ciberseguridad/ari105-2019-ayerbe-ciberseguridad-aplicada-a-la-automocion](http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ciberseguridad/ari105-2019-ayerbe-ciberseguridad-aplicada-a-la-automocion)



# TODO SOBRE LA NORMATIVA UNECE/R155

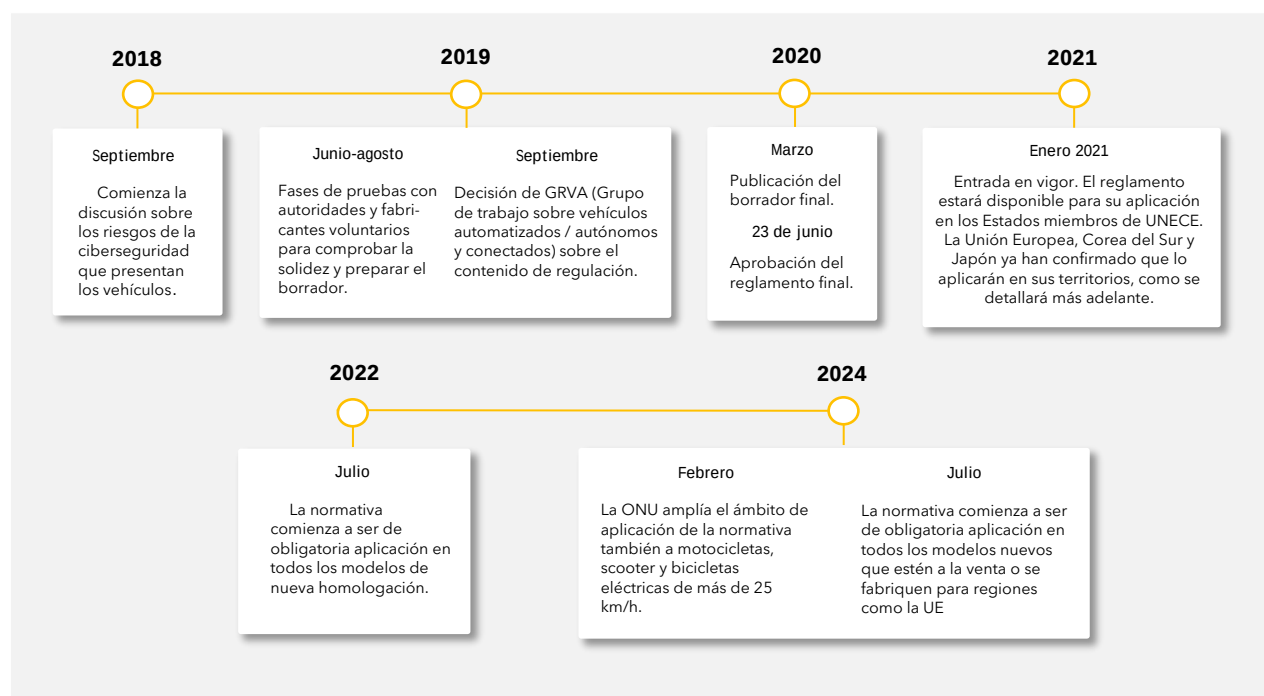
## LA NORMA QUE REGULA LA CIBERSEGURIDAD DE LOS VEHÍCULOS

### QUÉ DICE EL REGLAMENTO UNECE/R155

El 23 de junio de 2020, se aprobó esta norma que regula la ciberseguridad de los vehículos. La norma en cuestión es la ECE/TRANS/WP29/2020/79 y se titula “Reglamento de las Naciones Unidas sobre disposiciones uniformes relativas a la homologación de vehículos a motor en lo que respecta a la ciberseguridad y el sistema de gestión de ciberseguridad”.



### FASES DE DESARROLLO DE LA NORMA



En inglés, UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. Texto íntegro está disponible a través del siguiente enlace: <http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf>

**TRATA SOBRE MEDIDAS UNIFORMES NECESARIAS** para crear un sistema de gestión de ciberseguridad en los vehículos. Es decir, un sistema que trate el riesgo asociado con las amenazas y que proteja los vehículos de ataques cibernéticos.

## EL ÍNDICE DEL DOCUMENTO DEL REGLAMENTO UNECE/R155

1. **Ámbito de aplicación:** a qué vehículos afecta la norma.
2. **Definiciones de algunos términos** empleados a lo largo del reglamento.
3. **Solicitud de homologación:** documentación a presentar para lograr la aprobación.
4. **Marca de homologación:** símbolo que deberán incluir los vehículos que cumplan el reglamento en su placa de identificación.
5. **Homologación:** papel de la entidad verificadora del cumplimiento del reglamento.
6. **Certificado** de conformidad del CSMS.
7. **Especificaciones:** detalle de las exigencias que el reglamento hará cumplir.
8. **Modificación del tipo de vehículo y extensión de la homologación de tipo:** cómo efectuar modificaciones en los vehículos

9. **Conformidad de la producción.**
10. **Sanciones** por falta de conformidad de la producción.
11. **Cese definitivo de la producción:** cómo comunicar que un vehículo cesa su producción.
12. **Nombres y direcciones** de los servicios técnicos responsables de realizar los ensayos de homologación.

### ANEXOS

- 1 Ficha técnica.
- 2 Comunicación.
- 3 Disposición de la marca de homologación.
- 4 Modelo del certificado de conformidad.
- Lista de amenazas y sus medidas de mitigación.
- 5 Lista de amenazas a evitar y sus correspondientes modificaciones.

## ESTE REGLAMENTO PROPORCIONA UN MARCO PARA QUE EL SECTOR AUTOMOTRIZ ESTABLEZCA LOS PROCESOS NECESARIOS PARA:



Identificar y gestionar los riesgos de ciberseguridad en el diseño de vehículos.



Verificar que se gestionen los riesgos, incluidas las pruebas.



Asegurar que las evaluaciones de riesgos se mantengan actualizadas.



Monitorizar los ciberataques y que se responda efectivamente a ellos.



Analizar los ataques exitosos o intentados.



Evaluar si las medidas de ciberseguridad siguen siendo efectivas a la luz de las nuevas amenazas y vulnerabilidades

## EL CSMS DEBE PROTEGER A LOS VEHÍCULOS CONTRA 70 AMENAZAS DE CIBERSEGURIDAD ESPECÍFICAS, SEGÚN LA NORMATIVA UNECE/R155

PARA CUMPLIR CON LA NORMATIVA, LOS FABRICANTES TIENEN QUE CREAR PARA SUS VEHÍCULOS UN SISTEMA DE GESTIÓN DE CIBERSEGURIDAD -CSMS, POR SUS SIGLAS EN INGLÉS-.

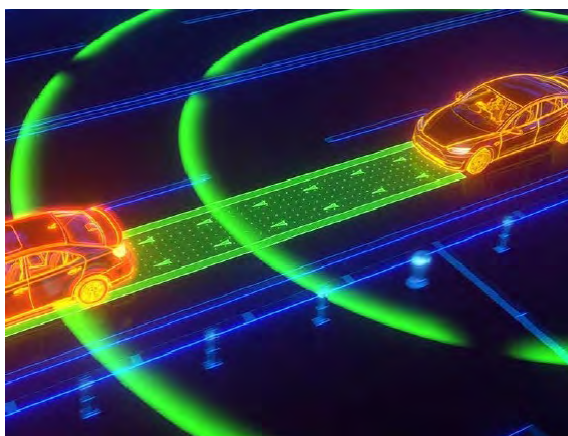
El CSMS es un sistema de procesos que, en conjunto, deben garantizar la ciberseguridad del vehículo de forma adecuada frente a diferentes ciberataques.

Un CSMS que cumpla con los requisitos marcados por la ONU significará que ese fabricante gestiona la ciberseguridad de sus modelos a lo largo de todo su ciclo de vida: desarrollo, producción y posproducción. Además, cada una de esas fases incluirá protecciones contra sus amenazas de ciberseguridad específicas.

**EL CSMS DEBE PROTEGER A LOS VEHÍCULOS CONTRA 70 AMENAZAS DE CIBERSEGURIDAD ESPECÍFICAS QUE LA ONU DETALLA EN SU REGLAMENTO. ESTAS VULNERABILIDADES SE DIVIDEN EN 7 APARTADOS Y SON:**

- **AMENAZAS RELACIONADAS CON LOS SERVIDORES BACK-END.** Estos servidores son los hacen que todo el sistema informático de los vehículos o las redes informáticas internas del fabricante funcionen. Se deberán evitar, entre otras amenazas, pérdidas de información en la nube, filtraciones de información por compartir datos de forma involuntaria y que un trabajador haga un uso ilícito de los datos a los que tiene acceso.

- **AMENAZAS RELACIONADAS CON LOS CANALES DE COMUNICACIÓN QUE USA EL VEHÍCULO PARA CONECTARSE CON SU ENTORNO** -por ejemplo, otros vehículos o la infraestructura-. Se deberán evitar, entre otras amenazas, que se pueda suplantar la identidad de otros vehículos, inyectar malware -programas que dañan los sistemas informáticos- por los canales de comunicación y manipular o eliminar los datos y códigos del software del vehículo.



• **AMENAZAS A LAS CONEXIONES Y CONECTIVIDAD EXTERNA.** Se deberán evitar, entre otras amenazas, la manipulación de funciones remotas, como la llave, el inmovilizador y la batería; manipular las conexiones telemáticas del vehículo, como la medición de la temperatura de la mercancía en vehículos industriales o desbloquear las puertas de forma remota; y causar interferencias en los sistemas inalámbricos de corto alcance o sensores.

• **AMENAZAS A LOS DATOS/CÓDIGO DEL VEHÍCULO.** Se deberán evitar, entre otras amenazas, que se pueda acceder sin deber a la información privada del propietario -quién es, su cuenta bancaria, ubicación, identificación electrónica del vehículo- y falsificar la identidad o manipular datos del vehículo -kilometraje, velocidad de conducción, enviar mensajes falsos e indicaciones al conductor, etc.-.

• **AMENAZAS RELACIONADAS CON LOS PROCEDIMIENTOS DE ACTUALIZACIÓN DE LOS VEHÍCULOS.** Se deberá de evitar cualquier tipo de amenaza que afecte a los procesos de actualización de los sistemas informáticos de los vehículos, ya sea que se lleven a cabo de forma inalámbrica -Over The Air- o mediante una descarga.

• **AMENAZAS RELACIONADAS CON ACCIONES HUMANAS NO INTENCIONADAS.** Se deberán de evitar, entre otras amenazas, que alguien con acceso al vehículo -como el propietario o un mecánico- pueda introducirle un virus de forma involuntaria si lo engaña un ciberdelincuente.

• **POSIBLES AMENAZAS QUE PODRÍAN EXPLOTARSE SI NO SE PROTEGEN O REFUERZAN LO SUFICIENTE.** Se deberán de evitar, entre otras amenazas, fallos de software, que la información del primer propietario del vehículo pase al segundo dueño -en caso de venderse en el mercado de ocasión-, o que se reemplacen elementos del vehículo que cumplan con la norma por otros que la incumplan.

**LA RESPONSABILIDAD DE CUMPLIR CON EL CSMS SERÁ DE LOS OEM -FABRICANTES-.** Además, también deberán comprobar que todos los proveedores de su cadena de suministro identifican y gestionan los riesgos de ciberseguridad del componente que pro-



porcionan. Por tanto, los proveedores no están directamente obligados a cumplir con los requisitos de la UNECE/R155 pero no hacerlo les perjudicará a la hora de ser competitivos y no serán rentables.

Si bien la normativa de ONU/UNECE WP29 establece un marco regulatorio y unos requisitos mínimos para los fabricantes a lo largo de la cadena de valor, el texto no incluye una guía de implementación detallada para traducir los requisitos en métodos concretos que eviten los ciberataques. Es decir, a los fabricantes se les proporciona un listado con los riesgos que deben evitar en sus modelos a lo largo de todo el ciclo de vida del vehículo, pero, por el momento, deben de ser ellos quienes piensen cómo darles solución, aunque el certificado deberá emitirlo una entidad externa.

## CÓMO OBTENER EL CERTIFICADO DE CIBERSEGURIDAD

### UNA ENTIDAD TÉCNICA EXTERNA AL FABRICANTE SERÁ LA QUE ACREDITE QUE EL VEHÍCULO CUMPLE CON LOS REQUISITOS MARCADOS POR LA ONU/UNECE

Para que un modelo de vehículo obtenga el certificado de ciberseguridad que acredite que cumple con los requisitos establecidos por la ONU, los fabricantes deberán someterlo a unas evaluaciones. Hasta ahora, los OEMs contrataban a empresas de consultoras de ciberseguridad para auditar de forma puntual algunos de los sistemas de sus vehículos, pero, con la entrada en vigor de la nueva normativa **tendrán la obligación de contratar un servicio técnico externo que certifique que su vehículo es ciberseguro.**

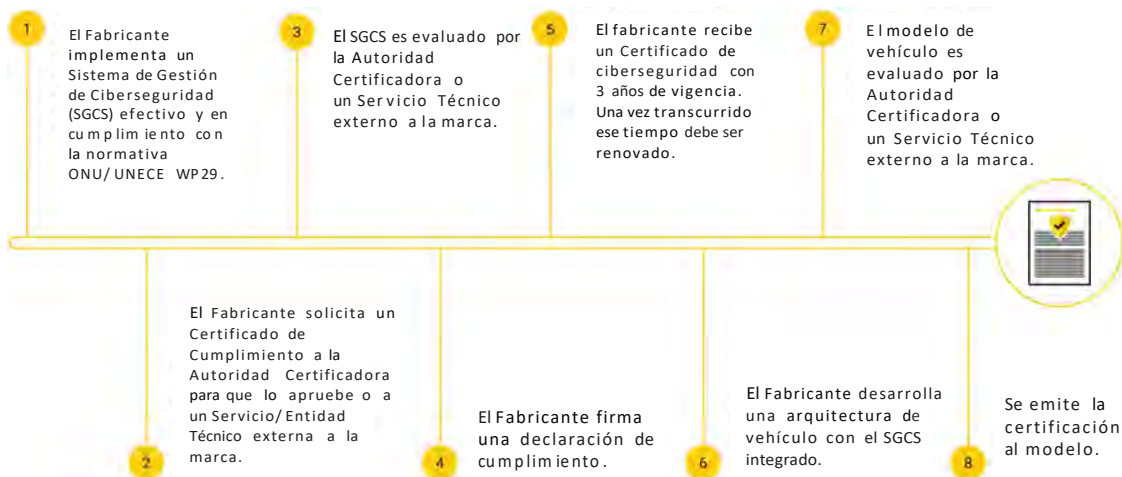
Deberán presentar documentación suficiente para poder evaluar el funcionamiento del CSMS. Entonces, una Entidad Autorizada analizará esos documentos y realizará pruebas al vehículo. Todo este proceso tiene el objetivo de poder certificar que el fabricante ha tomado las medidas mínimas necesarias para garantizar que el tipo de vehículo y su CSMS son ciberseguros, mediante la evaluación de la documentación presentada y la realización de pruebas al tipo de vehículo.

**LA ENTIDAD AUTORIZADA O SERVICIOS TÉCNICO** que lleve a cabo la evaluación del fabricante, debe

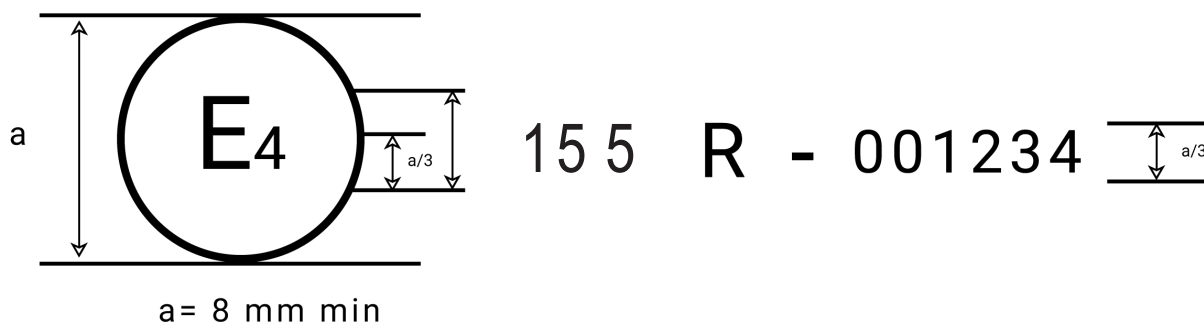
asegurar que cumple con los requisitos expuestos en Apéndice 2 del “Acuerdo con respecto a la adopción de reglamentos técnicos armonizados de las Naciones Unidas para vehículos con ruedas, equipos y piezas que pueden montarse y/o utilizarse en vehículos con ruedas y las condiciones para el reconocimiento recíproco de las aprobaciones concedidas sobre la base de este reglamento de las Naciones Unidas”. Algunos de los requisitos que establece el citado acuerdo son que la entidad escogida deberá demostrar que disponen de habilidades apropiadas, conocimientos técnicos específicos y experiencia probada en el campo que cubra cada normativa de la ONU (en el caso del reglamento de ONU/UNECE WP29, ciberseguridad para vehículos), debe de estar libre de cualquier control e influencia de las partes interesadas y debe tener acceso a las instalaciones de prueba y dispositivos de medición necesarios para realizar las pruebas.

Las Entidades Autorizadas deberán ser previamente designadas por los fabricantes para realizar las pruebas de evaluación e inspecciones. Hasta la fecha se desconoce si antes de la entrada en vigor del reglamento, se elaborará algún documento más específico, donde se acuerde una interpretación común de los métodos y criterios de evaluación.

## ASÍ ES EL PROCESO DE CERTIFICACIÓN







## ESTA ES LA ETIQUETA DE VEHÍCULO CIBERSEGURO

### ¿EL VEHÍCULO ES APTO O NO APTO?

El servicio técnico o entidad autorizada rechazará la concesión del certificado de cumplimiento con el CSMS del vehículo cuando:

1. No se cumpla con uno o más de los 70 requisitos de ciberseguridad exigidos por el reglamento de ONU/UNECE WP29.
2. En caso de que el fabricante **no proporcione a la Entidad Autorizada la suficiente información** para evaluar la ciberseguridad del tipo de vehículo.

**VIGENCIA DE TRES AÑOS.** El certificado de conformidad del CSMS **será válido por un máximo de tres años** a partir de la fecha de expedición, a menos que sea retirado. Cuando la validez del certificado esté próxima a finalizar, se deberá solicitar un nuevo certificado de cumplimiento -si ha habido cambios en el reglamento-, o extender la validez del anterior por un período adicional de tres años. Para esto, la Entidad Autorizada designada, deberá evaluar que se los requisitos expuestos en el reglamento se siguen cumpliendo. En el caso de que ya no se cumpla con los requisitos tras la caducidad del certificado, se procederá a la retirada de este.

**SERÁ OBLIGATORIO.** Además, el fabricante también deberá informar a la Entidad Autorizada de **cualquier cambio que afecte a la relevancia del certificado** de cumplimiento del CSMS, como la aparición de nuevos ciberataques. Tras consultar con el fabricante, la Entidad Autorizada decidirá si es necesario realizar nuevas comprobaciones para saber si se siguen cumpliendo los requisitos exigidos.

**LA ETIQUETA DE VEHÍCULO CIBERSEGURO.** Aquellos vehículos que reciban el certificado de cumplimiento con el CSMS deberán indicarlo en su ficha de homologación me-

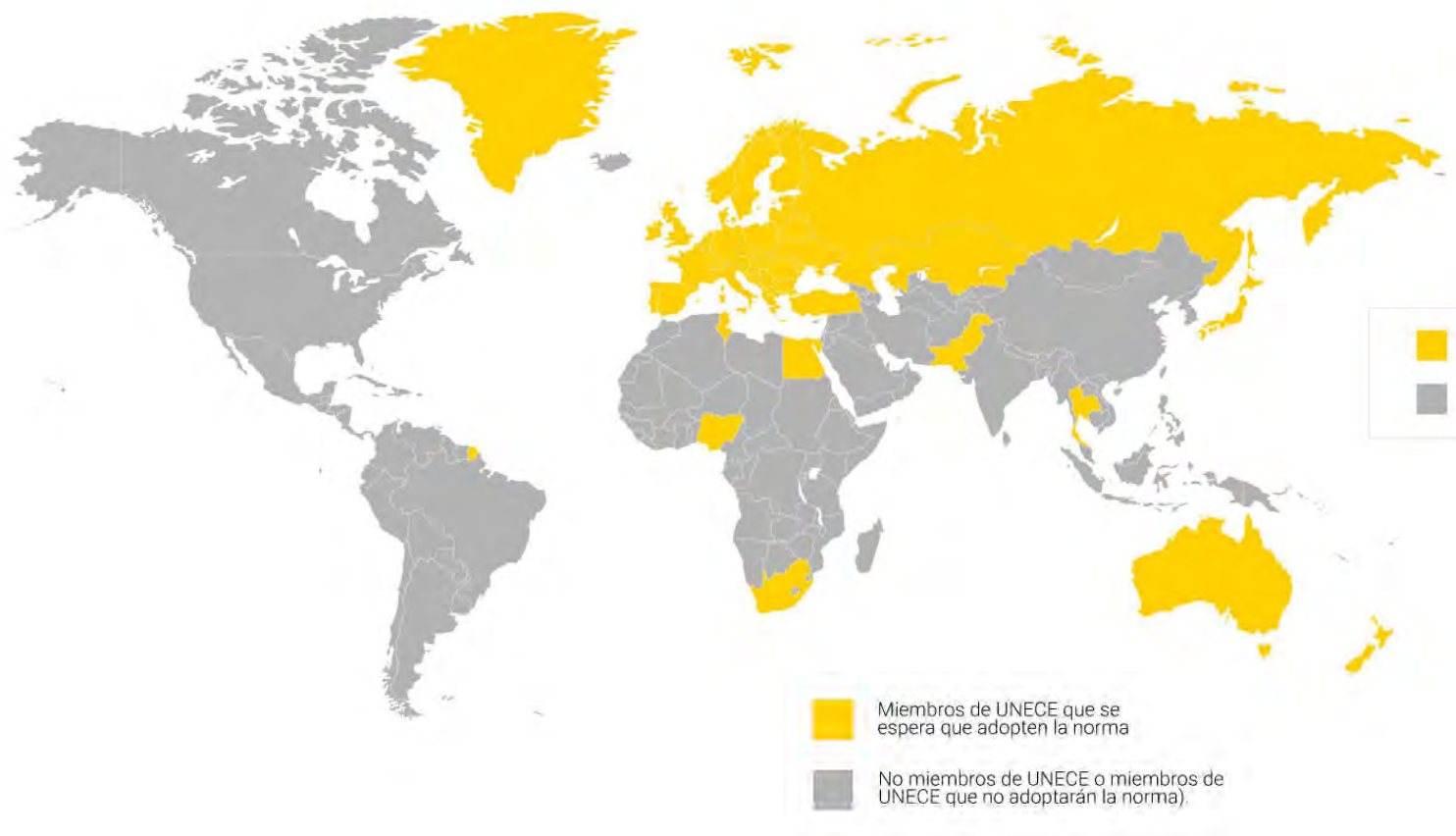
dante una marca. **Esta marca estará compuesta por:**

- Una letra "E" seguida del número distintivo del país que ha concedido la certificación, rodeados ambos por un círculo.
- A la derecha de esa marca se situará el **número del reglamento de la ONU**.
- A ese número lo seguirá una letra "R", un guion y el **número de homologación**.

Esta marca deberá situarse de forma visible y fácilmente accesible dentro o cerca de la placa de identificación del vehículo. La imagen de la parte superior es un ejemplo de marca de homologación para mostrar que un vehículo tiene un CSMS cuyo funcionamiento ha sido certificado según los requisitos de ONU/UNECE WP29. En este ejemplo, **los elementos que componen esta marca de homologación indican lo siguiente:**

- **E4:** Muestra que el CSMS del vehículo ha sido certificado en los Países Bajos -el número varía según el país-.
- **155:** Indica el número del reglamento para el cual el coche ha logrado la certificación.
- **R-001234:** El número de homologación. Los dos primeros dígitos del número de homologación -00- indican que se homologó con los requisitos del reglamento de la ONU en su forma original.





## MIEMBROS DE UNECE QUE ADOPTARÁN LA NORMATIVA UNECE/R155 PORQUE FIRMARON ACUERDO DE RECONOCIMIENTO RECÍPROCO DE APROBACIONES

### QUÉ PAÍSES APLICARÁN LA NORMA Y EN QUÉ PLAZOS

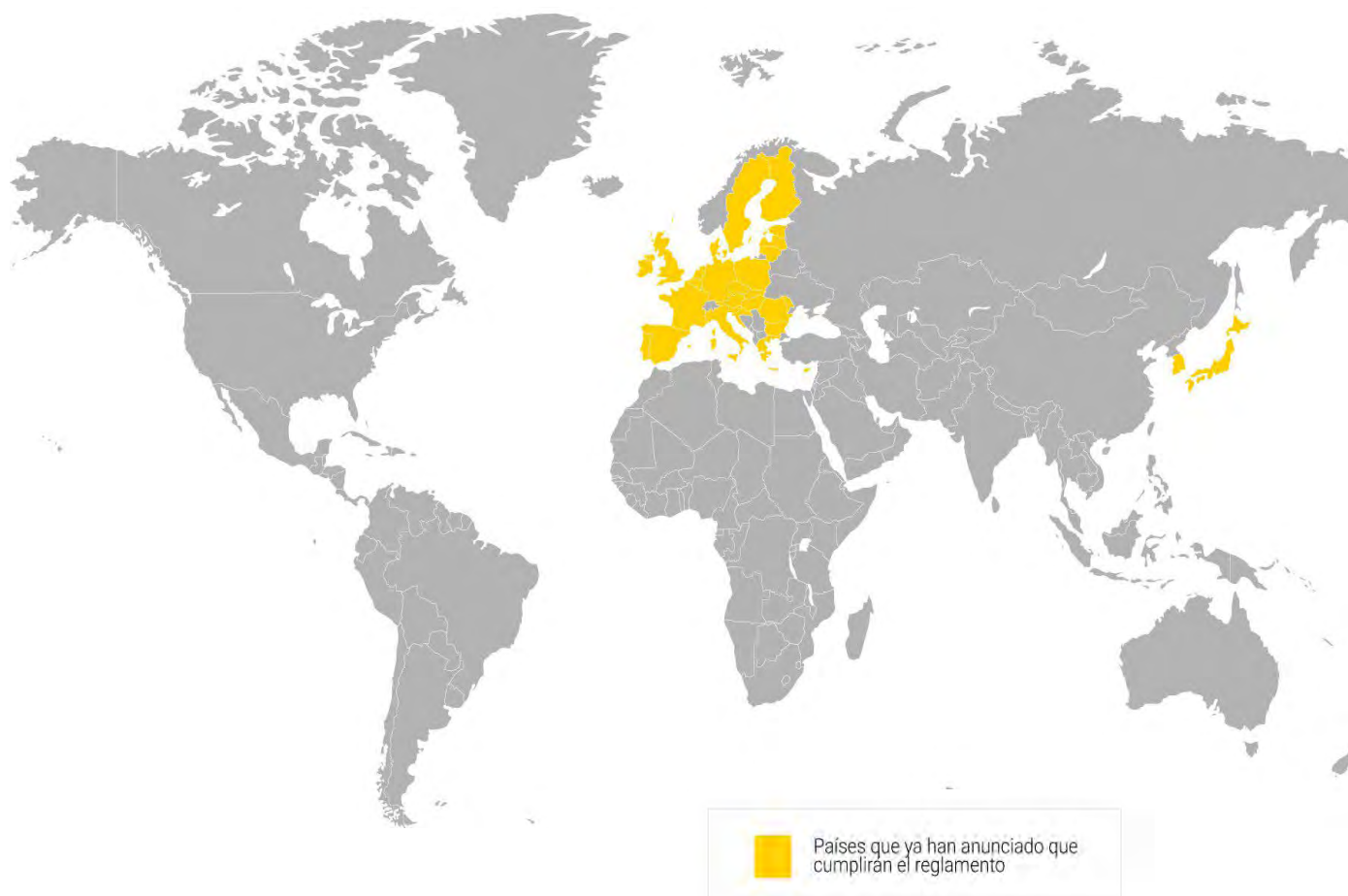
El texto ya está aprobado y desde el 22 de enero de 2021 entra en vigor. A partir de esa fecha, ya lo han adoptado 54 estados de los 56 estados miembros de UNECE -todos salvo EE.UU. y Canadá-, ya que son ellos los que tienen firmado un acuerdo de reconocimiento recíproco de las regulaciones que este foro apruebe. Esos países son los siguientes:

#### Los 54 miembros de UNECE que aplicaron la norma desde el 22 de enero 2021

|                     |             |               |                       |                  |              |
|---------------------|-------------|---------------|-----------------------|------------------|--------------|
| -Albania            | -Croacia    | -Hungría      | -Nueva Zelanda        | -Rumanía         | -Suiza       |
| -Armenia            | -Rep. Checa | -Italia       | -Nigeria              | -Federación Rusa | -Tailandia   |
| -Australia          | -Dinamarca  | -Japón        | -Macedonia            | -San Marino      | -Túnez       |
| -Austria            | -Egipto     | -Kazajistán   | -Noruega              | -Serbia          | -Turquía     |
| -Azerbaiján         | -Estonia    | -Letonia      | -Pakistán             | -Eslovaquia,     | -Ucrania     |
| -Bielorrusia        | -Finlandia  | -Lituania     | -Polonia              | -Eslovenia       | -Reino Unido |
| -Bélgica            | -Francia    | -Luxemburgo   | -Portugal             | -Sudáfrica       | -Irlanda     |
| -Bosnia Herzegovina | -Georgia    | -Malasia      | -Corea del Sur        | -España          | del Norte    |
| -Bulgaria           | -Alemania   | -Montenegro   | -República de Moldova | -Suecia          |              |
|                     | -Grecia     | -Países Bajos |                       |                  |              |

A la izquierda, los países en los que se aplica la norma UNECE/R155 dentro de sus territorios a fecha de 22 de enero de 2021.





## PAÍSES QUE YA HAN CONFIRMADO QUE APLICARÁN LA NORMA UNECE/R155 EN SUS TERRITORIOS

### Union Europea

|           |           |                 |                      |
|-----------|-----------|-----------------|----------------------|
| Alemania  | España    | Letonia         | República Eslovaca   |
| Austria   | Estonia   | Lituania        | Rumanía              |
| Bélgica   | Finlandia | Luxemburgo      | Suecia               |
| Bulgaria  | Francia   | Malta           |                      |
| Chipre    | Grecia    | Países Bajos    | <b>Asia Pacífico</b> |
| Croacia   | Hungría   | Polonia         |                      |
| Dinamarca | Irlanda   | Portugal        | Japón                |
| Eslovenia | Italia    | República Checa | Corea del Sur        |

La UE ha establecido que todos los vehículos que se están homologando desde julio del 2022 deben cumplirlo. Esa obligación se extiende a partir del 1 de julio de 2024 a todos los coches nuevos. Por su parte, las autoridades japonesas han trasladado que vienen exigiendo a las marcas que vendan vehículos dentro de sus fronteras que cumplan el reglamento desde enero de 2021.

En cuanto a Corea del Sur, ya viene aplicando el reglamento desde el segundo semestre de 2020, aunque, según parece, de forma gradual.

## A QUÉ VEHÍCULOS AFECTARÁ LA NORMATIVA UNECE/R155

### EL REGLAMENTO SE APLICARÁ A LAS SIGUIENTES CATEGORÍAS DE VEHÍCULOS

- **CATEGORÍA M.** Vehículos a motor destinados al transporte de personas y que tengan al menos cuatro ruedas, o tres ruedas y un peso máximo superior a 1 tonelada. Por ejemplo, turismos, autobuses y autocaravanas.
- **CATEGORÍA N.** Vehículos a motor destinados al transporte de mercancías y que tengan por lo menos cuatro ruedas, o tres ruedas y un peso máximo superior a 1 tonelada. Por ejemplo, furgonetas y camiones.
- **CATEGORÍA O.** Remolques y caravanas con una unidad de control electrónico.

• **CATEGORÍAS L6 Y L7.** Cuadriciclos con o sin cabina para el transporte de personas. En este caso, solo les afecta el reglamento si están equipados con funciones de conducción automatizada desde el nivel 3 en adelante.

Por tanto, todos los fabricantes de turismos, furgonetas, camiones y autobuses que quieran homologar nuevos modelos a partir de julio del 2022 o, simplemente, vender vehículos nuevos a partir del 1 de julio del 2024 en los países miembros de la UE ya deben cumplir con los requisitos exigidos por la normativa UNECE/R155.

## Categorías de vehículos afectados por la UNECE



**Categoría M:**  
Coches y autobuses.



**Categoría N:**  
Furgonetas y camiones.



**Categoría O:**  
Remolques y caravanas con una unidad de control electrónica.



**Categoría L6 y L7:**  
Cuadriciclos ligeros y sin cabina si cuentan con al menos nivel 3 de conducción autónoma.

## ¡ATENCIÓN! LA NORMATIVA SE HA AMPLIADO PARA INCLUIR A MOTOS, SCOOTER Y BICICLETAS ELÉCTRICAS DE MÁS DE 25 KM/H

EXCLUSIVAS

### ¡UNA EMPRESA DE CIBERSEGURIDAD VASCA PROVOCA UN CAMBIO EN LA NORMATIVA EUROPEA!

La ONU ha tomado una decisión crucial: incluir también en la normativa de ciberseguridad UNECE/R155... a las motocicletas. Un cambio provocado por la actuación de la empresa vasca, EUROCYBCAR, que demostró que este tipo de vehículos, cada vez más tecnológicos y conectados, también debían ser tenidos en cuenta en el texto de la norma.

HC - hace 2 meses 0



La ONU ha tomado una decisión crucial: incluir también en la normativa de ciberseguridad UNECE/R155 a las motocicletas. Un cambio provocado por la actuación de la empresa vasca, EUROCYBCAR, que demostró que este tipo de vehículos, cada vez más tecnológicos y conectados, también debían ser tenidos en cuenta en el texto de la norma. Así lo han destacado recientemente medios de comunicación como HackerCar.

El año 2024 iba a pasar a la historia porque, desde julio, todos los modelos que se vendan o fabriquen en o para la Unión Europea, y en Corea del Sur o Japón, deben ser ciberseguros por ley. Sin embargo, esta normativa, sorprendentemente, había dejado de lado a las motos, los scooters y bicicletas eléctricas, porque consideraban que no tenían suficiente conectividad.

Eso era hasta ahora. Y es que, tal y como ha confirmado la UNECE, la norma se actualiza para dar cabida a las motos, scooters y bicicletas eléctricas con una velocidad superior a 25 km/h. ¿La razón? Que, por fin, reconocen que EUROCYBCAR -empresa de ciberseguridad y tecnología con sede en Vitoria-Gasteiz-, tenía razón: Las motos sí disponen de suficiente conectividad para ser susceptibles de sufrir un ciberataque.

“Tras la revisión de los requisitos de ese reglamento y su posible idoneidad para abordar adecuadamente las especificidades de las motocicletas, el Grupo de Trabajo acordó insertar esta categoría de vehículos en el alcance del Reglamento 155 de la ONU, con el apoyo de la industria de las motocicletas”, ha destacado el comunicado oficial de UNECE.

■ Número de modelos ofrecidos en 2024

## ¿A CUÁNTOS VEHÍCULOS AFECTARÁ?

### NÚMERO DE MODELOS ACTUALES QUE TIENEN A LA VENTA CADA GRUPO AUTOMOVILÍSTICO Y LOS QUE LANZARÁN HASTA 2024

Para estimar la cantidad de vehículos que se verían afectados cada año por la normativa de ONU/UNECE WP29, se ha tomado como referencia 2023 -el último año completo del que se tienen datos de ventas de vehículos-. Ese año, en todo el mundo se vendieron aprox 92,4 millones vehículos. De esa cifra, 19.076.481 se vendieron en la UE, Japón y Corea del Sur -las regiones que ya han confirmado que aplicarán el reglamento UNECE/R155, distribuidas de la siguiente manera:

• **12.847.481 uds.** vendidas en 2023 en la Unión Europea.

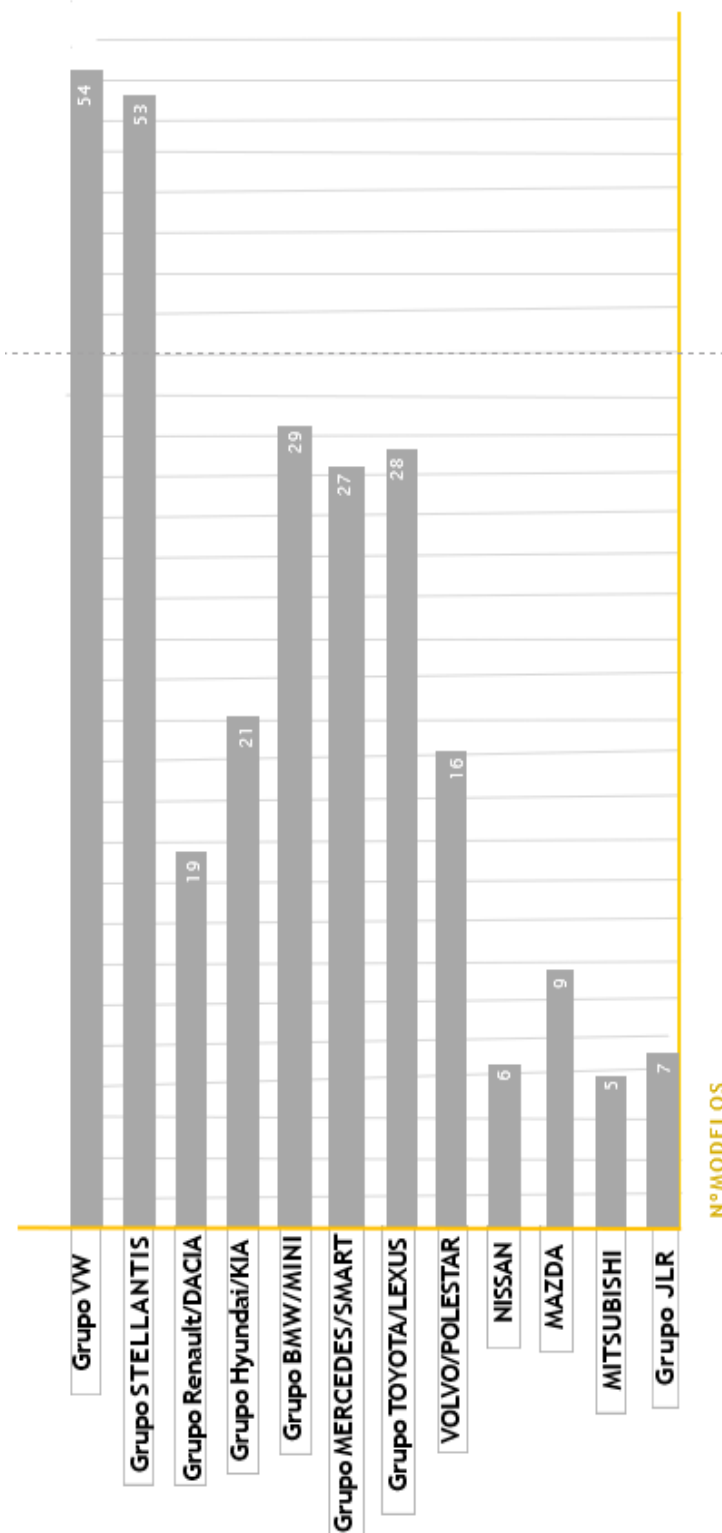
• **4.779.066 uds.** vendidas en 2023 en Japón.

• **1.449.885 uds.** vendidas en 2023 en Corea del Sur.

Eso supone que, de todos los vehículos que se venden cada año en el mundo, aproximadamente el 25% de ellos lo hacen en territorios donde se aplicará el reglamento UNECE/R155.

En cuanto a los nuevos modelos que se han comercializado durante el periodo 2021-2024, los principales grupos automovilísticos habrán puesto a la venta, en la UE, alrededor de 450 nuevos modelos.

**Por otro lado, se abre una oportunidad de negocio para las OEMs que fabrican coches en España, porque serán más competitivos si son de los primeros que fabrican coches ciberseguros -que cumplen con los requisitos de ciberseguridad que exige la nueva normativa, sometiendo sus vehículos al Test EUROCYBCAR.**



Nº MODELOS

| Fábricas Coches / Furgonetas    | Modelos Fabricados en España 2023                                                    |
|---------------------------------|--------------------------------------------------------------------------------------|
| SEAT/CUPRA<br>GRUPO PSA         | Barcelona: 5 modelos                                                                 |
| STELLANTIS                      | Vigo: 9 modelos<br>Figueruelas, Zaragoza: 4 modelos<br>Villaverde, Madrid: 2 modelos |
| GRUPO VW                        | Landaben, Pamplona: 3 modelos                                                        |
| RENAULT                         | Palencia: 2 modelos<br>Valladolid: 3 modelos                                         |
| MERCEDES                        | Vitoria: 2 modelos                                                                   |
| FORD                            | Alumssafes, Valencia: 2 modelos                                                      |
| IVECO                           | Madrid: 3 modelos                                                                    |
| Fábricas Camiones               | - IVECO Madrid: 3 modelos                                                            |
| Fábricas Autobuses / Carroceros | - 11 MARCAS: 70 modelos                                                              |

Esta información ha sido recopilada a fecha de enero de 2024. Es un calendario no oficial de lanzamientos previstos hasta el año 2024, basado en la información del ciclo de vida de los modelos actuales y en los datos recopilados por el equipo de expertos y análisis de mercado de Grupo Cybentia.

Datos de Expansión disponibles en <https://datosmacro.expansion.com/negocios/produccion-vehiculos>



## A QUÉ SANCIONES SE ENFRENTAN LOS FABRICANTES SI NO CUMPLEN LA NORMATIVA

LOS FABRICANTES QUE INCUMPLAN EL REGLAMENTO UNECE/R155 SE PUEDEN ENFRENTAR A DOS TIPOS DE SANCIONES: UNA DE LA PROPIA UNECE Y OTRA DE LA PROPIA UNIÓN EUROPEA

- **En el caso de la UNECE/R155**, el apartado 10 de su reglamento de ciberseguridad en vehículos afirma que un país podrá retirar la homologación concedida a un tipo de vehículo si descubre que no cumple con los requisitos establecidos por la UNECE/R155. Además, ese país deberá notificar inmediatamente la infracción al resto de estados que apliquen el reglamento.

- De forma paralela, como para poder homologar vehículos **en la UE será necesario cumplir con la normativa UNECE/R155** -según las condiciones explicadas anteriormente-, incumplirlo conllevará también incumplir el reglamento de homologación de la UE, por lo que el fabricante sería sancionado según el Reglamento sobre homologación y vigilancia del mercado de vehículos de motor.

En él se afirma que, si la UE detecta que un fabricante ha infringido la normativa de homologación en sus vehículos, podrá sancionar a la marca por cada unidad que no reúna las condiciones de ciberseguridad exigidas. La UE también podrá retirar o suspender la homologación de tipo de esos vehículos.

# ¿CÓMO CUMPLIR CON EL REGLAMENTO?

## LA METODOLOGÍA ESTP (EUROCYBCAR® STANDARD TEST PROTOCOL)

**LA ONU/UNECE HA DEJADO LIBERTAD A LOS FABRICANTES** a la hora de buscar soluciones para cumplir con los 70 requisitos que refleja en su reglamento, porque no detalla cómo evitar esas amenazas. Eso abre la puerta a que los fabricantes colaboren activamente con las empresas especializadas en soluciones de securización automotriz, como Argus, Upstream, Guardknox o Harman.

**Tampoco la normativa aún indica qué tipo de pruebas deben realizar las entidades homologadoras** para saber si un vehículo puede obtener el certificado APTO de ciberseguridad. Pero la empresa EUROCYBCAR ha patentado un test para evaluar el nivel de ciberseguridad de los vehículos y certificar si dicho vehículo cumple con los 70 requisitos de ciberseguridad que exige la norma UNECE/R155. Las pruebas se realizan en su laboratorio ubicado en Vitoria-Gasteiz, donde hackers, Ingenieros IT, probadores de coches y CyberQTester desde hace años realizan la evaluación técnica de ciberseguridad -el ESTP- a vehículos de organismos públicos y OEMs.

### EL TEST EUROCYBCAR CERTIFICA SI EL VEHÍCULO CUMPLE LOS REQUISITOS QUE EXIGE LA UNECE/R155, REALIZANDO TRES TIPOS DE PRUEBAS

- **DE ACCESO FÍSICO:** El equipo de expertos de EUROCYBCAR comprueba, por ejemplo, si un ciberdelincuente podría manipular -a través del puerto OBD del vehículo- el airbag, sus frenos o su dirección; o si a través del puerto USB se puede introducir un virus que provoque la paralización de los sistemas del vehículo y ponga en riesgo la vida de los pasajeros.

- **DE ACCESO REMOTO:** se analiza sistemas inalámbricos como la conexión Bluetooth -que permite enlazar el dispositivo móvil al vehículo para compartir sus datos-, WiFi -que proporciona conexión a internet a los dispositivos móviles de los pasajeros-, el eCall -llamada automática a Emergencias en caso de accidente- o el sistema keyless -que, por ejemplo, permite abrir o cerrar un coche sin necesidad de utilizar la llave- para comprobar su nivel de ciberseguridad y valorar si la seguridad del vehículo o los datos privados de los usuarios se está poniendo en riesgo.

- **PRUEBAS DE APLICACIONES:** Por último, se evalúan las vulnerabilidades de las aplicaciones que ya están integradas en el vehículo, y también las apps oficiales de la marca que el usuario se descarga en su móvil.

Algunas de estas aplicaciones permiten al usuario controlar desde su smartphone diversos parámetros del vehículo -como encender la calefacción antes de entrar- o acceder a información almacenada en el ve-

hículo -como el kilometraje o las rutas seguidas habitualmente por el conductor-. Esto, obviamente, es un peligro si un ciberdelincuente consigue vulnerar dichas aplicaciones, ya que podría acceder a sistemas del vehículo y llegar incluso a provocar un accidente.

**La Metodología ESTP** -EUROCYBCAR Standard Protocol Test- es el único TEST integral en todo el mundo -con patente internacional- que identifica vulnerabilidades y mide el nivel de ciberseguridad de un vehículo -coches, autobuses, camiones y furgonetas-, según lo requisitos de la nueva normativa UNECE/R155.

Una vez que el vehículo se ha sometido al protocolo de pruebas de EUROCYBCAR y lo ha superado -es APTO- se le concede un certificado de ciberseguridad, junto con AENOR, que avala el nivel de ciberseguridad que ha obtenido el vehículo.

Pero, sobre todo, una buena nota en el test será sinónimo de que el coche en cuestión lleva implementadas las medidas mínimas para evitar que alguien pueda tomar el control a distancia de sistemas como la dirección, los frenos, el motor... y causar accidentes con grave riesgo para la vida del conductor y los pasajeros, o la de otros usuarios de la vía-.



# PRIMER CERTIFICADO DE CIBERSEGURIDAD: EUROCYBCAR,® NUUK Mobility Solutions y AENOR

Como ya se ha expuesto, la normativa UNECE/R155 va a ampliarse para los vehículos de dos ruedas también deban contar con un certificado de ciberseguridad para que puedan ser comercializadas en el mercado europeo. Por ello es destacable que la firma NMS -NUUK Mobility Solutions-, consciente de la importancia que tiene la ciberseguridad, decidiera someter uno de sus vehículos -la CargoPro 6.0- al Test EUROCYBCAR, marcando un hito histórico mundial al ser el primer vehículo en el mundo que ha obtenido un certificado de ciberseguridad -proceso de certificación realizado en conjunto con AENOR-, según la normativa UNECE/R155 y aplicando la Metodología ESTP.

La entrega oficial de este primer certificado de ciberseguridad en vehículos fue realizada el día 25 de abril de 2022 en la sede que NMS tiene en el Parque Empresarial de Boroa/Amorebieta -Bizkaia-.



## COMUNICADO DE PRENSA || AENOR ENTREGA A NUUK EL PRIMER CERTIFICADO DE «CIBERSEGURIDAD EN VEHÍCULOS» DEL MUNDO

25 ABRIL, 2022

La NUUK CargoPro ha recibido el primer certificado de "Ciberseguridad en Vehículos" de AENOR, tras superar el Test EUROCYBCAR -que mide y evalúa el nivel de ciberseguridad de un vehículo, según los requisitos de la normativa UNECE/R155 y aplicando la metodología ESTP-.

■ NOTAS DE PRENSA



## COMUNICADO DE PRENSA || El primer «Vehículo Ciberseguro» del mundo es una moto fabricada en España

20 DICIEMBRE, 2021

Por primera vez en la historia, un vehículo ha superado el test que avala su condición de "vehículo ciberseguro" según la normativa UNECE/R155 y según el procedimiento y metodología ESTP desarrollado por EUROCYBCAR, una empresa tecnológica con sede en Vitoria-Gasteiz.

■ NOTAS DE PRENSA

Más información:

- <https://eurocybcar.com/comunicado-de-prensa-aenor-entrega-a-nuuk-el-primer-certificado-de-ciberseguridad-en-vehiculos-del-mundo/>
- <https://eurocybcar.com/comunicado-de-prensa-el-primer-vehiculo-ciberseguro-del-mundo-es-una-moto-fabricada-en-espana/>

# ¿QUÉ OPINAN LOS EXPERTOS?

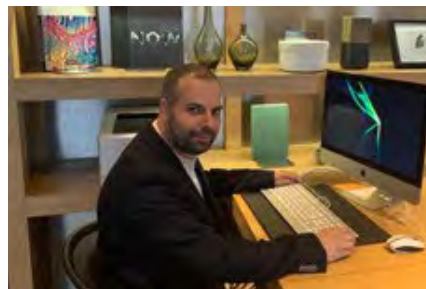


**AZUCENA HERNÁNDEZ**  
CEO DE EUROCYBCAR

Llevamos años concienciando a instituciones y empresas en España y en Europa para que la "cybersecurity by design" sea la base de la movilidad cibersegura del futuro y la ONU/UNECE "nos ha dado la razón" con esta normativa que entró en vigor el 22 de enero de 2021 y que ya obliga a los fabricantes de vehículos a incorporar la ciberseguridad desde la fase de diseño e, incluso, en sus sistemas de gestión.

La UNECE/R155 es una normativa drástica porque exige que los vehículos cuenten con un certificado de ciberseguridad que acredite que están mínimamente protegidos contra ciberataques y se llega, incluso, a cerrar el mercado europeo a los coches, autobuses, camiones y furgonetas que no cumplan con los 70 requisitos que establece dicha normativa.

La regulación es drástica, pero muy necesaria, porque los vehículos son grandes ordenadores sobre cuatro ruedas y deben protegerse, como mínimo, igual que se protege un móvil o un portátil. Las consecuencias de que no estén bien ciberprotegidos pueden ser trágicas: basta con que una persona introduzca en el puerto USB de su coche un pen drive con música que se ha descargado de internet, -sin saber que también lleva un virus o un malware que puede infectar el vehículo- para provocar que, por ejemplo, el motor del vehículo se pare.



**PABLO ESCAPA**  
INGENIERO Y MIEMBRO DE PETEC

Pablo Escapa ha participado en el grupo de trabajo español que ha contribuido al desarrollo de la normativa de UNECE/R155. Escapa afirma que estas normativas pretenden regular los mecanismos que deben equipar los vehículos para ser ciberseguros. Es decir, contar con herramientas tanto para evitar como para mitigar los ataques a los que puedan estar expuestos. La ciberseguridad 100% no existe, pero resultará más difícil ciberatacar a un coche que cumpla con toda la normativa.

Además, la norma se aplica a todos los automóviles vendidos en Europa -y otros países dentro del marco de la ONU/UNECE-. Se necesitará un certificado de conformidad en materia de ciberseguridad para poder homologar los vehículos destinados al espacio económico europeo. ¿Lo más revolucionario? El sistema de gestión de las actualizaciones online que coexiste con esta normativa.

Para los fabricantes de vehículos la adaptación a nueva norma para implementar la ciberseguridad en todos los procesos va a suponer un gran reto, tanto en costes de tiempo como económicos, porque los niveles que se requieren son muy exhaustivos -más propios de la protección de una infraestructura crítica- ya que la conducción autónoma se considera una actividad crítica.

Por suerte hay fabricantes que ya se están adelantando para adaptarse a la nueva regulación, incluso realizando el ESTP a sus modelos.

**NURIA ROMÁN // EX-JEFA DE ÁREA DE LA SUBDIRECCIÓN GENERAL DE CALIDAD Y SEGURIDAD INDUSTRIAL (MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO). ADEMÁS, LIDERÓ EL GRUPO DE TRABAJO ESPAÑOL DE LA NORMATIVA UNECE/R155**

**¿QUÉ ASPECTOS DE LA NORMA TE PARECEN LOS MÁS DESTACADOS?**

Los vehículos actuales ya se diseñan con arquitecturas electrónicas y de sistemas de información complejos que, por ejemplo, permiten abrir o arrancar el vehículo, manejan la inyección de combustible y, por tanto, los regímenes de funcionamiento del motor, monitorizan los sistemas del vehículo y ofrecen información de diagnóstico para su reparación o intervienen en casos de emergencia. Garantizar un nivel mínimo de seguridad en el acceso a estos sistemas es lo que pretende el nuevo reglamento de ciberseguridad.

Esta reglamentación permitirá evaluar la protección contra accesos no autorizados a la información y los sistemas contenidos en los vehículos, armonizando los mínimos que deben superarse en todos los fabricantes, que ya adoptaban medidas de protección, hasta ahora de forma no evaluada durante el proceso de homologación.

**UNA VEZ QUE LA NORMATIVA ENTRÓ EN VIGOR, ¿CUÁLES SON LOS SIGUIENTES PASOS QUE HUBO QUE DAR?**

El marco de homologación de vehículos en la Unión Europea establece una serie de reglamentos de Naciones Unidas o, en su caso, Reglamentos o Directivas UE, que los vehículos deben cumplir para poder ser comercializados en el mercado interior. Desde que se exige el reglamento de ciberseguridad para la homologación de tipo europea, desde 2022, dicho reglamento debe evaluarse, junto con el resto de los exigidos durante el proceso de homologación. Hasta ese momento, los fabricantes lo podían aplicar lo de forma voluntaria, pero a partir de que fue obligatorio, no podían homologarse nuevos tipos de vehículos que no lo cumplan.

**¿CÓMO ES EL PROCESO PARA EVALUAR SI UN TIPO DE VEHÍCULO POSEE UN CSMS ACORDE A ESTA NUEVA NORMATIVA?**

Se trata de un reglamento complejo, distinto a los tradicionales de homologación en el que no resulta posible identificar un ensayo a efectuar sobre el peor de los escenarios. El reglamento tiene en cuenta esta dificultad y emplea la metodología del análisis de riesgos y la especificación de amenazas y protecciones mínimas que deben contemplarse en un vehículo. Además, está en elaboración



**"Uno de los requisitos más destacados de la normativa es que obliga a considerar los aspectos de ciberseguridad desde el diseño de la arquitectura".**

una guía de aplicación que recomienda el uso de diversas metodologías de evaluación de los sistemas de gestión de la ciberseguridad y la seguridad de la información. En primera instancia es el fabricante el que debe evaluar el cumplimiento de los requisitos, documentando el análisis de riesgo, las medidas de protección, su implementación y las pruebas ejecutadas para verificar su efectividad. Posteriormente, el servicio técnico evaluará la conformidad de todas estas evidencias y por muestreo, llevará a cabo otras pruebas. En cualquier caso, deberá seguir las recomendaciones de la guía de aplicación, que aún está en elaboración.

**¿POR QUÉ JAPÓN Y COREA QUISIERON ADELANTARSE A LA FECHA DE IMPOSICIÓN DE LA NORMA? ¿TENÍAN ESTOS PAÍSES MÁS DESARROLLADOS SUS PROTOCOLOS DE EVALUACIÓN?**

Se trata de dos países muy avanzados en tecnología electrónica y automática. No conocíamos el estado de sus protocolos de evaluación, aunque la guía de aplicación desarrollada en el grupo de Naciones Unidas ya ofrecía la posibilidad de aplicar varias metodologías de evaluación estandarizadas. En cualquier caso, la fecha de aplicación en la UE también estaba muy próxima, en 2022. Dado que el acuerdo de 1958 sobre armonización técnica exige el reconocimiento mutuo de las homologaciones concedidas entre las partes firmantes, lo ideal es recurrir a la guía de aplicación que sea finalmente acordada en ese foro.



¿ESTÁN LOS FABRICANTES PREPARADOS PARA APLICAR LA NORMATIVA? ¿QUÉ ESFUERZOS LES HA SUPUESTO? ¿CUÁL ES EL MAYOR CAMBIO QUE HA DEBIDO REALIZAR UN FABRICANTE PARA CUMPLIR CON LOS REQUISITOS?

Evidentemente la entrada en vigor de un nuevo reglamento exige adaptaciones a la industria. No obstante, la tecnología suele ir por delante de la reglamentación, y en este caso, la industria no parte de cero para adaptarse a la normativa. Los fabricantes ya tenían en cuenta la protección de los sistemas de información presentes en el vehículo, lo que cambia ahora es que deben adaptarse a los requisitos del reglamento y evaluarse durante el proceso de homologación del vehículo.

LA NORMATIVA TAMBIÉN INDICA QUE SE VERÁN AFECTADOS TODOS LOS DEPARTAMENTOS INVOLUCRADOS EN LA PRODUCCIÓN DE UN TIPO DE VEHÍCULO, ¿CÓMO AFECTA ESTO A TALLERES Y PROVEEDORES?

El proceso de fabricación de los vehículos incorpora componentes y sistemas de una multiplicidad de proveedores. El reglamento obliga a definir la arquitectura de los vehículos teniendo en cuenta la ciberseguridad, por lo que la integración de los componentes estará prevista desde un punto de vista “ciberseguro”. Pero, además, es indudable que el reglamento afecta también a los proveedores de sistemas y componentes, y así el fabricante del vehículo debe evaluar los riesgos asociados al vehículo final, incorporando esos componentes, lo que impone tener en cuenta la ciberseguridad en toda la cadena de suministro.

¿POR QUÉ ESTA NORMATIVA NO AFECTA A OTROS TRANSPORTES, COMO BARCOS O TRENES? ¿SALDRÁ PRONTO ALGUNA NORMATIVA AL RESPECTO?

El acuerdo de Ginebra de 1958 sobre armonización técnica que sirve de marco al reglamento de ciberseguridad afecta solo a los vehículos de ruedas. En el caso de las motocicletas, aunque en principio no consideró incluirlas en la primera versión del reglamento debido a su menor grado de avance hacia la conducción automatizada, al final ya están contempladas. Con el resto de transportes podría suceder lo mismo.



# QUÉ SABER SOBRE EUROCYBCAR®

**EUROCYBCAR SL**, es una empresa de base tecnológica, con sede en Vitoria-Gasteiz, que desarrolla productos y servicios innovadores de ciberseguridad para el sector de la automoción/movilidad que protejan la vida y los datos de las personas y de los vehículos.

**EUROCYBCAR** es pionera a nivel global al aunar la ciberseguridad, la automoción y la movilidad en su core business, desarrollando en base a ello todo un portafolio de productos y servicios con el objetivo de conseguir una protección integral de la movilidad en el ámbito de la ciberseguridad.

**EUROCYBCAR** posee un demostrado expertise -más de 35 años de experiencia- en Investigación, Automoción, Movilidad y Ciberseguridad, estando el core del equipo formado por hackers, investigadores, ITs, expertos en Seguridad, probadores de coches y expertos en legislación.

**EUROCYBCAR** ha creado la primera evaluación técnica de ciberseguridad en el mundo que cumple con los requisitos de la nueva normativa de seguridad de UNE-CE/ R155, que mide y certifica el nivel de ciberseguridad de un coche, basándose en dos parámetros: de qué forma protege la privacidad del conductor y de los pasajeros -SUS DATOS- y, lo que es más importante, SU VIDA. El protocolo de la evaluación técnica de ciberseguridad -con patente internacional- se realiza en su laboratorio de Vitoria-Gasteiz.

Además, **EUROCYBCAR** dispone de un amplio portafolio de productos y servicios -siempre relacionados con la ciberseguridad y la movilidad-, con el objetivo de conseguir una ciberprotección integral de la movilidad: el Test Integral de Ciberseguridad para Sistemas de Gestión de Flotas, el Test V2D -test a las conexiones entre el coche y los dispositivos que el usuario conecta al vehículo-, el Test para Aplicaciones de Movilidad, el Test para neumáticos inteligentes o el Test para locomotoras/trenes son ejemplos de la preocupación de EUROCYBCAR por una movilidad más cibersegura.

## MÁS INFORMACIÓN:

[WWW.EUROCYBCAR.COM](http://WWW.EUROCYBCAR.COM)

**PARQUE TECNOLÓGICO DE ÁLAVA EDIFICIO BIC**

**ALBERT EINSTEIN KALEA, 15 - 01510**

**VITORIA-GASTEIZ, ÁLAVA**

**+34 619 291 892**

**[INFO@EUROCYBCAR.COM](mailto:INFO@EUROCYBCAR.COM)**





# **UNECE R/155**

**Uniform provisions  
concerning the approval of  
vehicles with regards to  
cyber security and cyber  
security management  
system**

4 March 2021

---

## **Agreement**

### **Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations\***

(Revision 3, including the amendments which entered into force on 14 September 2017)

---

#### **Addendum 154 – UN Regulation No. 155**

Date of entry into force as an annex to the 1958 Agreement: 22 January 2021

#### **Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system**

This document is meant purely as documentation tool. The authentic and legal binding text is: ECE/TRANS/WP.29/2020/79 (as amended by ECE/TRANS/WP.29/2020/94 and ECE/TRANS/WP.29/2020/97).



**UNITED NATIONS**

---

\* Former titles of the Agreement:

Agreement concerning the Adoption of Uniform Conditions of Approval and Reciprocal Recognition of Approval for Motor Vehicle Equipment and Parts, done at Geneva on 20 March 1958 (original version);  
Agreement concerning the Adoption of Uniform Technical Prescriptions for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these Prescriptions, done at Geneva on 5 October 1995 (Revision 2).



## UN Regulation No. 155

### Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

#### Contents

|                                                                                                                                | <i>Page</i> |
|--------------------------------------------------------------------------------------------------------------------------------|-------------|
| 1. Scope .....                                                                                                                 | 4           |
| 2. Definitions.....                                                                                                            | 4           |
| 3. Application for approval .....                                                                                              | 5           |
| 4. Markings .....                                                                                                              | 5           |
| 5. Approval .....                                                                                                              | 6           |
| 6. Certificate of Compliance for Cyber Security Management System .....                                                        | 8           |
| 7. Specifications .....                                                                                                        | 9           |
| 8. Modification and extension of the vehicle type .....                                                                        | 12          |
| 9. Conformity of production .....                                                                                              | 12          |
| 10. Penalties for non-conformity of production .....                                                                           | 12          |
| 11. Production definitively discontinued.....                                                                                  | 12          |
| 12. Names and addresses of Technical Services responsible for conducting approval test, and of Type Approval Authorities ..... | 13          |

#### Annexes

|                                                       |    |
|-------------------------------------------------------|----|
| 1 Information document .....                          | 14 |
| 2 Communication .....                                 | 16 |
| 3 Arrangement of approval mark .....                  | 17 |
| 4 Model of Certificate of Compliance for CSMS.....    | 18 |
| 5 List of threats and corresponding mitigations ..... | 19 |

## 1. Scope

- 1.1. This Regulation applies to vehicles, with regard to cyber security, of the Categories M and N.  
  
This Regulation also applies to vehicles of Category O if fitted with at least one electronic control unit.
- 1.2. This Regulation also applies to vehicles of the Categories L<sub>6</sub> and L<sub>7</sub> if equipped with automated driving functionalities from level 3 onwards, as defined in the reference document with definitions of Automated Driving under WP.29 and the General Principles for developing a UN Regulation on automated vehicles (ECE/TRANS/WP.29/1140).
- 1.3. This Regulation is without prejudice to other UN Regulations, regional or national legislations governing the access by authorized parties to the vehicle, its data, functions and resources, and conditions of such access. It is also without prejudice to the application of national and regional legislation on privacy and the protection of natural persons with regard to the processing of their personal data.
- 1.4. This Regulation is without prejudice to other UN Regulations, national or regional legislation governing the development and installation/system integration of replacement parts and components, physical and digital, with regards to cybersecurity.

## 2. Definitions

For the purpose of this Regulation the following definitions shall apply:

- 2.1. "*Vehicle type*" means vehicles which do not differ in at least the following essential respects:
  - (a) The manufacturer's designation of the vehicle type;
  - (b) Essential aspects of the electric/electronic architecture and external interfaces with respect to cyber security.
- 2.2. "*Cyber security*" means the condition in which road vehicles and their functions are protected from cyber threats to electrical or electronic components.
- 2.3. "*Cyber Security Management System (CSMS)*" means a systematic risk-based approach defining organisational processes, responsibilities and governance to treat risk associated with cyber threats to vehicles and protect them from cyber-attacks.
- 2.4. "*System*" means a set of components and/or sub-systems that implements a function or functions.
- 2.5. "*Development phase*" means the period before a vehicle type is type approved.
- 2.6. "*Production phase*" refers to the duration of production of a vehicle type.
- 2.7. "*Post-production phase*" refers to the period in which a vehicle type is no longer produced until the end-of-life of all vehicles under the vehicle type. Vehicles incorporating a specific vehicle type will be operational during this phase but will no longer be produced. The phase ends when there are no longer any operational vehicles of a specific vehicle type.
- 2.8. "*Mitigation*" means a measure that is reducing risk.
- 2.9. "*Risk*" means the potential that a given threat will exploit vulnerabilities of a vehicle and thereby cause harm to the organization or to an individual.
- 2.10. "*Risk Assessment*" means the overall process of finding, recognizing and describing risks (risk identification), to comprehend the nature of risk and to

determine the level of risk (risk analysis), and of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable (risk evaluation).

- 2.11. "*Risk Management*" means coordinated activities to direct and control an organization with regard to risk.
- 2.12. "*Threat*" means a potential cause of an unwanted incident, which may result in harm to a system, organization or individual.
- 2.13. "*Vulnerability*" means a weakness of an asset or mitigation that can be exploited by one or more threats.

### **3. Application for approval**

- 3.1. The application for approval of a vehicle type with regard to cyber security shall be submitted by the vehicle manufacturer or by their duly accredited representative.
- 3.2. It shall be accompanied by the undermentioned documents in triplicate, and by the following particulars:
  - 3.2.1. A description of the vehicle type with regard to the items specified in Annex 1 to this Regulation.
  - 3.2.2. In cases where information is shown to be covered by intellectual property rights or to constitute specific know-how of the manufacturer or of their suppliers, the manufacturer or their suppliers shall make available sufficient information to enable the checks referred to in this Regulation to be made properly. Such information shall be treated on a confidential basis.
  - 3.2.3. The Certificate of Compliance for CSMS according to paragraph 6 of this Regulation.
- 3.3. Documentation shall be made available in two parts:
  - (a) The formal documentation package for the approval, containing the material specified in Annex 1 which shall be supplied to the Approval Authority or its Technical Service at the time of submission of the type approval application. This documentation package shall be used by the Approval Authority or its Technical Service as the basic reference for the approval process. The Approval Authority or its Technical Service shall ensure that this documentation package remains available for at least 10 years counted from the time when production of the vehicle type is definitively discontinued.
  - (b) Additional material relevant to the requirements of this regulation may be retained by the manufacturer, but made open for inspection at the time of type approval. The manufacturer shall ensure that any material made open for inspection at the time of type approval remains available for at least a period of 10 years counted from the time when production of the vehicle type is definitively discontinued.

### **4. Marking**

- 4.1. There shall be affixed, conspicuously and in a readily accessible place specified on the approval form, to every vehicle conforming to a vehicle type approved under this Regulation an international approval mark consisting of:
  - 4.1.1. A circle surrounding the Letter "E" followed by the distinguishing number of the country which has granted approval.
  - 4.1.2. The number of this Regulation, followed by the letter "R", a dash and the approval number to the right of the circle described in paragraph 4.1.1. above.



- 4.2. If the vehicle conforms to a vehicle type approved under one or more other Regulations annexed to the Agreement in the country which has granted approval under this Regulation, the symbol prescribed in paragraph 4.1.1. above need not be repeated; in this case the Regulation and approval numbers and the additional symbols of all the Regulations under which approval has been granted in the country which has granted approval under this Regulation shall be placed in vertical columns to the right of the symbol prescribed in paragraph 4.1.1. above.
- 4.3. The approval mark shall be clearly legible and shall be indelible.
- 4.4. The approval mark shall be placed on or close to the vehicle data plate affixed by the Manufacturer.
- 4.5. Annex 3 to this Regulation gives examples of the arrangements of the approval mark.

## **5. Approval**

- 5.1. Approval Authorities shall grant, as appropriate, type approval with regard to cyber security, only to such vehicle types that satisfy the requirements of this Regulation.
- 5.1.1. The Approval Authority or the Technical Service shall verify by means of document checks that the vehicle manufacturer has taken the necessary measures relevant for the vehicle type to:
  - (a) Collect and verify the information required under this Regulation through the supply chain so as to demonstrate that supplier-related risks are identified and are managed;
  - (b) Document risks assessment (conducted during development phase or retrospectively), test results and mitigations applied to the vehicle type, including design information supporting the risk assessment;
  - (c) Implement appropriate cyber security measures in the design of the vehicle type;
  - (d) Detect and respond to possible cyber security attacks;
  - (e) Log data to support the detection of cyber-attacks and provide data forensic capability to enable analysis of attempted or successful cyber-attacks.
- 5.1.2. The Approval Authority or the Technical Service shall verify by testing of a vehicle of the vehicle type that the vehicle manufacturer has implemented the cyber security measures they have documented. Tests shall be performed by the Approval Authority or the Technical Service itself or in collaboration with the vehicle manufacturer by sampling. Sampling shall be focused but not limited to risks that are assessed as high during the risk assessment.
- 5.1.3. The Approval Authority or Technical Service shall refuse to grant the type approval with regard to cyber security where the vehicle manufacturer has not fulfilled one or more of the requirements referred to in paragraph 7.3., notably:
  - (a) The vehicle manufacturer did not perform the exhaustive risk assessment referred to in paragraph 7.3.3.; including where the manufacturer did not consider all the risks related to threats referred to in Annex 5, Part A;
  - (b) The vehicle manufacturer did not protect the vehicle type against risks identified in the vehicle manufacturer's risk assessment or proportionate mitigations were not implemented as required by paragraph 7.;

- (c) The vehicle manufacturer did not put in place appropriate and proportionate measures to secure dedicated environments on the vehicle type (if provided) for the storage and execution of aftermarket software, services, applications or data;
  - (d) The vehicle manufacturer did not perform, prior to the approval, appropriate and sufficient testing to verify the effectiveness of the security measures implemented.
- 5.1.4 The assessing Approval Authority shall also refuse to grant the type approval with regard to cyber security where the Approval Authority or Technical Service has not received sufficient information from the vehicle manufacturer to assess the cyber security of the vehicle type.
- 5.2. Notice of approval or of extension or refusal of approval of a vehicle type pursuant to this Regulation shall be communicated to the Parties to the 1958 Agreement which apply this Regulation, by means of a form conforming to the model in Annex 2 to this Regulation.
- 5.3. Approval Authorities shall not grant any type approval without verifying that the manufacturer has put in place satisfactory arrangements and procedures to manage properly the cyber security aspects as covered by this Regulation.
- 5.3.1. The Approval Authority and its Technical Services shall ensure, in addition to the criteria laid down in Schedule 2 of the 1958 Agreement that they have:
  - (a) Competent personnel with appropriate cyber security skills and specific automotive risk assessments knowledge;<sup>1</sup>
  - (b) Implemented procedures for the uniform evaluation according to this Regulation.
- 5.3.2. Each Contracting Party applying this Regulation shall notify and inform by its Approval Authority other Approval Authorities of the Contracting Parties applying this UN Regulation about the method and criteria taken as a basis by the notifying Authority to assess the appropriateness of the measures taken in accordance with this regulation and in particular with paragraphs 5.1., 7.2. and 7.3.  
  
 This information shall be shared (a) only before granting an approval according to this Regulation for the first time and (b) each time the method or criteria for assessment is updated.  
  
 This information is intended to be shared for the purposes of collection and analysis of the best practices and in view of ensuring the convergent application of this Regulation by all Approval Authorities applying this Regulation.
- 5.3.3. The information referred to in paragraph 5.3.2 shall be uploaded in English language to the secure internet database "DETA",<sup>2</sup> established by the United Nations Economic Commission for Europe, in due time and no later than 14 days before an approval is granted for the first time under the methods and criteria of assessment concerned. The information shall be sufficient to understand what minimum performance levels the Approval Authority adopted for each specific requirement referred to in paragraph 5.3.2 as well as the processes and measures it applies to verify that these minimum performance levels are met.<sup>3</sup>

<sup>1</sup> E.g. ISO 26262-2018, ISO/PAS 21448, ISO/SAE 21434

<sup>2</sup> <https://www.unece.org/trans/main/wp29/datasharing.html>

<sup>3</sup> Guidance for the detailed information (e.g. method, criteria, performance level) to be uploaded and the format shall be given in the interpretation document which is under preparation by the Task Force on Cyber Security and Over-the-Air issues for the seventh session of GRVA.

- 5.3.4. Approval Authorities receiving the information referred to in paragraph 5.3.2 may submit comments to the notifying Approval Authority by uploading them to DETA within 14 days after the day of notification.
- 5.3.5. If it is not possible for the granting Approval Authority to take into account the comments received in accordance with paragraph 5.3.4., the Approval Authorities having sent comments and the granting Approval Authority shall seek further clarification in accordance with Schedule 6 to the 1958 Agreement. The relevant subsidiary Working Party<sup>4</sup> of the World Forum for Harmonization of Vehicle Regulations (WP.29) for this Regulation shall agree on a common interpretation of methods and criteria of assessment.<sup>5</sup> That common interpretation shall be implemented and all Approval Authorities shall issue type approvals under this Regulation accordingly.
- 5.3.6. Each Approval Authority granting a type approval pursuant to this Regulation shall notify other Approval Authorities of the approval granted. The type approval together with the supplementing documentation shall be uploaded in English language by the Approval Authority within 14 days after the day of granting the approval to DETA.<sup>6</sup>
- 5.3.7. The Contracting Parties may study the approvals granted based on the information uploaded according to paragraph 5.3.6. In case of any diverging views between Contracting Parties this shall be settled in accordance with Article 10 and Schedule 6 of the 1958 Agreement. The Contracting Parties shall also inform the relevant subsidiary Working Party of the World Forum for Harmonization of Vehicle Regulations (WP.29) of the diverging interpretations within the meaning of Schedule 6 to the 1958 Agreement. The relevant Working Party shall support the settlement of the diverging views and may consult with WP.29 on this if needed.
- 5.4. For the purpose of paragraph 7.2. of this Regulation, the manufacturer shall ensure that the cyber security aspects covered by this Regulation are implemented.

## **6. Certificate of Compliance for Cyber Security Management System**

- 6.1. Contracting Parties shall appoint an Approval Authority to carry out the assessment of the manufacturer and to issue a Certificate of Compliance for CSMS.
- 6.2. An application for a Certificate of Compliance for Cyber Security Management System shall be submitted by the vehicle manufacturer or by their duly accredited representative.
- 6.3. It shall be accompanied by the undermentioned documents in triplicate, and by the following particular:
- 6.3.1. Documents describing the Cyber Security Management System.
- 6.3.2. A signed declaration using the model as defined in Appendix 1 to Annex 1.
- 6.4. In the context of the assessment, the manufacturer shall declare using the model as defined in Appendix 1 to Annex 1 and demonstrate to the satisfaction of the Approval Authority or its Technical Service that they have the necessary processes to comply with all the requirements for cyber security according to this Regulation.

---

<sup>4</sup> The Working Party on Automated/Autonomous and Connected Vehicles (GRVA)

<sup>5</sup> This interpretation shall be reflected in the interpretation document referred to in the footnote to paragraph 5.3.3.

<sup>6</sup> Further information on the minimum requirements for the documentation package will be developed by GRVA during its seven session.

- 6.5. When this assessment has been satisfactorily completed and in receipt of a signed declaration from the manufacturer according to the model as defined in Appendix 1 to Annex 1, a certificate named Certificate of Compliance for CSMS as described in Annex 4 to this Regulation (hereinafter the Certificate of Compliance for CSMS) shall be granted to the manufacturer.
- 6.6. The Approval Authority or its Technical Service shall use the model set out in Annex 4 to this Regulation for the Certificate of Compliance for CSMS.
- 6.7. The Certificate of Compliance for CSMS shall remain valid for a maximum of three years from the date of deliverance of the certificate unless it is withdrawn.
- 6.8. The Approval Authority which has granted the Certificate of Compliance for CSMS may at any time verify that the requirements for it continue to be met. The Approval Authority shall withdraw the Certificate of Compliance for CSMS if the requirements laid down in this Regulation are no longer met.
- 6.9. The manufacturer shall inform the Approval Authority or its Technical Service of any change that will affect the relevance of the Certificate of Compliance for CSMS. After consultation with the manufacturer, the Approval Authority or its Technical Service shall decide whether new checks are necessary.
- 6.10. In due time, permitting the Approval Authority to complete its assessment before the end of the period of validity of the Certificate of Compliance for CSMS, the manufacturer shall apply for a new or for the extension of the existing Certificate of Compliance for CSMS. The Approval Authority shall, subject to a positive assessment, issue a new Certificate of Compliance for CSMS or extend its validity for a further period of three years. The Approval Authority shall verify that the CSMS continue to comply with the requirements of this Regulation. The Approval Authority shall issue a new certificate in cases where changes have been brought to the attention of the Approval Authority or its Technical Service and the changes have been positively re-assessed.
- 6.11. The expiry or withdrawal of the manufacturer's Certificate of Compliance for CSMS shall be considered, with regard to the vehicle types to which the CSMS concerned was relevant, as modification of approval, as referred to in paragraph 8, which may include the withdrawal of the approval if the conditions for granting the approval are not met anymore.

## **7. Specifications**

- 7.1. General specifications
  - 7.1.1. The requirements of this Regulation shall not restrict provisions or requirements of other UN Regulations.
- 7.2. Requirements for the Cyber Security Management System
  - 7.2.1. For the assessment the Approval Authority or its Technical Service shall verify that the vehicle manufacturer has a Cyber Security Management System in place and shall verify its compliance with this Regulation.
  - 7.2.2. The Cyber Security Management System shall cover the following aspects:
    - 7.2.2.1. The vehicle manufacturer shall demonstrate to an Approval Authority or Technical Service that their Cyber Security Management System applies to the following phases:
      - (a) Development phase;
      - (b) Production phase;
      - (c) Post-production phase.

- 7.2.2.2. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System ensure security is adequately considered, including risks and mitigations listed in Annex 5. This shall include:
- (a) The processes used within the manufacturer's organization to manage cyber security;
  - (b) The processes used for the identification of risks to vehicle types. Within these processes, the threats in Annex 5, Part A, and other relevant threats shall be considered;
  - (c) The processes used for the assessment, categorization and treatment of the risks identified;
  - (d) The processes in place to verify that the risks identified are appropriately managed;
  - (e) The processes used for testing the cyber security of a vehicle type;
  - (f) The processes used for ensuring that the risk assessment is kept current;
  - (g) The processes used to monitor for, detect and respond to cyber-attacks, cyber threats and vulnerabilities on vehicle types and the processes used to assess whether the cyber security measures implemented are still effective in the light of new cyber threats and vulnerabilities that have been identified.
  - (h) The processes used to provide relevant data to support analysis of attempted or successful cyber-attacks.
- 7.2.2.3. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that, based on categorization referred to in paragraph 7.2.2.2 (c) and 7.2.2.2 (g), cyber threats and vulnerabilities which require a response from the vehicle manufacturer shall be mitigated within a reasonable timeframe.
- 7.2.2.4. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that the monitoring referred to in paragraph 7.2.2.2 (g) shall be continual. This shall:
- (a) Include vehicles after first registration in the monitoring;
  - (b) Include the capability to analyse and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs. This capability shall respect paragraph 1.3. and the privacy rights of car owners or drivers, particularly with respect to consent.
- 7.2.2.5. The vehicle manufacturer shall be required to demonstrate how their Cyber Security Management System will manage dependencies that may exist with contracted suppliers, service providers or manufacturer's sub-organizations in regards of the requirements of paragraph 7.2.2.2.
- 7.3. Requirements for vehicle types
- 7.3.1. The manufacturer shall have a valid Certificate of Compliance for the Cyber Security Management System relevant to the vehicle type being approved.
- However, for type approvals prior to 1 July 2024, if the vehicle manufacturer can demonstrate that the vehicle type could not be developed in compliance with the CSMS, then the vehicle manufacturer shall demonstrate that cyber security was adequately considered during the development phase of the vehicle type concerned.
- 7.3.2. The vehicle manufacturer shall identify and manage, for the vehicle type being approved, supplier-related risks.



- 7.3.3. The vehicle manufacturer shall identify the critical elements of the vehicle type and perform an exhaustive risk assessment for the vehicle type and shall treat/manage the identified risks appropriately. The risk assessment shall consider the individual elements of the vehicle type and their interactions. The risk assessment shall further consider interactions with any external systems. While assessing the risks, the vehicle manufacturer shall consider the risks related to all the threats referred to in Annex 5, Part A, as well as any other relevant risk.
- 7.3.4. The vehicle manufacturer shall protect the vehicle type against risks identified in the vehicle manufacturer's risk assessment. Proportionate mitigations shall be implemented to protect the vehicle type. The mitigations implemented shall include all mitigations referred to in Annex 5, Part B and C which are relevant for the risks identified. However, if a mitigation referred to in Annex 5, Part B or C, is not relevant or not sufficient for the risk identified, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented.
- In particular, for type approvals prior to 1 July 2024, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented if a mitigation measure referred to in Annex 5, Part B or C is technically not feasible. The respective assessment of the technical feasibility shall be provided by the manufacturer to the approval authority.
- 7.3.5. The vehicle manufacturer shall put in place appropriate and proportionate measures to secure dedicated environments on the vehicle type (if provided) for the storage and execution of aftermarket software, services, applications or data.
- 7.3.6. The vehicle manufacturer shall perform, prior to type approval, appropriate and sufficient testing to verify the effectiveness of the security measures implemented.
- 7.3.7. The vehicle manufacturer shall implement measures for the vehicle type to:
- (a) Detect and prevent cyber-attacks against vehicles of the vehicle type;
  - (b) Support the monitoring capability of the vehicle manufacturer with regards to detecting threats, vulnerabilities and cyber-attacks relevant to the vehicle type;
  - (c) Provide data forensic capability to enable analysis of attempted or successful cyber-attacks.
- 7.3.8. Cryptographic modules used for the purpose of this Regulation shall be in line with consensus standards. If the cryptographic modules used are not in line with consensus standards, then the vehicle manufacturer shall justify their use.
- 7.4. Reporting provisions
- 7.4.1. The vehicle manufacturer shall report at least once a year, or more frequently if relevant, to the Approval Authority or the Technical Service the outcome of their monitoring activities, as defined in paragraph 7.2.2.2.(g)), this shall include relevant information on new cyber-attacks. The vehicle manufacturer shall also report and confirm to the Approval Authority or the Technical Service that the cyber security mitigations implemented for their vehicle types are still effective and any additional actions taken.
- 7.4.2. The Approval Authority or the Technical Service shall verify the provided information and, if necessary, require the vehicle manufacturer to remedy any detected ineffectiveness.
- If the reporting or response is not sufficient the Approval Authority may decide to withdraw the CSMS in compliance with paragraph 6.8.

## **8. Modification and extension of the vehicle type**

- 8.1. Every modification of the vehicle type which affects its technical performance with respect to cybersecurity and/or documentation required in this Regulation shall be notified to the approval authority which approved the vehicle type. The Approval Authority may then either:
  - 8.1.1. Consider that the modifications made still comply with the requirements and documentation of existing type approval; or
  - 8.1.2. Proceed to necessary complementary assessment pursuant to paragraph 5, and require, where relevant, a further test report from the Technical Service responsible for conducting the tests.
  - 8.1.3. Confirmation or extension or refusal of approval, specifying the alterations, shall be communicated by means of a communication form conforming to the model in Annex 2 to this Regulation. The Approval Authority issuing the extension of approval shall assign a series number for such an extension and inform there of the other Parties to the 1958 Agreement applying this Regulation by means of a communication form conforming to the model in Annex 2 to this Regulation.

## **9. Conformity of production**

- 9.1. The Conformity of Production Procedures shall comply with those set out in the 1958 Agreement, Schedule 1 (E/ECE/TRANS/505/Rev.3) with the following requirements:
  - 9.1.1. The holder of the approval shall ensure that results of the conformity of production tests are recorded and that the annexed documents remain available for a period determined in agreement with the Approval Authority or its Technical Service. This period shall not exceed 10 years counted from the time when production is definitively discontinued;
  - 9.1.2. The Approval Authority which has granted type approval may at any time verify the conformity control methods applied in each production facility. The normal frequency of these verifications shall be once every three years.

## **10. Penalties for non-conformity of production**

- 10.1. The approval granted in respect of a vehicle type pursuant to this Regulation may be withdrawn if the requirements laid down in this Regulation are not complied with or if sample vehicles fail to comply with the requirements of this Regulation.
- 10.2. If an Approval Authority withdraws an approval it has previously granted, it shall forthwith so notify the Contracting Parties applying this Regulation, by means of a communication form conforming to the model in Annex 2 to this Regulation.

## **11. Production definitively discontinued**

- 11.1. If the holder of the approval completely ceases to manufacture a type of vehicle approved in accordance with this Regulation, he shall so inform the authority which granted the approval. Upon receiving the relevant communication that authority shall inform thereof the other Contracting Parties to the Agreement applying this Regulation by means of a copy of the approval form bearing at the end, in large letters, the signed and dated annotation "PRODUCTION DISCONTINUED".

**12. Names and addresses of Technical Services responsible for conducting approval test, and of Type Approval Authorities**

- 12.1. The Contracting Parties to the Agreement which apply this Regulation shall communicate to the United Nations Secretariat the names and addresses of the Technical Services responsible for conducting approval tests and of the Type Approval Authorities which grant approval and to which forms certifying approval or extension or refusal or withdrawal of approval, issued in other countries, are to be sent.

## Annex 1

### Information document

The following information, if applicable, shall be supplied in triplicate and include a list of contents. Any drawings shall be supplied in appropriate scale and in sufficient detail on size A4 or on a folder of A4 format. Photographs, if any, shall show sufficient detail.

1. Make (trade name of manufacturer): .....
2. Type and general commercial description(s): .....
3. Means of identification of type, if marked on the vehicle: .....
4. Location of that marking: .....
5. Category(ies) of vehicle: .....
6. Name and address of manufacturer/ manufacturer's representative: .....
7. Name(s) and Address(es) of assembly plant(s): .....
8. Photograph(s) and/or drawing(s) of a representative vehicle: .....
9. Cyber Security
  - 9.1. General construction characteristics of the vehicle type, including:
    - (a) The vehicle systems which are relevant to the cyber security of the vehicle type;
    - (b) The components of those systems that are relevant to cyber security;
    - (c) The interactions of those systems with other systems within the vehicle type and external interfaces.
  - 9.2. Schematic representation of the vehicle type
  - 9.3. The number of the Certificate of Compliance for CSMS: .....
  - 9.4. Documents for the vehicle type to be approved describing the outcome of its risk assessment and the identified risks: .....
  - 9.5. Documents for the vehicle type to be approved describing the mitigations that have been implemented on the systems listed, or to the vehicle type, and how they address the stated risks: .....
  - 9.6. Documents for the vehicle type to be approved describing protection of dedicated environments for aftermarket software, services, applications or data: .....
  - 9.7. Documents for the vehicle type to be approved describing what tests have been used to verify the cyber security of the vehicle type and its systems and the outcome of those tests: .....
  - 9.8. Description of the consideration of the supply chain with respect to cyber security: ...

## Annex 1 - Appendix 1

### Model of Manufacturer's Declaration of Compliance for CSMS

#### Manufacturer's declaration of compliance with the requirements for the Cyber Security Management System

Manufacturer Name: .....

Manufacturer Address: .....

.....(*Manufacturer Name*) attests that the necessary processes to comply with  
the requirements for the Cyber Security Management System laid down in  
paragraph 7.2 of UN Regulation 155 are installed and will be maintained.

Done at: ..... (*place*)

Date: .....

Name of the signatory: .....

Function of the signatory: .....

.....

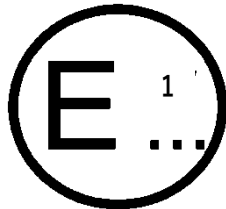
(*Stamp and signature of the manufacturer's representative*)

## Annex 2

### Communication

(Maximum format: A4 (210 x 297 mm))

issued by: Name of administration:



.....  
.....  
.....

Concerning:<sup>8</sup>

Approval granted  
Approval extended  
Approval withdrawn with effect from dd/mm/yyyy  
Approval refused  
Production definitively discontinued

of a vehicle type, pursuant to UN Regulation No. 155

Approval No.: .....

Extension No.: .....

Reason for extension: .....

1. Make (trade name of manufacturer): .....
2. Type and general commercial description(s) .....
3. Means of identification of type, if marked on the vehicle: .....
- 3.1. Location of that marking: .....
4. Category(ies) of vehicle: .....
5. Name and address of manufacturer / manufacturer's representative: .....
6. Name(s) and Address(es) of the production plant(s) .....
7. Number of the certificate of compliance for cyber security management system: .....
8. Technical Service responsible for carrying out the tests: .....
9. Date of test report: .....
10. Number of test report: .....
11. Remarks: (if any). .....
12. Place: .....
13. Date: .....
14. Signature: .....
15. The index to the information package lodged with the Approval Authority, which may be obtained on request is attached:

<sup>7</sup> Distinguishing number of the country which has granted/extended/refused/withdrawn approval (see approval provisions in the Regulation).

<sup>8</sup> Strike out what does not apply.

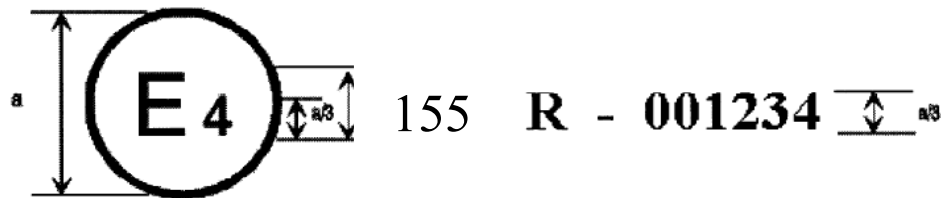


## Annex 3

### Arrangement of approval mark

#### Model A

(See paragraph 4.2 of this Regulation)



$a = 8 \text{ mm min.}$

The above approval mark affixed to a vehicle shows that the road vehicle type concerned has been approved in the Netherlands (E 4), pursuant to Regulation No. 155, and under the approval number 001234. The first two digits of the approval number indicate that the approval was granted in accordance with the requirements of this Regulation in its original form (00).

## Annex 4

### Model of Certificate of Compliance for CSMS

#### **Certificate of compliance for cyber security management system**

With UN Regulation No. [*This Regulation*]

Certificate Number [*Reference number*]

[..... *Approval Authority*]

Certifies that

Manufacturer: .....

Address of the manufacturer: .....

complies with the provisions of paragraph 7.2 of Regulation No. 155

Checks have been performed on:.....

by (name and address of the Approval Authority or Technical Service): .....

Number of report: .....

The certificate is valid until [.....*Date*]

Done at [.....*Place*]

On [.....*Date*]

[.....*Signature*]

Attachments: description of the Cyber Security Management System by the manufacturer.

## Annex 5

### List of threats and corresponding mitigations

1. This annex consists of three parts. Part A of this annex describes the baseline for threats, vulnerabilities and attack methods. Part B of this annex describes mitigations to the threats which are intended for vehicle types. Part C describes mitigations to the threats which are intended for areas outside of vehicles, e.g. on IT backends.
2. Part A, Part B, and Part C shall be considered for risk assessment and mitigations to be implemented by vehicle manufacturers.
3. The high-level vulnerability and its corresponding examples have been indexed in Part A. The same indexing has been referenced in the tables in Parts B and C to link each of the attack/vulnerability with a list of corresponding mitigation measures.
4. The threat analysis shall also consider possible attack impacts. These may help ascertain the severity of a risk and identify additional risks. Possible attack impacts may include:
  - (a) Safe operation of vehicle affected;
  - (b) Vehicle functions stop working;
  - (c) Software modified, performance altered;
  - (d) Software altered but no operational effects;
  - (e) Data integrity breach;
  - (f) Data confidentiality breach;
  - (g) Loss of data availability;
  - (h) Other, including criminality.

### Part A. Vulnerability or attack method related to the threats

1. High level descriptions of threats and relating vulnerability or attack method are listed in Table A1.

Table A1  
**List of vulnerability or attack method related to the threats**

| <i>High level and sub-level descriptions of vulnerability/ threat</i>     |   |                                                                                                                          | <i>Example of vulnerability or attack method</i> |                                                                                                                                                             |
|---------------------------------------------------------------------------|---|--------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.3.1 Threats regarding back-end servers related to vehicles in the field | 1 | Back-end servers used as a means to attack a vehicle or extract data                                                     | 1.1                                              | Abuse of privileges by staff ( <b>insider attack</b> )                                                                                                      |
|                                                                           |   |                                                                                                                          | 1.2                                              | <b>Unauthorized internet access</b> to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means) |
|                                                                           |   |                                                                                                                          | 1.3                                              | <b>Unauthorized physical access</b> to the server (conducted by for example USB sticks or other media connecting to the server)                             |
|                                                                           | 2 | Services from back-end server being disrupted, affecting the operation of a vehicle                                      | 2.1                                              | <b>Attack on back-end server stops it functioning</b> , for example it prevents it from interacting with vehicles and providing services they rely on       |
|                                                                           | 3 | Vehicle related data held on back-end servers being lost or compromised ("data breach")                                  | 3.1                                              | Abuse of privileges by staff ( <b>insider attack</b> )                                                                                                      |
|                                                                           |   |                                                                                                                          | 3.2                                              | <b>Loss of information in the cloud</b> . Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers |
|                                                                           |   |                                                                                                                          | 3.3                                              | <b>Unauthorized internet access to the server</b> (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means) |
|                                                                           |   |                                                                                                                          | 3.4                                              | <b>Unauthorized physical access to the server</b> (conducted for example by USB sticks or other media connecting to the server)                             |
|                                                                           |   |                                                                                                                          | 3.5                                              | <b>Information breach</b> by unintended sharing of data (e.g. admin errors)                                                                                 |
| 4.3.2 Threats to vehicles regarding their communication channels          | 4 | Spoofing of messages or data received by the vehicle                                                                     | 4.1                                              | <b>Spoofing of messages</b> by impersonation (e.g. 802.11p V2X during platooning, GNSS messages, etc.)                                                      |
|                                                                           |   |                                                                                                                          | 4.2                                              | <b>Sybil attack</b> (in order to spoof other vehicles as if there are many vehicles on the road)                                                            |
|                                                                           | 5 | Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle held code/data | 5.1                                              | Communications channels permit <b>code injection</b> , for example tampered software binary might be injected into the communication stream                 |
|                                                                           |   |                                                                                                                          | 5.2                                              | Communications channels permit <b>manipulate</b> of vehicle held data/code                                                                                  |
|                                                                           |   |                                                                                                                          | 5.3                                              | Communications channels permit <b>overwrite</b> of vehicle held data/code                                                                                   |
|                                                                           |   |                                                                                                                          | 5.4                                              | Communications channels permit <b>erasure</b> of vehicle held data/code                                                                                     |
|                                                                           |   |                                                                                                                          | 5.5                                              | Communications channels permit introduction of data/code to the vehicle (write data code)                                                                   |
|                                                                           | 6 | Communication channels permit untrusted/unreliable messages to be accepted or are                                        | 6.1                                              | Accepting information from an <b>unreliable or untrusted source</b>                                                                                         |
|                                                                           |   |                                                                                                                          | 6.2                                              | <b>Man in the middle</b> attack/ session hijacking                                                                                                          |

| High level and sub-level descriptions of vulnerability/ threat                           |    |                                                                                                                                                                  | Example of vulnerability or attack method |                                                                                                                                                               |
|------------------------------------------------------------------------------------------|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                          |    | vulnerable to session hijacking/replay attacks                                                                                                                   | 6.3                                       | <b>Replay attack</b> , for example an attack against a communication gateway allows the attacker to downgrade software of an ECU or firmware of the gateway   |
|                                                                                          | 7  | Information can be readily disclosed. For example, through eavesdropping on communications or through allowing unauthorized access to sensitive files or folders | 7.1                                       | <b>Interception of information</b> / interfering radiations / monitoring communications                                                                       |
|                                                                                          |    |                                                                                                                                                                  | 7.2                                       | Gaining <b>unauthorized access</b> to files or data                                                                                                           |
|                                                                                          | 8  | Denial of service attacks via communication channels to disrupt vehicle functions                                                                                | 8.1                                       | <b>Sending</b> a large number of garbage <b>data</b> to vehicle information system, <b>so that it is unable to provide services</b> in the normal manner      |
|                                                                                          |    |                                                                                                                                                                  | 8.2                                       | <b>Black hole attack</b> , in order to disrupt communication between vehicles the attacker is able to block messages between the vehicles                     |
|                                                                                          | 9  | An unprivileged user is able to gain privileged access to vehicle systems                                                                                        | 9.1                                       | An unprivileged user is able to <b>gain privileged access</b> , for example root access                                                                       |
|                                                                                          | 10 | Viruses embedded in communication media are able to infect vehicle systems                                                                                       | 10.1                                      | <b>Virus</b> embedded in communication media infects vehicle systems                                                                                          |
|                                                                                          | 11 | Messages received by the vehicle (for example X2V or diagnostic messages), or transmitted within it, contain malicious content                                   | 11.1                                      | Malicious <b>internal</b> (e.g. CAN) <b>messages</b>                                                                                                          |
|                                                                                          |    |                                                                                                                                                                  | 11.2                                      | Malicious <b>V2X messages</b> , e.g. infrastructure to vehicle or vehicle-vehicle messages (e.g. CAM, DENM)                                                   |
|                                                                                          |    |                                                                                                                                                                  | 11.3                                      | Malicious diagnostic messages                                                                                                                                 |
|                                                                                          |    |                                                                                                                                                                  | 11.4                                      | Malicious <b>proprietary messages</b> (e.g. those normally sent from OEM or component/system/function supplier)                                               |
| 4.3.3. Threats to vehicles regarding their update procedures                             | 12 | Misuse or compromise of update procedures                                                                                                                        | 12.1                                      | Compromise of <b>over the air software update procedures</b> . This includes fabricating the system update program or firmware                                |
|                                                                                          |    |                                                                                                                                                                  | 12.2                                      | Compromise of <b>local/physical software update procedures</b> . This includes fabricating the system update program or firmware                              |
|                                                                                          |    |                                                                                                                                                                  | 12.3                                      | The <b>software</b> is <b>manipulated before the update process</b> (and is therefore corrupted), although the update process is intact                       |
|                                                                                          |    |                                                                                                                                                                  | 12.4                                      | <b>Compromise</b> of cryptographic keys of the software provider <b>to allow invalid update</b>                                                               |
|                                                                                          | 13 | It is possible to deny legitimate updates                                                                                                                        | 13.1                                      | Denial of Service attack against update server or network to <b>prevent rollout of critical software updates</b> and/or unlock of customer specific features  |
| 4.3.4 Threats to vehicles regarding unintended human actions facilitating a cyber attack | 15 | Legitimate actors are able to take actions that would unwittingly facilitate a cyber-attack                                                                      | 15.1                                      | Innocent victim (e.g. owner, operator or maintenance engineer) being <b>tricked into taking an action</b> to unintentionally load malware or enable an attack |
|                                                                                          |    |                                                                                                                                                                  | 15.2                                      | <b>Defined security procedures</b> are not followed                                                                                                           |

| High level and sub-level descriptions of vulnerability/ threat                  |    |                                                                                                                                                                                                         | Example of vulnerability or attack method |                                                                                                                                                                                                     |
|---------------------------------------------------------------------------------|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.3.5 Threats to vehicles regarding their external connectivity and connections | 16 | Manipulation of the connectivity of vehicle functions enables a cyber-attack, this can include telematics; systems that permit remote operations; and systems using short range wireless communications | 16.1                                      | Manipulation of <b>functions designed to remotely operate systems</b> , such as remote key, immobilizer, and charging pile                                                                          |
|                                                                                 |    |                                                                                                                                                                                                         | 16.2                                      | <b>Manipulation of vehicle telematics</b> (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors)                                                                 |
|                                                                                 |    |                                                                                                                                                                                                         | 16.3                                      | Interference with <b>short range wireless systems</b> or sensors                                                                                                                                    |
|                                                                                 | 17 | Hosted 3rd party software, e.g. entertainment applications, used as a means to attack vehicle systems                                                                                                   | 17.1                                      | <b>Corrupted applications</b> , or those with poor software security, used as a method to attack vehicle systems                                                                                    |
|                                                                                 | 18 | Devices connected to external interfaces e.g. USB ports, OBD port, used as a means to attack vehicle systems                                                                                            | 18.1                                      | <b>External interfaces</b> such as USB or other ports used as a point of attack, for example through code injection                                                                                 |
|                                                                                 |    |                                                                                                                                                                                                         | 18.2                                      | Media infected with a <b>virus</b> connected to a vehicle system                                                                                                                                    |
|                                                                                 |    |                                                                                                                                                                                                         | 18.3                                      | <b>Diagnostic access (e.g. dongles in OBD port)</b> used to facilitate an attack, e.g. manipulate vehicle parameters (directly or indirectly)                                                       |
| 4.3.6 Threats to vehicle data/code                                              | 19 | Extraction of vehicle data/code                                                                                                                                                                         | 19.1                                      | Extraction of copyright or proprietary software from vehicle systems (product <b>piracy</b> )                                                                                                       |
|                                                                                 |    |                                                                                                                                                                                                         | 19.2                                      | Unauthorized access to the <b>owner's privacy information</b> such as personal identity, payment account information, address book information, location information, vehicle's electronic ID, etc. |
|                                                                                 |    |                                                                                                                                                                                                         | 19.3                                      | Extraction of cryptographic keys                                                                                                                                                                    |
|                                                                                 | 20 | Manipulation of vehicle data/code                                                                                                                                                                       | 20.1                                      | Illegal/unauthorized changes to <b>vehicle's electronic ID</b>                                                                                                                                      |
|                                                                                 |    |                                                                                                                                                                                                         | 20.2                                      | <b>Identity fraud</b> . For example, if a user wants to display another identity when communicating with toll systems, manufacturer backend                                                         |
|                                                                                 |    |                                                                                                                                                                                                         | 20.3                                      | Action to <b>circumvent monitoring systems</b> (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs)                                                          |
|                                                                                 |    |                                                                                                                                                                                                         | 20.4                                      | Data manipulation to <b>falsify vehicle's driving data</b> (e.g. mileage, driving speed, driving directions, etc.)                                                                                  |
|                                                                                 |    |                                                                                                                                                                                                         | 20.5                                      | Unauthorized changes to <b>system diagnostic data</b>                                                                                                                                               |
|                                                                                 | 21 | Erasure of data/code                                                                                                                                                                                    | 21.1                                      | Unauthorized deletion/manipulation of <b>system event logs</b>                                                                                                                                      |
|                                                                                 | 22 | Introduction of malware                                                                                                                                                                                 | 22.2                                      | Introduce <b>malicious software</b> or malicious software activity                                                                                                                                  |
|                                                                                 | 23 | Introduction of new software or overwrite existing software                                                                                                                                             | 23.1                                      | <b>Fabrication of software</b> of the vehicle control system or information system                                                                                                                  |



| High level and sub-level descriptions of vulnerability/ threat                                    |    |                                                                             | Example of vulnerability or attack method |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------------------------|----|-----------------------------------------------------------------------------|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                   | 24 | Disruption of systems or operations                                         | 24.1                                      | <b>Denial of service</b> , for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a high rate of messaging                                                                                                                                                                                                                                                     |
|                                                                                                   | 25 | Manipulation of vehicle parameters                                          | 25.1                                      | Unauthorized access of <b>falsify the configuration parameters</b> of vehicle's key functions, such as brake data, airbag deployed threshold, etc.                                                                                                                                                                                                                                                                            |
|                                                                                                   |    |                                                                             | 25.2                                      | Unauthorized access of <b>falsify the charging parameters</b> , such as charging voltage, charging power, battery temperature, etc.                                                                                                                                                                                                                                                                                           |
| 4.3.7 Potential vulnerabilities that could be exploited if not sufficiently protected or hardened | 26 | Cryptographic technologies can be compromised or are insufficiently applied | 26.1                                      | Combination of short <b>encryption keys</b> and long period of validity enables attacker to break encryption                                                                                                                                                                                                                                                                                                                  |
|                                                                                                   |    |                                                                             | 26.2                                      | Insufficient use of cryptographic algorithms to protect sensitive systems                                                                                                                                                                                                                                                                                                                                                     |
|                                                                                                   |    |                                                                             | 26.3                                      | Using already or soon to be deprecated <b>cryptographic algorithms</b>                                                                                                                                                                                                                                                                                                                                                        |
|                                                                                                   | 27 | Parts or supplies could be compromised to permit vehicles to be attacked    | 27.1                                      | <b>Hardware or software, engineered to enable an attack</b> or fails to meet design criteria to stop an attack                                                                                                                                                                                                                                                                                                                |
|                                                                                                   | 28 | Software or hardware development permits vulnerabilities                    | 28.1                                      | <b>Software bugs</b> . The presence of software bugs can be a basis for potential exploitable vulnerabilities. This is particularly true if software has not been tested to verify that known bad code/bugs is not present and reduce the risk of unknown bad code/bugs being present                                                                                                                                         |
|                                                                                                   |    |                                                                             | 28.2                                      | <b>Using remainders</b> from development (e.g. debug ports, JTAG ports, microprocessors, development certificates, developer passwords, ...) can permit access to ECUs or permit attackers to gain higher privileges                                                                                                                                                                                                          |
|                                                                                                   | 29 | Network design introduces vulnerabilities                                   | 29.1                                      | <b>Superfluous internet ports left open</b> , providing access to network systems                                                                                                                                                                                                                                                                                                                                             |
|                                                                                                   |    |                                                                             | 29.2                                      | Circumvent <b>network separation</b> to gain control. Specific example is the use of unprotected gateways, or access points (such as truck-trailer gateways), to circumvent protections and gain access to other network segments to perform malicious acts, such as sending arbitrary CAN bus messages                                                                                                                       |
|                                                                                                   | 31 | Unintended transfer of data can occur                                       | 31.1                                      | Information breach. Personal data may be leaked when the <b>car changes user</b> (e.g. is sold or is used as hire vehicle with new hirers)                                                                                                                                                                                                                                                                                    |
|                                                                                                   | 32 | Physical manipulation of systems can enable an attack                       | 32.1                                      | <b>Manipulation of electronic hardware</b> , e.g. unauthorized electronic hardware added to a vehicle to enable "man-in-the-middle" attack<br><br><b>Replacement of authorized electronic hardware</b> (e.g., sensors) with unauthorized electronic hardware<br><br><b>Manipulation of the information</b> collected by a sensor (for example, using a magnet to tamper with the Hall effect sensor connected to the gearbox) |

## Part B. Mitigations to the threats intended for vehicles

### 1. Mitigations for "Vehicle communication channels"

Mitigations to the threats which are related to "Vehicle communication channels" are listed in Table B1.

Table B1

#### Mitigation to the threats which are related to "Vehicle communication channels"

| Table A1 reference | Threats to "Vehicle communication channels"                                                                                                                    | Ref       | Mitigation                                                                                                                                                                                   |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.1                | Spoofing of messages (e.g. 802.11p V2X during platooning, GNSS messages, etc.) by impersonation                                                                | M10       | The vehicle shall verify the authenticity and integrity of messages it receives                                                                                                              |
| 4.2                | Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road)                                                                      | M11       | Security controls shall be implemented for storing cryptographic keys (e.g., use of Hardware Security Modules)                                                                               |
| 5.1                | Communication channels permit code injection into vehicle held data/code, for example tampered software binary might be injected into the communication stream | M10<br>M6 | The vehicle shall verify the authenticity and integrity of messages it receives<br>Systems shall implement security by design to minimize risks                                              |
| 5.2                | Communication channels permit manipulation of vehicle held data/code                                                                                           | M7        | Access control techniques and designs shall be applied to protect system data/code                                                                                                           |
| 5.3                | Communication channels permit overwrite of vehicle held data/code                                                                                              |           |                                                                                                                                                                                              |
| 5.4<br>21.1        | Communication channels permit erasure of vehicle held data/code                                                                                                |           |                                                                                                                                                                                              |
| 5.5                | Communication channels permit introduction of data/code to vehicle systems (write data code)                                                                   |           |                                                                                                                                                                                              |
| 6.1                | Accepting information from an unreliable or untrusted source                                                                                                   | M10       | The vehicle shall verify the authenticity and integrity of messages it receives                                                                                                              |
| 6.2                | Man in the middle attack / session hijacking                                                                                                                   | M10       | The vehicle shall verify the authenticity and integrity of messages it receives                                                                                                              |
| 6.3                | Replay attack, for example an attack against a communication gateway allows the attacker to downgrade software of an ECU or firmware of the gateway            |           |                                                                                                                                                                                              |
| 7.1                | Interception of information / interfering radiations / monitoring communications                                                                               | M12       | Confidential data transmitted to or from the vehicle shall be protected                                                                                                                      |
| 7.2                | Gaining unauthorized access to files or data                                                                                                                   | M8        | Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data. Example of Security Controls can be found in OWASP |
| 8.1                | Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner                            | M13       | Measures to detect and recover from a denial of service attack shall be employed                                                                                                             |

| <i>Table A1<br/>reference</i> | <i>Threats to "Vehicle communication channels"</i>                                                                     | <i>Ref</i> | <i>Mitigation</i>                                                                 |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------|------------|-----------------------------------------------------------------------------------|
| 8.2                           | Black hole attack, disruption of communication between vehicles by blocking the transfer of messages to other vehicles | M13        | Measures to detect and recover from a denial of service attack shall be employed  |
| 9.1                           | An unprivileged user is able to gain privileged access, for example root access                                        | M9         | Measures to prevent and detect unauthorized access shall be employed              |
| 10.1                          | Virus embedded in communication media infects vehicle systems                                                          | M14        | Measures to protect systems against embedded viruses/malware should be considered |
| 11.1                          | Malicious internal (e.g. CAN) messages                                                                                 | M15        | Measures to detect malicious internal messages or activity should be considered   |
| 11.2                          | Malicious V2X messages, e.g. infrastructure to vehicle or vehicle-vehicle messages (e.g. CAM, DENM)                    | M10        | The vehicle shall verify the authenticity and integrity of messages it receives   |
| 11.3                          | Malicious diagnostic messages                                                                                          |            |                                                                                   |
| 11.4                          | Malicious proprietary messages (e.g. those normally sent from OEM or component/system/function supplier)               |            |                                                                                   |

## 2. Mitigations for "Update process"

Mitigations to the threats which are related to "Update process" are listed in Table B2.

Table B2

### Mitigations to the threats which are related to "Update process"

| <i>Table A1<br/>reference</i> | <i>Threats to "Update process"</i>                                                                                                                    | <i>Ref</i> | <i>Mitigation</i>                                                                                                                                                                                                              |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.1                          | Compromise of over the air software update procedures. This includes fabricating the system update program or firmware                                | M16        | Secure software update procedures shall be employed                                                                                                                                                                            |
| 12.2                          | Compromise of local/physical software update procedures. This includes fabricating the system update program or firmware                              |            |                                                                                                                                                                                                                                |
| 12.3                          | The software is manipulated before the update process (and is therefore corrupted), although the update process is intact                             |            |                                                                                                                                                                                                                                |
| 12.4                          | Compromise of cryptographic keys of the software provider to allow invalid update                                                                     | M11        | Security controls shall be implemented for storing cryptographic keys                                                                                                                                                          |
| 13.1                          | Denial of Service attack against update server or network to prevent rollout of critical software updates and/or unlock of customer specific features | M3         | Security Controls shall be applied to back-end systems. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage. Example Security Controls can be found in OWASP |

## 3. Mitigations for "Unintended human actions facilitating a cyber attack"

Mitigations to the threats which are related to "Unintended human actions facilitating a cyber attack" are listed in Table B3.

Table B3

**Mitigations to the threats which are related to "Unintended human actions facilitating a cyber attack"**

| <i>Table A1 reference</i> | <i>Threats relating to "Unintended human actions"</i>                                                                                               | <i>Ref</i> | <i>Mitigation</i>                                                                                                                                                   |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 15.1                      | Innocent victim (e.g. owner, operator or maintenance engineer) is tricked into taking an action to unintentionally load malware or enable an attack | M18        | Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege                       |
| 15.2                      | Defined security procedures are not followed                                                                                                        | M19        | Organizations shall ensure security procedures are defined and followed including logging of actions and access related to the management of the security functions |

4. Mitigations for "External connectivity and connections"

Mitigations to the threats which are related to "external connectivity and connections" are listed in Table B4.

Table B4

**Mitigation to the threats which are related to "external connectivity and connections"**

| <i>Table A1 reference</i> | <i>Threats to "External connectivity and connections"</i>                                                                              | <i>Ref</i> | <i>Mitigation</i>                                                                                                                                                                                                                |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 16.1                      | Manipulation of functions designed to remotely operate vehicle systems, such as remote key, immobiliser, and charging pile             | M20        | Security controls shall be applied to systems that have remote access                                                                                                                                                            |
| 16.2                      | Manipulation of vehicle telematics (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors)           |            |                                                                                                                                                                                                                                  |
| 16.3                      | Interference with short range wireless systems or sensors                                                                              |            |                                                                                                                                                                                                                                  |
| 17.1                      | Corrupted applications, or those with poor software security, used as a method to attack vehicle systems                               | M21        | Software shall be security assessed, authenticated and integrity protected.<br><br>Security controls shall be applied to minimise the risk from third party software that is intended or foreseeable to be hosted on the vehicle |
| 18.1                      | External interfaces such as USB or other ports used as a point of attack, for example through code injection                           | M22        | Security controls shall be applied to external interfaces                                                                                                                                                                        |
| 18.2                      | Media infected with viruses connected to the vehicle                                                                                   |            |                                                                                                                                                                                                                                  |
| 18.3                      | Diagnostic access (e.g. dongles in OBD port) used to facilitate an attack, e.g. manipulate vehicle parameters (directly or indirectly) | M22        | Security controls shall be applied to external interfaces                                                                                                                                                                        |

5. Mitigations for "Potential targets of, or motivations for, an attack "

Mitigations to the threats which are related to "Potential targets of, or motivations for, an attack " are listed in Table B5.

Table B5

**Mitigations to the threats which are related to "Potential targets of, or motivations for, an attack"**

| <i>Table A1 reference</i> | <i>Threats to "Potential targets of, or motivations for, an attack"</i>                                                                                                                      | <i>Ref</i> | <i>Mitigation</i>                                                                                                                                                                                                                                                                     |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 19.1                      | Extraction of copyright or proprietary software from vehicle systems (product piracy / stolen software)                                                                                      | M7         | Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP                                                                                                                                                   |
| 19.2                      | Unauthorized access to the owner's privacy information such as personal identity, payment account information, address book information, location information, vehicle's electronic ID, etc. | M8         | Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data. Examples of Security Controls can be found in OWASP                                                                                         |
| 19.3                      | Extraction of cryptographic keys                                                                                                                                                             | M11        | Security controls shall be implemented for storing cryptographic keys e.g. Security Modules                                                                                                                                                                                           |
| 20.1                      | Illegal/unauthorised changes to vehicle's electronic ID                                                                                                                                      | M7         | Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP                                                                                                                                                   |
| 20.2                      | Identity fraud. For example, if a user wants to display another identity when communicating with toll systems, manufacturer backend                                                          |            |                                                                                                                                                                                                                                                                                       |
| 20.3                      | Action to circumvent monitoring systems (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs)                                                          | M7         | Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP.<br><br>Data manipulation attacks on sensors or transmitted data could be mitigated by correlating the data from different sources of information |
| 20.4                      | Data manipulation to falsify vehicle's driving data (e.g. mileage, driving speed, driving directions, etc.)                                                                                  |            |                                                                                                                                                                                                                                                                                       |
| 20.5                      | Unauthorised changes to system diagnostic data                                                                                                                                               |            |                                                                                                                                                                                                                                                                                       |
| 21.1                      | Unauthorized deletion/manipulation of system event logs                                                                                                                                      | M7         | Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP.                                                                                                                                                  |
| 22.2                      | Introduce malicious software or malicious software activity                                                                                                                                  | M7         | Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP.                                                                                                                                                  |
| 23.1                      | Fabrication of software of the vehicle control system or information system                                                                                                                  |            |                                                                                                                                                                                                                                                                                       |
| 24.1                      | Denial of service, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a high rate of messaging                            | M13        | Measures to detect and recover from a denial of service attack shall be employed                                                                                                                                                                                                      |
| 25.1                      | Unauthorized access to falsify configuration parameters of vehicle's key functions, such as brake data, airbag deployed threshold, etc.                                                      | M7         | Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP                                                                                                                                                   |
| 25.2                      | Unauthorized access to falsify charging parameters, such as charging voltage, charging power, battery temperature, etc.                                                                      |            |                                                                                                                                                                                                                                                                                       |

6. Mitigations for "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened"

Mitigations to the threats which are related to "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened" are listed in Table B6.

Table B6

**Mitigations to the threats which are related to "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened"**

| <i>Table A1 reference</i> | <i>Threats to "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened"</i>                                                                                                                                                                                  | <i>Ref</i> | <i>Mitigation</i>                                                                                                                                                                |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 26.1                      | Combination of short encryption keys and long period of validity enables attacker to break encryption                                                                                                                                                                                            | M23        | Cybersecurity best practices for software and hardware development shall be followed                                                                                             |
| 26.2                      | Insufficient use of cryptographic algorithms to protect sensitive systems                                                                                                                                                                                                                        |            |                                                                                                                                                                                  |
| 26.3                      | Using deprecated cryptographic algorithms                                                                                                                                                                                                                                                        |            |                                                                                                                                                                                  |
| 27.1                      | Hardware or software, engineered to enable an attack or fail to meet design criteria to stop an attack                                                                                                                                                                                           | M23        | Cybersecurity best practices for software and hardware development shall be followed                                                                                             |
| 28.1                      | The presence of software bugs can be a basis for potential exploitable vulnerabilities. This is particularly true if software has not been tested to verify that known bad code/bugs is not present and reduce the risk of unknown bad code/bugs being present                                   | M23        | Cybersecurity best practices for software and hardware development shall be followed.<br>Cybersecurity testing with adequate coverage                                            |
| 28.2                      | Using remainders from development (e.g. debug ports, JTAG ports, microprocessors, development certificates, developer passwords, ...) can permit an attacker to access ECUs or gain higher privileges                                                                                            |            |                                                                                                                                                                                  |
| 29.1                      | Superfluous internet ports left open, providing access to network systems                                                                                                                                                                                                                        |            |                                                                                                                                                                                  |
| 29.2                      | Circumvent network separation to gain control. Specific example is the use of unprotected gateways, or access points (such as truck-trailer gateways), to circumvent protections and gain access to other network segments to perform malicious acts, such as sending arbitrary CAN bus messages | M23        | Cybersecurity best practices for software and hardware development shall be followed.<br>Cybersecurity best practices for system design and system integration shall be followed |

7. Mitigations for "Data loss / data breach from vehicle"

Mitigations to the threats which are related to "Data loss / data breach from vehicle" are listed in Table B7.

Table B7

**Mitigations to the threats which are related to "Data loss / data breach from vehicle"**

| <i>Table A1 reference</i> | <i>Threats of "Data loss / data breach from vehicle"</i>                                                                              | <i>Ref</i> | <i>Mitigation</i>                                                                                                    |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------|------------|----------------------------------------------------------------------------------------------------------------------|
| 31.1                      | Information breach. Personal data may be breached when the car changes user (e.g. is sold or is used as hire vehicle with new hirers) | M24        | Best practices for the protection of data integrity and confidentiality shall be followed for storing personal data. |

## 8. Mitigations for "Physical manipulation of systems to enable an attack"

Mitigation to the threats which are related to "Physical manipulation of systems to enable an attack" are listed in Table B8.

Table B8

**Mitigations to the threats which are related to "Physical manipulation of systems to enable an attack"**

| <i>Table A1 reference</i> | <i>Threats to "Physical manipulation of systems to enable an attack"</i>                                         | <i>Ref</i> | <i>Mitigation</i>                                                    |
|---------------------------|------------------------------------------------------------------------------------------------------------------|------------|----------------------------------------------------------------------|
| 32.1                      | Manipulation of OEM hardware, e.g. unauthorised hardware added to a vehicle to enable "man-in-the-middle" attack | M9         | Measures to prevent and detect unauthorized access shall be employed |

**Part C. Mitigations to the threats outside of vehicles**

## 1. Mitigations for "Back-end servers"

Mitigations to the threats which are related to "Back-end servers" are listed in Table C1.

Table C1

**Mitigations to the threats which are related to "Back-end servers"**

| <i>Table A1 reference</i> | <i>Threats to "Back-end servers"</i>                                                                                                                 | <i>Ref</i> | <i>Mitigation</i>                                                                                                                                                                                                         |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.1 & 3.1                 | Abuse of privileges by staff (insider attack)                                                                                                        | M1         | Security Controls are applied to back-end systems to minimise the risk of insider attack                                                                                                                                  |
| 1.2 & 3.3                 | Unauthorised internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means) | M2         | Security Controls are applied to back-end systems to minimise unauthorised access. Example Security Controls can be found in OWASP                                                                                        |
| 1.3 & 3.4                 | Unauthorised physical access to the server (conducted by for example USB sticks or other media connecting to the server)                             | M8         | Through system design and access control it should not be possible for unauthorised personnel to access personal or system critical data                                                                                  |
| 2.1                       | Attack on back-end server stops it functioning, for example it prevents it from interacting with vehicles and providing services they rely on        | M3         | Security Controls are applied to back-end systems. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage. Example Security Controls can be found in OWASP |
| 3.2                       | Loss of information in the cloud. Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers  | M4         | Security Controls are applied to minimise risks associated with cloud computing. Example Security Controls can be found in OWASP and NCSC cloud computing guidance                                                        |
| 3.5                       | Information breach by unintended sharing of data (e.g. admin errors, storing data in servers in garages)                                             | M5         | Security Controls are applied to back-end systems to prevent data breaches. Example Security Controls can be found in OWASP                                                                                               |



2. Mitigations for "Unintended human actions"  
Mitigations to the threats which are related to "Unintended human actions" are listed in Table C2.

Table C2

**Mitigations to the threats which are related to "Unintended human actions"**

| <i>Table A1 reference</i> | <i>Threats relating to "Unintended human actions"</i>                                                                                               | <i>Ref</i> | <i>Mitigation</i>                                                                                                                                                   |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 15.1                      | Innocent victim (e.g. owner, operator or maintenance engineer) is tricked into taking an action to unintentionally load malware or enable an attack | M18        | Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege                       |
| 15.2                      | Defined security procedures are not followed                                                                                                        | M19        | Organizations shall ensure security procedures are defined and followed including logging of actions and access related to the management of the security functions |

3. Mitigations for "Physical loss of data"  
Mitigations to the threats which are related to "Physical loss of data" are listed in Table C3.

Table C3

**Mitigations to the threats which are related to "Physical loss of data loss"**

| <i>Table A1 reference</i> | <i>Threats of "Physical loss of data"</i>                                                                                                                     | <i>Ref</i> | <i>Mitigation</i>                                                                                                                                                           |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 30.1                      | Damage caused by a third party. Sensitive data may be lost or compromised due to physical damages in cases of traffic accident or theft                       | M24        | Best practices for the protection of data integrity and confidentiality shall be followed for storing personal data. Example Security Controls can be found in ISO/SC27/WG5 |
| 30.2                      | Loss from DRM (digital right management) conflicts. User data may be deleted due to DRM issues                                                                |            |                                                                                                                                                                             |
| 30.3                      | The (integrity of) sensitive data may be lost due to IT components wear and tear, causing potential cascading issues (in case of key alteration, for example) |            |                                                                                                                                                                             |



# **UNECE R/155**

## **APÉNDICES A LA NORMATIVA R155 DESDE 2021 A 2024**

25 November 2022

---

## **Agreement**

### **Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations\***

(Revision 3, including the amendments which entered into force on 14 September 2017)

---

## **Addendum 154 – UN Regulation No. 155**

### **Amendment 1**

Supplement 1 to the original version of the Regulation – Date of entry into force:  
8 October 2022

### **Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system**

This document is meant purely as documentation tool. The authentic and legal binding text is: ECE/TRANS/WP.29/2022/54.



**UNITED NATIONS**

---

\* Former titles of the Agreement:

Agreement concerning the Adoption of Uniform Conditions of Approval and Reciprocal Recognition of Approval for Motor Vehicle Equipment and Parts, done at Geneva on 20 March 1958 (original version);  
Agreement concerning the Adoption of Uniform Technical Prescriptions for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these Prescriptions, done at Geneva on 5 October 1995 (Revision 2).



*Paragraph 7.3.1., amend to read:*

"7.3.1. The manufacturer shall have a valid Certificate of Compliance for the Cyber Security Management System relevant to the vehicle type being approved.

However, for type approvals first issued before 1 July 2024 and for each extension thereof, if the vehicle manufacturer can demonstrate that the vehicle type could not be developed in compliance with the CSMS, then the vehicle manufacturer shall demonstrate that cyber security was adequately considered during the development phase of the vehicle type concerned."

*Paragraph 7.3.4., amend to read:*

"7.3.4. The vehicle manufacturer shall protect the vehicle type against risks identified in the vehicle manufacturer's risk assessment. Proportionate mitigations shall be implemented to protect the vehicle type. The mitigations implemented shall include all mitigations referred to in Annex 5, Part B and C which are relevant for the risks identified. However, if a mitigation referred to in Annex 5, Part B or C, is not relevant or not sufficient for the risk identified, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented.

In particular, for type approvals first issued before 1 July 2024 and for each extension thereof, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented if a mitigation measure referred to in Annex 5, Part B or C is technically not feasible. The respective assessment of the technical feasibility shall be provided by the manufacturer to the approval authority."

---

4 March 2024

---

## **Agreement**

### **Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations\***

(Revision 3, including the amendments which entered into force on 14 September 2017)

---

## **Addendum 154 – UN Regulation No. 155**

### **Amendment 2**

Supplement 2 to the original version of the Regulation – Date of entry into force:  
5 January 2024

### **Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system**

This document is meant purely as documentation tool. The authentic and legal binding text is: ECE/TRANS/WP.29/2023/70.



**UNITED NATIONS**

---

\* Former titles of the Agreement:

Agreement concerning the Adoption of Uniform Conditions of Approval and Reciprocal Recognition of Approval for Motor Vehicle Equipment and Parts, done at Geneva on 20 March 1958 (original version);  
Agreement concerning the Adoption of Uniform Technical Prescriptions for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these Prescriptions, done at Geneva on 5 October 1995 (Revision 2).

*Annex 5, Part A, second major row of Table A1, item 4, amend to read:*

|                                                                  |   |                                                      |     |                                                                                                                                       |
|------------------------------------------------------------------|---|------------------------------------------------------|-----|---------------------------------------------------------------------------------------------------------------------------------------|
| 4.3.2 Threats to vehicles regarding their communication channels | 4 | Spoofing of messages or data received by the vehicle | 4.1 | <b>Spoofing of messages</b> by impersonation (e.g. V2X cooperative awareness or manoeuvre coordination messages, GNSS messages, etc.) |
|                                                                  |   |                                                      | 4.2 | <b>Sybil attack</b> (in order to spoof other vehicles as if there are many vehicles on the road)                                      |

*Annex 5, Part B, first row of Table B1, amend to read:*

| <i>Table A1 reference</i> | <i>Threats to "Vehicle communication channels"</i>                                                                             | <i>Ref</i> | <i>Mitigation</i>                                                               |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------|------------|---------------------------------------------------------------------------------|
| 4.1                       | Spoofing of messages (e.g. V2X cooperative awareness or manoeuvre coordination messages, GNSS messages, etc.) by impersonation | M10        | The vehicle shall verify the authenticity and integrity of messages it receives |



# **UNECE R/155**

## **LA ONU AMPLÍA LA NORMATIVA A LAS MOTOCICLETAS, SCOOTERS Y BICICLETAS**



UNECE (/) **TRANSPORT (/TRANSPORT)**

# UN extends its cyber security management regulation to motorcycles and scooters

Autonomous Driving   Vehicle Regulations   Transport

26 January 2024

UNECE's Working Party on Automated/Autonomous and Connected Vehicles today decided to include motorcycles, scooters and electric bicycles with speed exceeding 25 km/h in the scope of the UN Regulation No. 155 on cyber security and cyber security management (<https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security>).



In force since January 2021, UN Regulation 155 is applied in various regions of the world and covers passenger cars, trucks, and buses. Its purpose is to offer an international framework for the type approval of road vehicles with regard to cyber security.

Following the review of the requirements in that regulation and their possible suitability to adequately address the specificities of motorcycles, the Working Group agreed to insert this vehicle category in the scope of UN Regulation 155, with support of the motorcycle industry.

The decision to extend the scope of UN Regulation 155 to motorcycles (vehicle category L) will be submitted to the UNECE-hosted World Forum for Harmonization of Vehicle Regulations (WP.29) for adoption in June 2024. National implementation roadmaps can deviate from that and can also have roadmaps with earlier milestones.

It comes at a time when the motorcycle industry has already introduced complex assistance systems in powered two wheelers, such as Adaptive Cruise Control and advanced connectivity. These developments are justifying the growing concerns about potential cyber risks for this type of vehicles.

Furthermore, it comes in a context of increased regulation affecting the automotive industry, especially in China, Europe and India, as well as regulations to ensure a risk-based identified minimum level of cybersecurity protection of all products with digital elements available in the



market, such as the upcoming European Union Cyber Resilience Act.

Going forward, the Working Party will strive to offer the broadest scope possible to its Contracting Parties to approve a wide variety of vehicles in category L and to allow manufacturers to apply for a type approval.

## **Note to editors**

### **About autonomous driving at the World Forum for Harmonization of Vehicle Regulations**

The World Forum for Harmonization of Vehicle Regulations, hosted by UNECE, is the intergovernmental platform responsible for the regulatory frameworks regarding the safety and environmental performance of vehicles, their subsystems and parts.

Its dedicated Working Party on Automated/Autonomous and Connected Vehicles (GRVA) ([http://www.unece.org/trans/main/wp29/meeting\\_docs\\_grva.html](http://www.unece.org/trans/main/wp29/meeting_docs_grva.html)) brings together countries including the EU, USA, China, Japan and Canada to develop internationally harmonized regulations, resolutions and guidelines governing automated driving functionalities, such as provisions related to the dynamics of vehicles (braking, steering), Advanced Driver Assistance Systems, Automated Driving Systems, as well as Connected Vehicles and Cyber Security provisions. The group currently supervises eight informal work groups (IWGs) and tasks forces.

UN Regulations enter into force six months after their adoption by the World Forum. This is the time given to contracting Parties to the UN Vehicles agreements to notify the United Nations Office of Legal Affairs about their opposition to the adopted text, or their intention not to adopt its provisions, and also to provide countries with sufficient time for implementation.

If you wish to subscribe to the UNECE Weekly newsletter, please send an email to:  
[unece\\_info@un.org](mailto:unece_info@un.org) ([mailto:unece\\_info@un.org](mailto:unece_info@un.org))

## **United Nations Economic Commission for Europe**

### **Information Unit**

Tel.: +41 (0) 22 917 12 34

Email: [unece\\_info@un.org](mailto:unece_info@un.org) ([mailto:unece\\_info@un.org](mailto:unece_info@un.org))

Reproduction is permitted provided that the source is acknowledged.



# **UNECE R/156**

**Uniform provisions  
concerning the approval of  
vehicles with regards to  
software update and  
software updates  
management system**

4 March 2021

---

## **Agreement**

### **Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations\***

(Revision 3, including the amendments which entered into force on 14 September 2017)

---

#### **Addendum 155 – UN Regulation No. 156**

Date of entry into force as an annex to the 1958 Agreement: 22 January 2021

#### **Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system**

This document is meant purely as documentation tool. The authentic and legal binding text is: ECE/TRANS/WP.29/2020/80.



**UNITED NATIONS**

---

\* Former titles of the Agreement:

Agreement concerning the Adoption of Uniform Conditions of Approval and Reciprocal Recognition of Approval for Motor Vehicle Equipment and Parts, done at Geneva on 20 March 1958 (original version);  
Agreement concerning the Adoption of Uniform Technical Prescriptions for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these Prescriptions, done at Geneva on 5 October 1995 (Revision 2).



## UN Regulation No. 156

### Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system

#### Contents

|                                                                                                                                | <i>Page</i> |
|--------------------------------------------------------------------------------------------------------------------------------|-------------|
| 1. Scope .....                                                                                                                 | 4           |
| 2. Definitions.....                                                                                                            | 4           |
| 3. Application for approval .....                                                                                              | 4           |
| 4. Markings .....                                                                                                              | 5           |
| 5. Approval .....                                                                                                              | 6           |
| 6. Certificate of compliance for Software Update Management System .....                                                       | 6           |
| 7. General specifications .....                                                                                                | 7           |
| 8. Modification and extension of the vehicle type .....                                                                        | 10          |
| 9. Conformity of production .....                                                                                              | 11          |
| 10. Penalties for non-conformity of production .....                                                                           | 11          |
| 11. Production definitively discontinued .....                                                                                 | 11          |
| 12. Names and addresses of Technical Services responsible for conducting approval tests and of Type Approval Authorities ..... | 11          |

#### Annexes

|   |                                                                                      |    |
|---|--------------------------------------------------------------------------------------|----|
| 1 | Information document .....                                                           | 12 |
|   | Appendix 1 Model of declaration of compliance for Software Update Management System. | 13 |
| 2 | Communication .....                                                                  | 14 |
| 3 | Arrangement of approval mark .....                                                   | 15 |
| 4 | Model of Certificate of Compliance for Software Update Management System .....       | 16 |

## 1. Scope

- 1.1. This Regulation applies to vehicles of Categories<sup>1</sup> M, N, O, R, S and T that permit software updates.

## 2. Definitions

- 2.1. "*Vehicle type*" means vehicles which do not differ in at least the following:
- (a) The manufacturer's designation of the vehicle type;
  - (b) Essential aspects of the design of the vehicle type with respect to software update processes.
- 2.2. "*RX Software Identification Number (RXSWIN)*" means a dedicated identifier, defined by the vehicle manufacturer, representing information about the type approval relevant software of the Electronic Control System contributing to the Regulation N° X type approval relevant characteristics of the vehicle.
- 2.3. "*Software update*" means a package used to upgrade software to a new version including a change of the configuration parameters.
- 2.4. "*Execution*" means the process of installing and activating an update that has been downloaded.
- 2.5. "*Software Update Management System (SUMS)*" means a systematic approach defining organizational processes and procedures to comply with the requirements for delivery of software updates according to this Regulation.
- 2.6. "*Vehicle user*" means a person operating or driving the vehicle, a vehicle owner, an authorised representative or employee of a fleet manager, an authorised representative or employee of the vehicle manufacturer, or an authorized technician.
- 2.7. "*Safe state*" means an operating mode in case of a failure of an item without an unreasonable level of risk.
- 2.8. "*Software*" means the part of an Electronic Control System that consists of digital data and instruction.
- 2.9. "*Over-the-Air (OTA) update*" means any method of making data transfers wirelessly instead of using a cable or other local connection.
- 2.10. "*System*" means a set of components and/or sub-systems that implement a function of functions.
- 2.11. "*Integrity validation data*" means a representation of digital data, against which comparisons can be made to detect errors or changes in the data. This may include checksums and hash values.

## 3. Application for approval

- 3.1. The application for approval of a vehicle type with regard to software update processes shall be submitted by the vehicle manufacturer or by their duly accredited representative.
- 3.2. It shall be accompanied by the undermentioned documents in triplicate, and by the following particulars:

---

<sup>1</sup> As defined in the Consolidated Resolution on the Construction of Vehicles (R.E.3.), document ECE/TRANS/WP.29/78/Rev.6, para. 2 – [www.unece.org/transport/standards/transport/vehicle-regulations-wp29/resolutions](http://www.unece.org/transport/standards/transport/vehicle-regulations-wp29/resolutions)

- 3.3. A description of the vehicle type with regard to the items specified in Annex 1 to this Regulation.
- 3.4. In cases where information is shown to be covered by intellectual property rights or to constitute specific know-how of the manufacturer or of their suppliers, the manufacturer or their suppliers shall make available sufficient information to enable the checks referred to in this Regulation to be made properly. Such information shall be treated on a confidential basis.
- 3.5. The Certificate of Compliance for Software Update Management System according to paragraph 6. of this Regulation.
- 3.6. A vehicle representative of the vehicle type to be approved shall be submitted to the Technical Service responsible for conducting approval tests.
- 3.7. Documentation shall be made available in two parts:
  - (a) The formal documentation package for the approval, containing the material specified in Annex 1 which shall be supplied to the Approval Authority or its Technical Service at the time of submission of the type approval application. This documentation package shall be used by the Approval Authority or its Technical Service as the basic reference for the approval process. The Approval Authority or its Technical Service shall ensure that this documentation package remains available for at least 10 years counted from the time when production of the vehicle type is definitely discontinued.
  - (b) Additional material relevant to the requirements of this regulation may be retained by the manufacturer but made open for inspection at the time of type approval. The manufacturer shall ensure that any material made open for inspection at the time of type approval remains available for at least a period of 10 years counted from the time when production of the vehicle type is definitely discontinued.

## 4. Marking

- 4.1. There shall be affixed, conspicuously and in a readily accessible place specified on the approval form, to every vehicle conforming to a vehicle type approved under this Regulation an international approval mark consisting of:
  - 4.1.1. A circle surrounding the Letter "E" followed by the distinguishing number of the country which has granted approval.<sup>2</sup>
  - 4.1.2. The number of this Regulation, followed by the letter "R", a dash and the approval number to the right of the circle described in paragraph 4.1.1. above.
- 4.2. If the vehicle conforms to a vehicle type approved under one or more other Regulations annexed to the Agreement in the country which has granted approval under this Regulation, the symbol prescribed in paragraph 4.1.1. above need not be repeated; in this case the Regulation and approval numbers and the additional symbols of all the Regulations under which approval has been granted in the country which has granted approval under this Regulation shall be placed in vertical columns to the right of the symbol prescribed in paragraph 4.1.1. above.
- 4.3. The approval mark shall be clearly legible and shall be indelible.

---

<sup>2</sup> The distinguishing numbers of the Contracting Parties to the 1958 Agreement are reproduced in Annex 3 to the Consolidated Resolution on the Construction of Vehicles (R.E.3), document ECE/TRANS/WP.29/78/Rev.6 – [www.unece.org/transport/standards/transport/vehicle-regulations-wp29/resolutions](http://www.unece.org/transport/standards/transport/vehicle-regulations-wp29/resolutions).

- 4.4. The approval mark shall be placed on or close to the vehicle data plate affixed by the Manufacturer.
- 4.5. Annex 3 to this Regulation gives examples of the arrangements of the approval mark.

## **5. Approval**

- 5.1. Approval Authorities shall grant, as appropriate, type approval with regard to software update procedures and processes, only to such vehicle types that satisfy the requirements of this Regulation.
  - 5.1.1. The Approval Authority or the Technical Service shall verify by testing a vehicle of the vehicle type that the vehicle manufacturer has implemented the measures they have documented. Tests shall be performed by approval authority or the technical service itself or in collaboration with the vehicle manufacturer by sampling.
- 5.2. Notice of approval or of extension or refusal of approval of a vehicle type pursuant to this Regulation shall be communicated to the Parties to the 1958 Agreement which apply this Regulation, by means of a form conforming to the model in Annex 2 to this Regulation.
- 5.3. Approval Authorities shall not grant any type approval without ensuring that the manufacturer has put in place satisfactory arrangements and procedures to manage properly the software update processes aspects as covered by this regulation.

## **6. Certificate of Compliance for Software Update Management System**

- 6.1. Contracting Parties shall appoint an Approval Authority to carry out the assessment of the manufacturer and to issue a Certificate of Compliance for Software Update Management System.
- 6.2. An application for a Certificate of Compliance for Software Update Management System shall be submitted by the vehicle manufacturer or by their duly accredited representative.
- 6.3. It shall be accompanied by the undermentioned documents in triplicate, and by the following particular:
  - 6.3.1. Documents describing the Software Update Management System.
  - 6.3.2. A signed declaration using the model as defined in Appendix 1 to Annex 1.
- 6.4. In the context of the assessment, the manufacturer shall declare using the model as defined in Appendix 1 to Annex 1 and demonstrate to the satisfaction of the Approval Authority or its Technical Service that they have the necessary processes to comply with all the requirements for software updates according to this Regulation.
- 6.5. When this assessment has been satisfactorily completed and in receipt of a signed declaration from the manufacturer according to the model as defined in Appendix 1 to Annex 1, a certificate named Certificate of Compliance for SUMS as described in Annex 4 to this Regulation (hereinafter the Certificate of Compliance for SUMS) shall be granted to the manufacturer.
- 6.6. The Certificate of Compliance for SUMS shall remain valid for a maximum of three years from the date of deliverance of the certificate unless it is withdrawn.
- 6.7. The Approval Authority which has granted the Certificate of Compliance for Software Update Management System may at any time verify its continued

compliance. The Certificate of Compliance for Software Update Management System may be withdrawn if the requirements laid down in this Regulation are no longer met.

- 6.8. The manufacturer shall inform the Approval Authority or its Technical Service of any change that will affect the relevance of the Certificate of Compliance for Software Update Management System. After consultation with the manufacturer, the Approval Authority or its Technical Service shall decide whether new checks are necessary.
- 6.9. At the end of the period of validity of the Certificate of Compliance for Software Update Management System, the Approval Authority shall, after a positive assessment, issue a new Certificate of Compliance for Software Update Management System or extends its validity for a further period of three years. The Approval Authority shall issue a new certificate in cases where changes have been brought to the attention of the Approval Authority or its Technical Service and the changes have been positively re-assessed.
- 6.10. Existing vehicle type approvals shall not lose their validity due to the expiration of the manufacturer's Certificate of Compliance for Software Update Management System.

## **7. General specifications**

- 7.1. Requirements for the Software Update Management System of the vehicle manufacturer
  - 7.1.1. Processes to be verified at initial assessment
    - 7.1.1.1. A process whereby information relevant to this Regulation is documented and securely held at the vehicle manufacturer and can be made available to an Approval Authority or its Technical Service upon request;
    - 7.1.1.2. A process whereby information regarding all initial and updated software versions, including integrity validation data, and relevant hardware components of a type approved system can be uniquely identified;
    - 7.1.1.3. A process whereby, for a vehicle type that has an RXSWIN, information regarding the RXSWIN of the vehicle type before and after an update can be accessed and updated. This shall include the ability to update information regarding the software versions and their integrity validation data of all relevant software for each RXSWIN;
    - 7.1.1.4. A process whereby, for a vehicle type that has an RXSWIN, the vehicle manufacturer can verify that the software version(s) present on a component of a type approved system are consistent with those defined by the relevant RXSWIN;
    - 7.1.1.5. A process whereby any interdependencies of the updated system with other systems can be identified;
    - 7.1.1.6. A process whereby the vehicle manufacturer is able to identify target vehicles for a software update;
    - 7.1.1.7. A process to confirm the compatibility of a software update with the target vehicle(s) configuration before it is issued. This shall include an assessment of the last known software/hardware configuration of the target vehicle(s) for compatibility with the update before it is issued;
    - 7.1.1.8. A process to assess, identify and record whether a software update will affect any type approved systems. This shall consider whether the update will impact or alter any of the parameters used to define the systems the update may affect or whether it may change any of the parameters used to type approve those system (as defined in the relevant legislation);



- 7.1.1.9. A process to assess, identify and record whether a software update will add, alter or enable any functions that were not present, or enabled, when the vehicle was type approved or alter or disable any other parameters or functions that are defined within legislation. The assessment shall include consideration of whether:
- (a) Entries in the information package will need to be modified;
  - (b) Test results no longer cover the vehicle after modification;
  - (c) Any modification to functions on the vehicle will affect the vehicle's type approval.
- 7.1.1.10. A process to assess, identify and record if a software update will affect any other system required for the safe and continued operation of the vehicle or if the update will add or alter functionality of the vehicle compared to when it was registered;
- 7.1.1.11. A process whereby the vehicle user is able to be informed about updates;
- 7.1.1.12. A process whereby the vehicle manufacturer shall be able to make the information according to paragraph 7.1.2.3. and 7.1.2.4. available to responsible Authorities or the Technical Services. This may be for the purpose of type approval, conformity of production, market surveillance, recalls and Periodic Technical Inspection (PTI).
- 7.1.2. The vehicle manufacturer shall record, and store, the following information for each update applied to a given vehicle type:
- 7.1.2.1. Documentation describing the processes used by the vehicle manufacturer for software updates and any relevant standards used to demonstrate their compliance;
- 7.1.2.2. Documentation describing the configuration of any relevant type approved systems before and after an update, this shall include unique identification for the type approved system's hardware and software (including software versions) and any relevant vehicle or system parameters;
- 7.1.2.3. For every RXSWIN, there shall be an auditable register describing all the software relevant to the RXSWIN of the vehicle type before and after an update. This shall include information of the software versions and their integrity validation data for all relevant software for each RXSWIN.
- 7.1.2.4. Documentation listing target vehicles for the update and confirmation of the compatibility of the last known configuration of those vehicles with the update.
- 7.1.2.5. Documentation for all software updates for that vehicle type describing:
- (a) The purpose of the update;
  - (b) What systems or functions of the vehicle the update may affect;
  - (c) Which of these are type approved (if any);
  - (d) If applicable, whether the software update affects the fulfilment of any of the relevant requirements of those type approved system;
  - (e) Whether the software update affects any system type approval parameter;
  - (f) Whether an approval for the update was sought from an approval body;
  - (g) How the update may be executed and under what conditions;
  - (h) Confirmation that the software update will be conducted safely and securely;
  - (i) Confirmation that the software update has undergone and successfully passed verification and validation procedures.

- 7.1.3. Security - the vehicle manufacturer shall demonstrate:
  - 7.1.3.1. The process they will use to ensure that software updates will be protected to reasonably prevent manipulation before the update process is initiated.;
  - 7.1.3.2. The update processes used are protected to reasonably prevent them being compromised, including development of the update delivery system;
  - 7.1.3.3. The processes used to verify and validate software functionality and code for the software used in the vehicle are appropriate.
- 7.1.4. Additional requirements for software updates over the air
  - 7.1.4.1. The vehicle manufacturer shall demonstrate the processes and procedures they will use to assess that over the air updates will not impact safety, if conducted during driving.
  - 7.1.4.2. The vehicle manufacturer shall demonstrate the processes and procedures they will use to ensure that, when an over the air update requires a specific skilled or complex action, for example recalibrate a sensor post-programming, in order to complete the update process, the update can only proceed when a person skilled to do that action is present or is in control of the process.
- 7.2. Requirements for the Vehicle Type
  - 7.2.1. Requirements for Software updates
    - 7.2.1.1. The authenticity and integrity of software updates shall be protected to reasonably prevent their compromise and reasonably prevent invalid updates.
    - 7.2.1.2. Where a vehicle type uses RXSWIN:
      - 7.2.1.2.1. Each RXSWIN shall be uniquely identifiable. When type approval relevant software is modified by the vehicle manufacturer, the RXSWIN shall be updated if it leads to a type approval extension or to a new type approval.
      - 7.2.1.2.2. Each RXSWIN shall be easily readable in a standardized way via the use of an electronic communication interface, at least by the standard interface (OBD port).
 

If RXSWINs are not held on the vehicle, the manufacturer shall declare the software version(s) of the vehicle or single ECUs with the connection to the relevant type approvals to the Approval Authority. This declaration shall be updated each time the declared software version(s) is updated. In this case, the software version(s) shall be easily readable in a standardized way via the use of an electronic communication interface, at least by the standard interface (OBD port).
      - 7.2.1.2.3. The vehicle manufacturer shall protect the RXSWINs and/or software version(s) on a vehicle against unauthorised modification. At the time of Type Approval, the means implemented to protect against unauthorized modification of the RXSWIN and/or software version(s) chosen by the vehicle manufacturer shall be confidentially provided.
  - 7.2.2. Additional Requirements for over the air updates
    - 7.2.2.1. The vehicle shall have the following functionality with regards to software updates:
      - 7.2.2.1.1. The vehicle manufacturer shall ensure that the vehicle is able to restore systems to their previous version in case of a failed or interrupted update or that the vehicle can be placed into a safe state after a failed or interrupted update.
      - 7.2.2.1.2. The vehicle manufacturer shall ensure that software updates can only be executed when the vehicle has enough power to complete the update process (including that needed for a possible recovery to the previous version or for the vehicle to be placed into a safe state).

- 7.2.2.1.3. When the execution of an update may affect the safety of the vehicle, the vehicle manufacturer shall demonstrate how the update will be executed safely. This shall be achieved through technical means that ensures the vehicle is in a state where the update can be executed safely.
- 7.2.2.2. The vehicle manufacturer shall demonstrate that the vehicle user is able to be informed about an update before the update is executed. The information made available shall contain:
- (a) The purpose of the update. This could include the criticality of the update and if the update is for recall, safety and/or security purposes;
  - (b) Any changes implemented by the update on vehicle functions;
  - (c) The expected time to complete execution of the update;
  - (d) Any vehicle functionalities which may not be available during the execution of the update;
  - (e) Any instructions that may help the vehicle user safely execute the update;
- In case of groups of updates with a similar content one information may cover a group.
- 7.2.2.3. In the situation where the execution of an update whilst driving may not be safe, the vehicle manufacturer shall demonstrate how they will:
- (a) Ensure the vehicle cannot be driven during the execution of the update;
  - (b) Ensure that the driver is not able to use any functionality of the vehicle that would affect the safety of the vehicle or the successful execution of the update.
- 7.2.2.4. After the execution of an update the vehicle manufacturer shall demonstrate how the following will be implemented:
- (a) The vehicle user is able to be informed of the success (or failure) of the update;
  - (b) The vehicle user is able to be informed about the changes implemented and any related updates to the user manual (if applicable).
- 7.2.2.5. The vehicle shall ensure that preconditions have to be met before the software update is executed.

## **8. Modification and extension of the vehicle type**

- 8.1. Every modification of the vehicle type which affects its technical performance and/or documentation required in this Regulation shall be notified to the approval authority which granted the approval. The approval authority may then either:
- 8.1.1. Consider that the modifications made still comply with the requirements and documentation of prior type approval; or
  - 8.1.2. Require a further test report from the Technical Service responsible for conducting the tests.
  - 8.1.3. Confirmation or extension or refusal of approval, specifying the alterations, shall be communicated by means of a communication form conforming to the model in Annex 2 to this Regulation. The approval authority issuing the extension of approval shall assign a series number for such an extension and inform there of the other Parties to the 1958 Agreement applying this Regulation by means of a communication form conforming to the model in Annex 2 to this Regulation.

## **9. Conformity of production**

- 9.1. The Conformity of Production Procedures shall comply with those set out in the 1958 Agreement, Schedule 1 (E/ECE/TRANS/505/Rev.3) with the following requirements:
  - 9.1.1. The holder of the approval shall ensure that results of the conformity of production tests are recorded and that the annexed documents remain available for a period determined in agreement with the Approval Authority or its Technical Service. This period shall not exceed 10 years counted from the time when production is definitively discontinued;
  - 9.1.2. The Approval Authority which has granted type approval may at any time verify the conformity control methods applied in each production facility. The normal frequency of these verifications shall be once every three years.
  - 9.1.3. The Approval Authority or its Technical Service shall periodically validate that the processes used and decisions made by the vehicle manufacturer are compliant, particularly for instances where the vehicle manufacturer chose not to notify the Approval Authority or its Technical Service about an update. This may be achieved on a sampling basis.

## **10. Penalties for non-conformity of production**

- 10.1. The approval granted in respect of a vehicle type pursuant to this Regulation may be withdrawn if the requirement laid down in this Regulation are not complied with or if sample vehicles fail to comply with the requirements of this Regulation.
- 10.2. If an Approval Authority withdraws an approval it has previously granted, it shall forthwith so notify the Contracting Parties applying this Regulation, by means of a communication form conforming to the model in Annex 2 to this Regulation.

## **11. Production definitively discontinued**

- 11.1. If the holder of the approval completely ceases to manufacture a type of vehicle approved in accordance with this Regulation, he shall so inform the authority which granted the approval. Upon receiving the relevant communication that authority shall inform thereof the other Contracting Parties to the Agreement applying this Regulation by means of a copy of the approval form bearing at the end, in large letters, the signed and dated annotation "PRODUCTION DISCONTINUED".

## **12. Names and addresses of Technical Services responsible for conducting approval test, and of Type Approval Authorities**

- 12.1. The Contracting Parties to the Agreement which apply this Regulation shall communicate to the United Nations Secretariat the names and addresses of the Technical Services responsible for conducting approval tests and of the Type Approval Authorities which grant approval and to which forms certifying approval or extension or refusal or withdrawal of approval, issued in other countries, are to be sent.

## Annex 1

### Information document

The following information, if applicable, shall be supplied in triplicate and include a list of contents. Any drawings shall be supplied in appropriate scale and in sufficient detail on size A4 or on a folder of A4 format. Photographs, if any, shall show sufficient detail.

1. Make (trade name of manufacturer): .....
2. Type and general commercial description(s): .....  
(Type is the type to be approved, commercial description refers to the product in which the approved type is used)
3. Means of identification of type, if marked on the vehicle: .....
4. Location of that marking: .....
5. Category(ies) of vehicle: .....
6. Name and address of manufacturer/ manufacturer's representative: .....
7. Name(s) and Address(es) of assembly plant(s): .....
8. Photograph(s) and/or drawing(s) of a representative vehicle: .....
9. Software Updates
  - 9.1. General construction characteristics of the vehicle type:.....
  - 9.2. The number of the Certificate of Compliance for Software Update Management System: .....
  - 9.3. Security measures.
    - 9.3.1. Documents for the vehicle type to be approved describing that the update process will be performed securely .....
    - 9.3.2. Documents for the vehicle type to be approved describing that the RXSWINs on a vehicle are protected against unauthorized manipulation .....
  - 9.4. Software updates over the air
    - 9.4.1. Documents for the vehicle type to be approved describing that the update process will be performed safely .....
    - 9.4.2. How a vehicle user is able to be informed about an update before and after its execution.....

## Annex 1 - Appendix 1

### Model of declaration of compliance for Software Update Management System

#### Manufacturer's declaration of compliance with the requirements for Software Update Management System

Manufacturer Name: .....

Manufacturer Address: .....

.....(Manufacturer Name) attests that the necessary processes to comply with the requirements for the Software Update Management System laid down in paragraph 7.1 of UN Regulation No. 156 are installed and will be maintained.

Done at: .....(place)

Date: .....

Name of the signatory: .....

Function of the signatory: .....

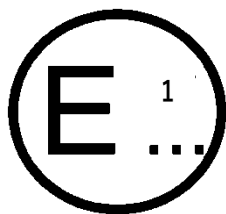
.....

(Stamp and signature of the manufacturer's representative)

## Annex 2

### Communication

(Maximum format: A4 (210 x 297 mm))



issued by: Name of administration:

.....  
.....  
.....

Concerning:<sup>2</sup> Approval granted  
Approval extended  
Approval withdrawn with effect from dd/mm/yyyy  
Approval refused  
Production definitively discontinued

of a vehicle type, pursuant to UN Regulation No. 156

Approval No.: .....

Extension No.: .....

Reason for extension: .....

1. Make (trade name of manufacturer): .....
2. Type and general commercial description(s) .....
3. Means of identification of type, if marked on the vehicle: .....
- 3.1. Location of that marking: .....
4. Category(ies) of vehicle: .....
5. Name and address of manufacturer / manufacturer's representative: .....
6. Name(s) and Address(es) of the production plant(s) .....
7. Number of the certificate of compliance for software update management system: ...
8. Software updates over the air included (Yes/no): .....
9. Technical Service responsible for carrying out the tests: .....
10. Date of test report: .....
11. Number of test report: .....
12. Remarks: (if any). .....
13. Place: .....
14. Date: .....
15. Signature: .....
16. The index to the information package lodged with the Approval Authority, which may be obtained on request is attached.

<sup>1</sup> Distinguishing number of the country which has granted/extended/refused/withdrawn approval (see marking provisions (footnote) in this Regulation).

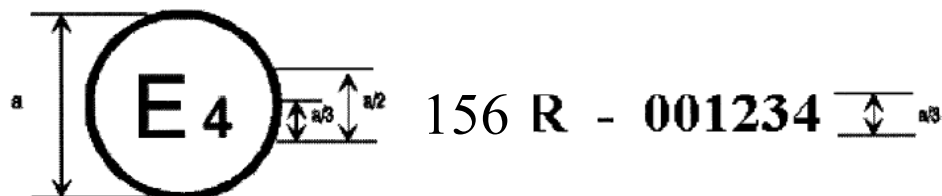
<sup>2</sup> Strike out what does not apply.

## Annex 3

### Arrangement of approval mark

#### Model A

(See paragraph 4.2 of this Regulation)



$a = 8 \text{ mm min.}$

The above approval mark affixed to a vehicle shows that the road vehicle type concerned has been approved in the Netherlands (E 4), pursuant to Regulation No. 156, and under the approval number 001234. The first two digits of the approval number indicate that the approval was granted in accordance with the requirements of this Regulation in its original form (00).



## Annex 4

### Model of Certificate of Compliance for Software Update Management System

#### CERTIFICATE OF COMPLIANCE FOR SOFTWARE UPDATE MANAGEMENT SYSTEM

With UN Regulation No. 156

Certificate Number [*Reference number*]

[..... *Approval Authority*]

Certifies that

Manufacturer: .....

Address of the manufacturer: .....

Complies with the provisions of Regulation No. [*this Regulation*]

Verifications have been performed on: .....

by (name and address of the Approval Authority): .....

Number of report:.....

The certificate is valid until: [.....*Date*]

Done at: [.....*Place*]

On: [.....*Date*]

[.....*Signature*]

---



# **UNECE R/155**

## **Reglamento R155 de la ONU sobre ciberseguridad y su impacto en los vehículos eléctricos**

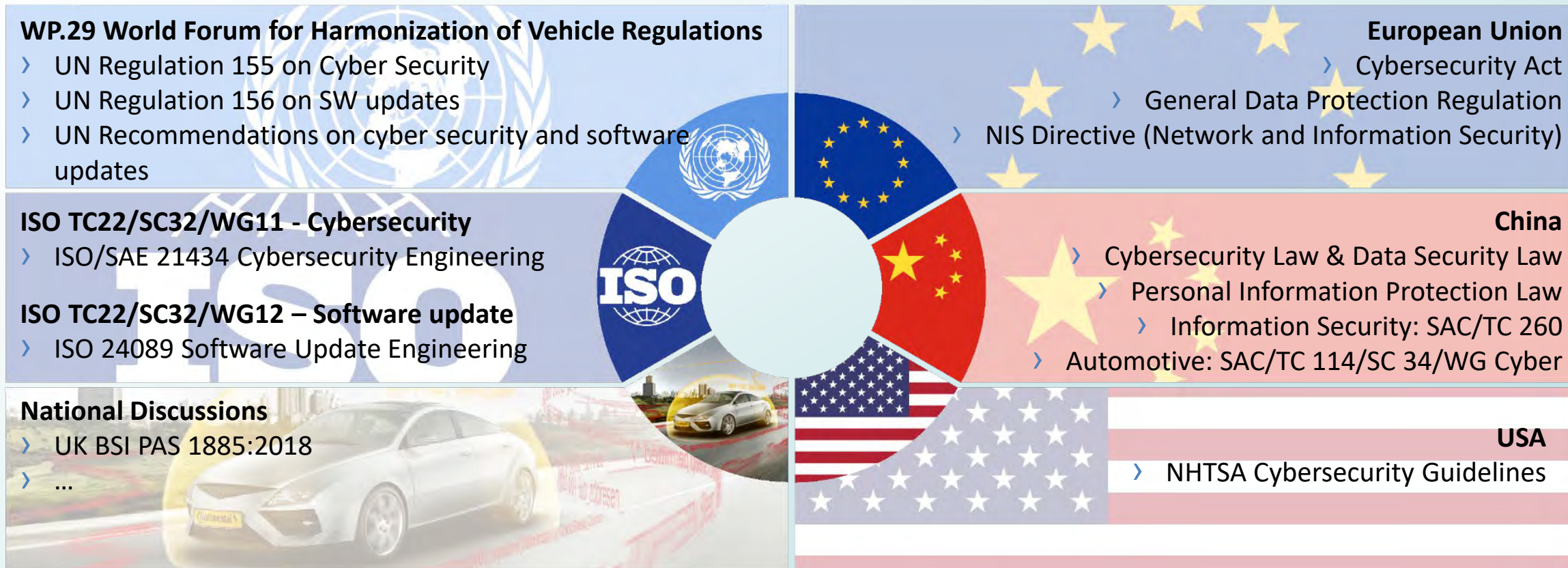


# UN REGULATION 155 ON CYBERSECURITY AND ITS IMPACT WITH REGARD TO ELECTRIC VEHICLES

Kai Frederik Zastrow, Senior Fellow Regulation Certification Standards (Stellantis)  
Pilot of Cluster 4 Cybersecurity & Software Updates, International Organization of Motor  
Vehicle Manufacturers (OICA), industry mirror of UNECE/GRVA/IWG CS&OTA



# Global Automotive Standards and Regulations to address Cybersecurity and SW updates



**UN Regulations (adopted in June 2020) are worldwide consensus:**

Developed under GRVA (chaired by Germany, Japan and China)

/ IWG Cybersecurity & OTA issues (chaired by UK, Japan and USA).

=> **Japan and European Union** are the first regions that make the regulations mandatory in their territory.



# Why cybersecurity regulation?

## ➤ Risk of cyberattacks

### ▪ **Safety/Security/Environmental impact:**

- Hacker may
  - o **be the vehicle user**
  - o **manipulate** existing vehicle software
  - o get access to **private/confidential data** (incl. location and charging history)
  - o use vehicle for **criminal actions**

### ▪ **Economic impact:**

- Economic risk for vehicle manufacturer, e.g. for recalls

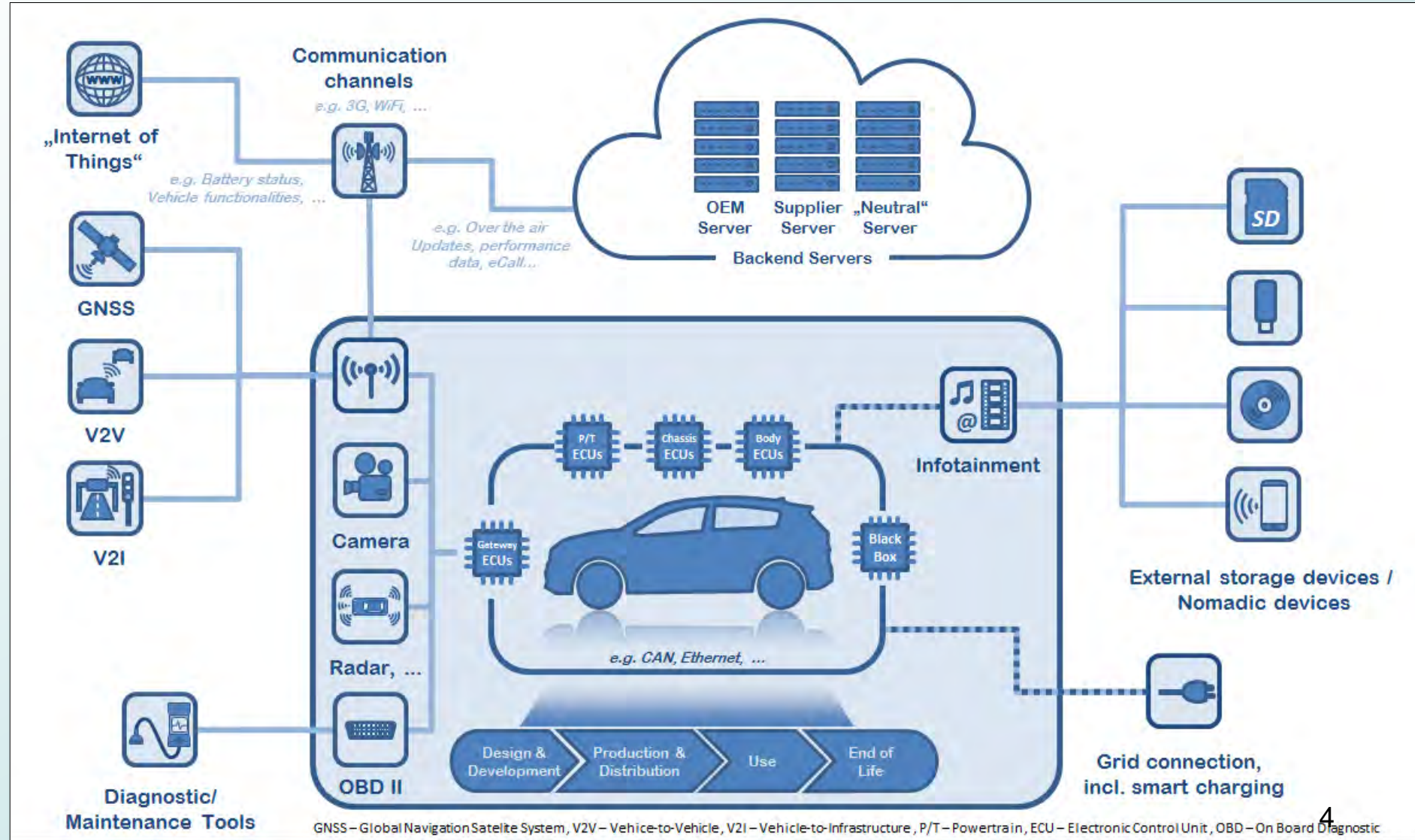
## ➤ Objective of the regulation

### ▪ **Protect the vehicle from cyber-attacks**





# @ Cybersecurity concerns the **whole vehicle**



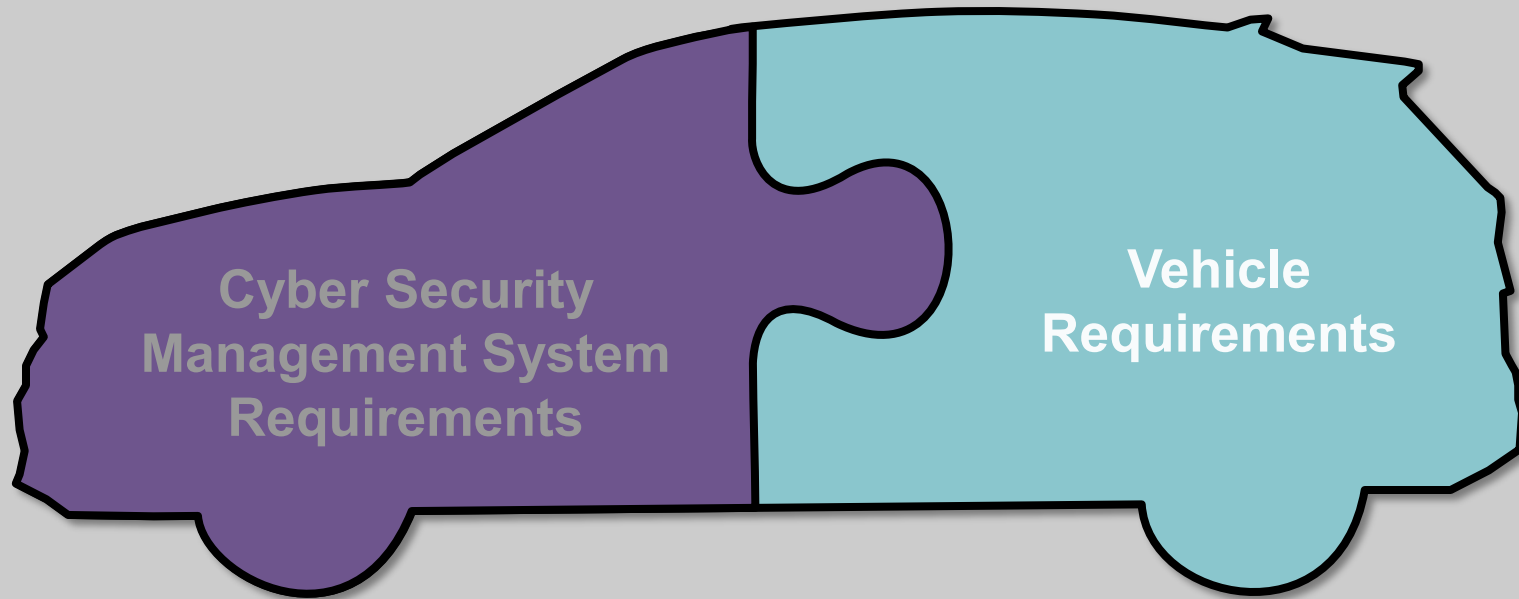
⇒ **Cybersecurity cannot be covered by certification of only some specific components**



# @ UN Regulation 155 on Automotive Cybersecurity

Split approach for the cybersecurity assessment:

- i) Assessment and certification of vehicle manufacturer **Cyber Security Management System**
- ii) Assessment and certification of **vehicles**



Organizational structure  
& processes

Design of the vehicle EE architecture,  
risk assessment and implementation  
of mitigations



## 7.2 Requirements for the CSMS Cyber Security Management System

7.2.2.1. Vehicle manufacturer shall demonstrate that their Cyber Security Management System considers:

- Development phase
- Production phase
- Post-production phase

Vehicle  
manufacturer

documentation

questions / audit

Authority/  
Technical Service

delivers

Certificate of  
Compliance of CSMS

7.2.2.2. Vehicle manufacturer shall demonstrate that processes used ensure security including:

- manage cyber security
- identification of risks to vehicle types (see Annex 5, part A)
- assessment, categorization and treatment of the risks identified
- verify that the risks identified are appropriately managed
- testing the security of the system
- ensuring that the risk assessment is kept current
- monitor for, detect and respond to cyber-attacks on vehicle types and assess whether the cyber security measures implemented are still effective
- Provide relevant data to support analyses of attempted or successful attacks

7.2.2.3. The vehicle manufacturer shall demonstrate that mitigation happen in a reasonable timeframe

7.2.2.4. The vehicle manufacturer shall demonstrate that monitoring of vehicles is continual.

7.2.2.5. The vehicle manufacturer shall demonstrate how he manages dependencies with contracted suppliers and service providers in regards of the requirements of paragraph 7.2.2.2





## 7.3. Requirements for vehicle types

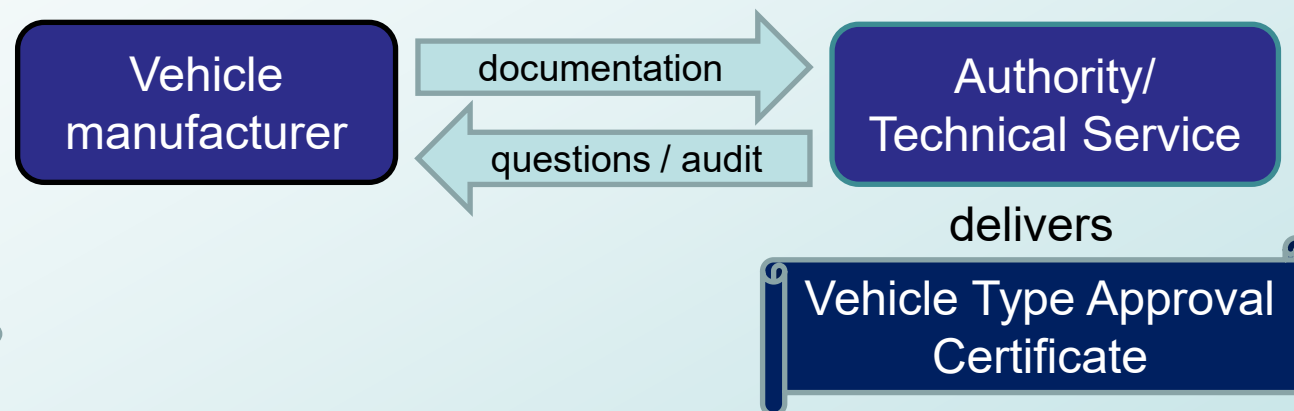
7.3.1. Vehicle manufacturer shall have valid Certificate of Compliance relevant to the vehicle type being approved.

7.3.2. Manufacturer shall identify and manage, for the vehicle type being approved, supplier-related risks

7.3.3. Vehicle manufacturer shall demonstrate an exhaustive risk assessment => Annex 5, part A

7.3.4. Vehicle manufacturer shall demonstrate proportionate mitigations => Annex 5, part B & C.

7.3.7. Vehicle manufacturer shall implement measures to detect and monitor cyber-attacks, provide data forensic for analysis of attempted attacks.



## 7.4 Monitoring and Reporting

7.4.1. Vehicle manufacturer shall report at least once a year, or more frequently if relevant, the outcome of the monitoring activities.

7.4.2. The Authority shall if necessary require to remedy any detected ineffectiveness. If the response is not sufficient, the CSMS may be withdrawn.



# Annex 5, Part A: List of threats

Table A1  
List of vulnerability or attack method related to the threats

| High level and sub-level descriptions of vulnerability/ threat            |   |                                                                      | Example of vulnerability or attack method |                                                                                                                                                             |
|---------------------------------------------------------------------------|---|----------------------------------------------------------------------|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.3.1 Threats regarding back-end servers related to vehicles in the field | 1 | Back-end servers used as a means to attack a vehicle or extract data | 1.1                                       | Abuse of privileges by staff ( <b>insider attack</b> )                                                                                                      |
|                                                                           |   |                                                                      | 1.2                                       | <b>Unauthorized internet access</b> to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means) |

| High level and sub-level descriptions of vulnerability/ threat                  |    |                                                                                                                                                                                                         | Example of vulnerability or attack method |                                                                                                                                     |
|---------------------------------------------------------------------------------|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| 4.3.5 Threats to vehicles regarding their external connectivity and connections | 16 | Manipulation of the connectivity of vehicle functions enables a cyber-attack, this can include telematics; systems that permit remote operations; and systems using short range wireless communications | 16.1                                      | Manipulation of <b>functions designed to remotely operate systems</b> , such as remote key, immobilizer, and charging pile          |
|                                                                                 |    |                                                                                                                                                                                                         | 16.2                                      | <b>Manipulation of vehicle telematics</b> (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors) |
|                                                                                 |    |                                                                                                                                                                                                         | 16.3                                      | Interference with <b>short range wireless systems</b> or sensors                                                                    |





# Annex 5, Part B: Mitigations on vehicles

Table B1

**Mitigation to the threats which are related to "Vehicle communication channels"**

| <i>Table A1 reference</i> | <i>Threats to "Vehicle communication channels"</i> | <i>Ref</i> | <i>Mitigation</i>                             |
|---------------------------|----------------------------------------------------|------------|-----------------------------------------------|
| 4.1                       | Spoofing of messages (e.g. 802.11p                 | M10        | The vehicle shall verify the authenticity and |

| <i>Table A1 reference</i> | <i>Threats to "External connectivity and connections"</i>                                                                    | <i>Ref</i> | <i>Mitigation</i>                                                     |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------|------------|-----------------------------------------------------------------------|
| 16.1                      | Manipulation of functions designed to remotely operate vehicle systems, such as remote key, immobiliser, and charging pile   | M20        | Security controls shall be applied to systems that have remote access |
| 16.2                      | Manipulation of vehicle telematics (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors) |            |                                                                       |
| 16.3                      | Interference with short range wireless systems or sensors                                                                    |            |                                                                       |



# Annex 5, Part C: Mitigations outside the vehicle

Table C1

Mitigations to the threats which are related to "Back-end servers"

| <i>Table A1 reference</i> | <i>Threats to "Back-end servers"</i>                                                                                                                 | <i>Ref</i> | <i>Mitigation</i>                                                                                                                                                                                                         |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.1 & 3.1                 | Abuse of privileges by staff (insider attack)                                                                                                        | M1         | Security Controls are applied to back-end systems to minimise the risk of insider attack                                                                                                                                  |
| 1.2 & 3.3                 | Unauthorised internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means) | M2         | Security Controls are applied to back-end systems to minimise unauthorised access. Example Security Controls can be found in OWASP                                                                                        |
| 1.3 & 3.4                 | Unauthorised physical access to the server (conducted by for example USB sticks or other media connecting to the server)                             | M8         | Through system design and access control it should not be possible for unauthorised personnel to access personal or system critical data                                                                                  |
| 2.1                       | Attack on back-end server stops it functioning, for example it prevents it from interacting with vehicles and providing services they rely on        | M3         | Security Controls are applied to back-end systems. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage. Example Security Controls can be found in OWASP |
| 2.2                       | Insider staff access to the back-end                                                                                                                 | M4         | Security Controls are applied to back-end systems                                                                                                                                                                         |



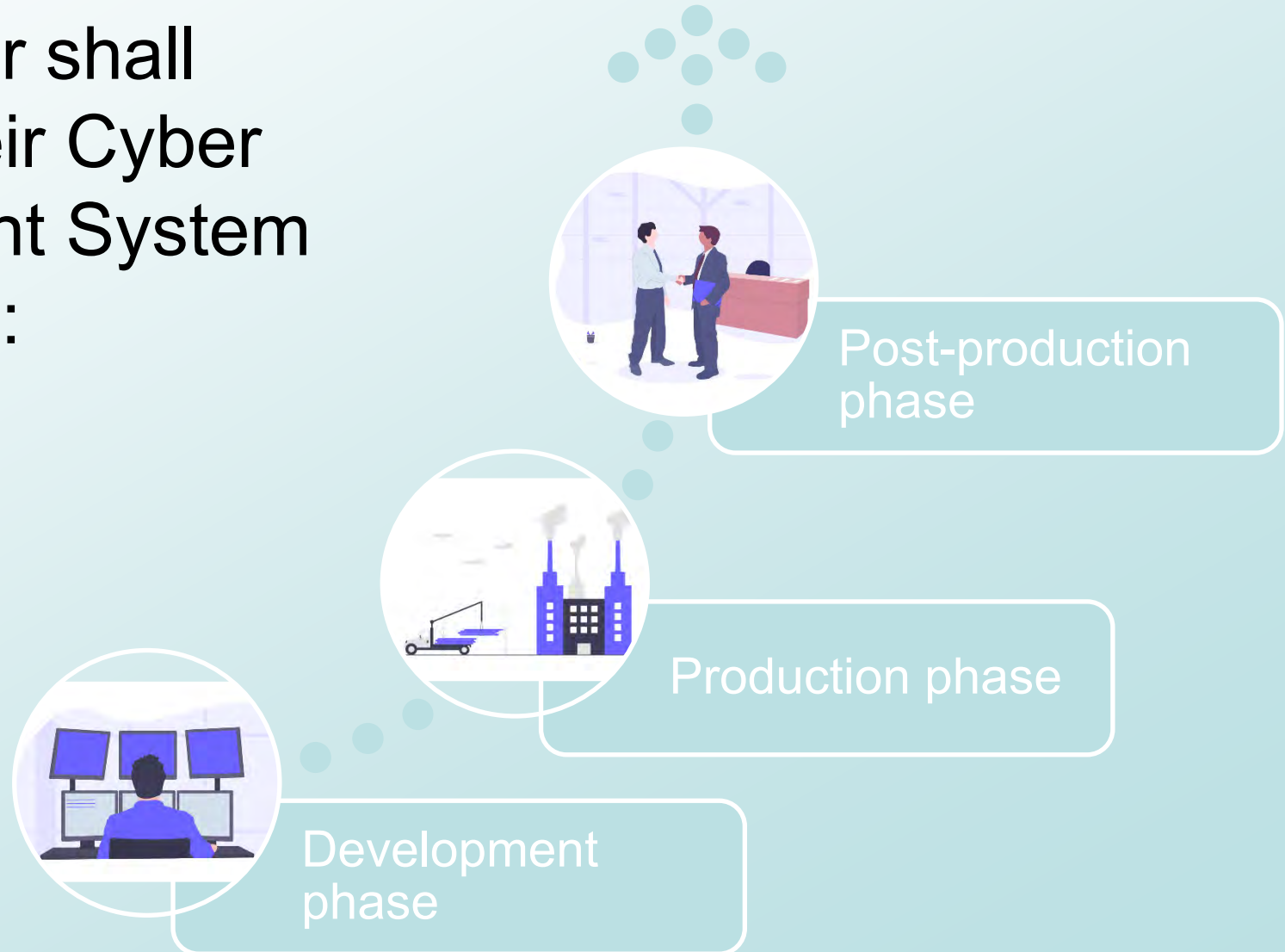
# Requirements for the whole vehicle life cycle

➤ Vehicle manufacturer shall demonstrate that their Cyber Security Management System considers (§ 7.2.2.1):

a) Development phase

b) Production phase

c) Post-production phase







# Conclusions



- UN R155 requires an exhaustive cybersecurity risk analysis and the implementation of appropriate mitigations.
- Cyberattacks must be reported to the approval authority.
- As more and more vehicles will be type approved according to R155 (mandatory for all first vehicle registrations from July 2024 in Japan & European Union), the reports to approval authorities will show the part of cyberattacks via the electric charging interface.
- According to those reports, additional measures may be introduced.
- UN R155 is part of a broader effort to address the cybersecurity challenges associated with the increasing connectivity and complexity of vehicles, including EVs. All stakeholders are expected to work together to implement and enforce these cybersecurity measures.



**ANNEX**



# Link to UN documents

- UN Regulation 155 Cybersecurity <https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security>
- Interpretation document on Cybersecurity <https://unece.org/sites/default/files/2022-04/ECE-TRANS-WP.29-2022-61e.pdf>
- UN Regulation 156 SW update <https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update>
- Interpretation document on SW update <http://unece.org/sites/default/files/2020-12/ECE-TRANS-WP29-2021-060e.pdf>
- Recommendations on uniform provisions concerning cyber security and software updates <https://unece.org/sites/default/files/2022-04/ECE-TRANS-WP.29-2022-60e.pdf>
- UN Regulation 157 ALKS (see chapter 9 with link to UN Regulations 155 and 156 and Annex point 19) <https://unece.org/transport/documents/2021/03/standards/un-regulation-no-157-automated-lane-keeping-systems-alks>
- Consolidated Resolution on the Construction of Vehicles (R.E.3), Annex 7: Provisions on Software Identification Numbers (integration of RXSWIN in system regulations) <http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29/ECE-TRANS-WP29-2020-082e.pdf>





# ISO 15118 Vehicle to grid communication interface

ISO/TC 22/SC 31 “Data communication” developed a series of standards for charging/discharging “Vehicle to grid communication interface”

- ISO 15118-1: General information and use-case definition
- ISO 15118-2: Network and application protocol requirements (TLS Transport Layer Security 1.2)
- ISO 15118-3: Physical and data link layer requirements
- ISO 15118-4: Network and application protocol conformance test
- ISO 15118-5: Physical and data link layer conformance test
- ISO 15118-6: Physical and data link layer requirements for differential Power Line Communication
- ISO 15118-8: Physical layer and data link layer requirements for wireless communication
- ISO 15118-9: Physical and data link layer conformance test for wireless communication
- ISO 15118-10: Physical layer and data link layer requirements for wired ethernet communication
- ISO 15118-20: 2nd generation network and application protocol requirements (TLS 1.3 ; bi-directional charging possible)

This standard (parts 2 & 20) includes secure communication protocols between the vehicle and the charging station.



# IEC 61851 Electric vehicle charging system

IEC TC 69 developed a series of standards for electric vehicle conductive charging systems

- IEC 61851 covers the mechanical, electrical, communications, EMC and performance requirements for EV supply equipment used to charge electric vehicles, including light electric vehicles.
- IEC 61851 is divided into several parts as follows:
  - Part 1: General Requirements,
  - Part 21-14: Electric vehicle onboard charger EMC requirements for conductive connection to an AC/DC supply.
  - Part 21-25: EMC requirements for OFF board electric vehicle charging systems.
  - Part 23: DC electric vehicle charging station
  - Part 24: Digital communication between a DC EV charging station and an electric vehicle
  - for control of DC charging



# Thank you!





**Reglamento nº155 de la  
Comisión Económica para  
Europa (CEPE) de las  
Naciones Unidas //**  
**Disposiciones uniformes  
relativas a la homologación de  
los vehículos de motor en lo  
que respecta a la  
ciberseguridad y al sistema de  
gestión de esta [2021/387]**

Solo los textos originales de la CEPE surten efectos jurídicos con arreglo al Derecho internacional público. La situación y la fecha de entrada en vigor del presente Reglamento deben verificarse en la última versión del documento de situación de la CEPE TRANS/WP.29/343, disponible en:  
<http://www.unece.org/trans/main/wp29/wp29wgs/wp29gen/wp29docstts.html>

**Reglamento n.º 155 de la Comisión Económica para Europa (CEPE) de las Naciones Unidas —  
Disposiciones uniformes relativas a la homologación de los vehículos de motor en lo que respecta a la  
ciberseguridad y al sistema de gestión de esta [2021/387]**

Fecha de entrada en vigor: 22 de enero de 2021

El presente documento tiene valor meramente informativo. Los textos auténticos y jurídicamente vinculantes son los siguientes:

- ECE/TRANS/WP.29/2020/79
- ECE/TRANS/WP.29/2020/94 y
- ECE/TRANS/WP.29/2020/97

ÍNDICE

REGLAMENTO

1. Ámbito de aplicación
2. Definiciones
3. Solicitud de homologación
4. Marcados
5. Homologación
6. Certificado de conformidad del sistema de gestión de la ciberseguridad
7. Especificaciones
8. Modificación del tipo de vehículo y extensión de la homologación de tipo
9. Conformidad de la producción
10. Sanciones por falta de conformidad de la producción
11. Cese definitivo de la producción
12. Nombres y direcciones de los servicios técnicos responsables de realizar los ensayos de homologación y de las autoridades de homologación de tipo

ANEXOS

- 1 Ficha técnica
- 2 Comunicación
- 3 Disposición de la marca de homologación
- 4 Modelo de certificado de conformidad del sistema de gestión de la ciberseguridad
- 5 Lista de amenazas y sus correspondientes medidas de mitigación

1. ÁMBITO DE APLICACIÓN

- 1.1. El presente Reglamento es aplicable a los vehículos de las categorías M y N, en lo que respecta a la ciberseguridad.  
El presente Reglamento es aplicable también a los vehículos de la categoría O si llevan instalada al menos una unidad de control electrónico.



- 1.2. Asimismo, el presente Reglamento es aplicable a los vehículos de las Categorías L<sub>6</sub> y L<sub>7</sub> si están equipados con funciones de conducción automatizada desde el nivel 3 en adelante, tal y como se definen en el «Documento de referencia en el que se proponen las definiciones de la conducción automatizada en el marco del Grupo de Trabajo 29 (WP.29) y de los principios generales para la elaboración de un Reglamento de las Naciones Unidas sobre los vehículos automatizados» (ECE/TRANS/WP.29/1140).
- 1.3. El presente Reglamento debe entenderse sin perjuicio de otros Reglamentos de las Naciones Unidas, de la legislación regional o nacional que rige el acceso de partes autorizadas al vehículo, sus datos, funciones y recursos, así como las condiciones de dicho acceso. Se entenderá también sin perjuicio de la aplicación de la legislación nacional y regional en materia de privacidad y protección de las personas físicas con respecto al tratamiento de sus datos personales.
- 1.4. El presente Reglamento se entenderá sin perjuicio de otros Reglamentos de las Naciones Unidas y de la legislación nacional o regional por los que se rigen el desarrollo y la instalación o la integración de sistemas de sustitución de piezas y componentes, físicos y digitales, con respecto a la ciberseguridad.

## 2. DEFINICIONES

A los efectos del presente Reglamento, se entenderá por:

- 2.1. «Tipo de vehículo»: los vehículos que no difieran entre sí en al menos los siguientes aspectos esenciales:
  - a) la designación del tipo de vehículo dada por el fabricante;
  - b) aspectos esenciales de la arquitectura eléctrica y electrónica y las interfaces externas con respecto a la ciberseguridad;
- 2.2. «Ciberseguridad»: la condición en la cual los vehículos de carretera y sus funciones se encuentran protegidos de ciberamenazas a sus componentes eléctricos o electrónicos.
- 2.3. «Sistema de gestión de la ciberseguridad»: un enfoque sistemático basado en el riesgo, por el que se definen los procesos organizativos, las responsabilidades y la gobernanza para abordar los riesgos asociados con las ciberamenazas a los vehículos y para protegerlos de ciberataques.
- 2.4. «Sistema»: conjunto de componentes o subsistemas que ejecuta una función o funciones.
- 2.5. «Fase de desarrollo»: periodo que precede a la homologación de tipo de un tipo de vehículo.
- 2.6. «Fase de producción»: duración de la producción de un tipo de vehículo.
- 2.7. «Fase de posproducción»: período que transcurre entre el momento en que un tipo de vehículo se deja de producir y el final de la vida útil de todos los vehículos de dicho tipo. Los vehículos que incorporan un tipo de vehículo específico seguirán funcionando durante esta fase, pero dejarán de producirse. La fase concluye cuando ya no hay vehículos de un tipo de vehículo concreto en funcionamiento.
- 2.8. «Medida de mitigación»: una medida que contribuye a reducir los riesgos.
- 2.9. «Riesgo»: la posibilidad de que una determinada amenaza se aproveche de las vulnerabilidades de un vehículo y, al hacerlo, ocasione daños a la organización o a una persona.
- 2.10. «Evaluación de riesgos»: proceso general de detección, reconocimiento y descripción de los riesgos (identificación del riesgo) con vistas a comprender la naturaleza del riesgo y determinar su nivel (análisis del riesgo), y a comparar los resultados del análisis del riesgo con los criterios de riesgo para determinar si este y su magnitud son aceptables o tolerables (valoración de riesgos).
- 2.11. «Gestión del riesgo»: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- 2.12. «Amenaza»: la posible causa de un incidente no deseado que pueda ocasionar daños a un sistema, una organización o una persona.
- 2.13. «Vulnerabilidad»: una debilidad de un elemento o de una medida de mitigación que pueda ser aprovechada por una o varias amenazas.

## 3. SOLICITUD DE HOMOLOGACIÓN

- 3.1. La solicitud de homologación de un tipo de vehículo en lo que concierne a la ciberseguridad será presentada por el fabricante del vehículo o por su representante debidamente acreditado.

- 3.2. Deberá ir acompañada de los documentos que se mencionan a continuación, por triplicado, así como de los elementos siguientes:
- 3.2.1. una descripción del tipo de vehículo en lo que concierne a los aspectos especificados en el anexo 1 del presente Reglamento.
- 3.2.2. En los casos en que dicha información resulte estar cubierta por derechos de propiedad industrial o esté constituida por conocimientos especializados del fabricante o sus proveedores, el fabricante o sus proveedores facilitarán información suficiente para que puedan realizarse correctamente los ensayos a que se refiere el presente Reglamento. Dicha información se tratará de forma confidencial.
- 3.2.3. El certificado de conformidad para sistemas de gestión de la ciberseguridad con arreglo al punto 6 del presente Reglamento.
- 3.3. La documentación deberá estar disponible en dos partes:
- a) la documentación oficial para la homologación, que contendrá el material especificado en el anexo 1, se presentará a la autoridad de homologación o a su servicio técnico cuando se presente la solicitud de homologación de tipo. La autoridad de homologación o su servicio técnico utilizarán dicha información como la referencia básica para el proceso de homologación. La autoridad de homologación o su servicio técnico se asegurarán de que esta documentación esté disponible durante al menos diez años a partir del momento en el que se interrumpa definitivamente la producción del tipo de vehículo;
- b) el material adicional pertinente para los requisitos del presente Reglamento, que podrá conservar el fabricante, pero que se presentará a inspección en el momento de la homologación de tipo. El fabricante garantizará que todo material presentado a inspección en el momento de la homologación de tipo esté disponible durante un período mínimo de diez años a partir del momento en el que se interrumpa definitivamente la producción del tipo de vehículo.
4. MARCADO
- 4.1. Se colocará una marca de homologación internacional, de manera visible y en un lugar fácilmente accesible especificado en el formulario de homologación, en cada vehículo que se ajuste a un tipo de vehículo homologado con arreglo al presente Reglamento; la marca consistirá en:
- 4.1.1. La letra mayúscula «E» dentro de un círculo seguida del número distintivo del país que ha concedido la homologación.
- 4.1.2. El número del presente Reglamento, seguido de la letra «R», un guion y el número de homologación a la derecha del círculo descrito en el punto 4.1.1.
- 4.2. Si el vehículo se ajusta a un tipo de vehículo homologado de acuerdo con uno o varios Reglamentos adjuntos al Acuerdo en el país que haya concedido la homologación con arreglo al presente Reglamento, no es necesario repetir el símbolo que se establece en el punto 4.1.1; en ese caso, el Reglamento, los números de homologación y los símbolos adicionales de todos los Reglamentos según los cuales se ha concedido la homologación en el país que la concedió de conformidad con el presente Reglamento se colocarán en columnas verticales a la derecha del símbolo exigido en el punto 4.1.1.
- 4.3. La marca de homologación aparecerá claramente legible y será indeleble.
- 4.4. La marca de homologación se situará en la placa informativa del vehículo colocada por el fabricante, o cerca de la misma.
- 4.5. En el anexo 3 del presente Reglamento figuran algunos ejemplos de las marcas de homologación.
5. HOMOLOGACIÓN
- 5.1. Las autoridades de homologación concederán, cuando proceda, la homologación de tipo en lo que concierne a la ciberseguridad únicamente a los tipos de vehículos que cumplan los requisitos previstos en el presente Reglamento.



- 5.1.1. La autoridad de homologación o el servicio técnico verificarán mediante el control de los documentos que el fabricante del vehículo haya adoptado las medidas necesarias con respecto al tipo de vehículo a fin de:
- a) recopilar y verificar la información requerida en virtud del presente Reglamento a través de la cadena de suministro a fin de constatar que se detectan y gestionan los riesgos relacionados con los proveedores;
  - b) documentar la evaluación de riesgos (realizada durante la fase de desarrollo o con carácter retrospectivo), los resultados de los ensayos y las medidas de mitigación aplicadas al tipo de vehículo, incluida la información relativa al diseño que respalde la evaluación de riesgos;
  - c) aplicar las medidas de ciberseguridad adecuadas al diseño del tipo de vehículo;
  - d) detectar los posibles ataques a la ciberseguridad y responder a ellos;
  - e) registrar los datos para facilitar la detección de ciberataques y proporcionar capacidad forense en relación con los datos a fin de permitir el análisis de los intentos de ciberataques o de los ciberataques consumados.
- 5.1.2. La autoridad de homologación o el servicio técnico verificará, mediante ensayos en un vehículo del tipo de vehículo que su fabricante haya aplicado, las medidas de ciberseguridad que ha documentado. Los ensayos los realizarán la autoridad de homologación o el servicio técnico, por sí mismos o en colaboración con el fabricante del vehículo mediante un muestreo. El muestreo se centrará, entre otros, en los riesgos que se consideraron altos durante la evaluación de riesgos.
- 5.1.3. La autoridad de homologación o el servicio técnico denegarán la concesión de la homologación de tipo en lo que respecta a la ciberseguridad cuando el fabricante del vehículo no cumpla uno o varios de los requisitos a que se refiere el punto 7.3, en particular si:
- a) el fabricante del vehículo no ha realizado la evaluación exhaustiva de riesgos a que se refiere el punto 7.3.3, incluso en caso de que el fabricante no haya considerado todos los riesgos relacionados con las amenazas a que se refiere la parte A del anexo 5;
  - b) el fabricante del vehículo no ha protegido el tipo de vehículo contra los riesgos detectados en la evaluación de riesgos del fabricante del vehículo o no ha aplicado las medidas de mitigación tal y como requiere el punto 7;
  - c) el fabricante del vehículo no ha adoptado medidas adecuadas y proporcionadas para garantizar entornos específicos del tipo de vehículo (si se incluyen) para el almacenamiento y la ejecución del *software*, los servicios, las aplicaciones o los datos posventa;
  - d) el fabricante del vehículo no ha realizado, antes de la homologación, ensayos adecuados y suficientes para verificar la eficacia de las medidas de seguridad aplicadas.
- 5.1.4. La autoridad de homologación que realiza la evaluación también denegará la concesión de la homologación de tipo en lo que respecta a la ciberseguridad cuando dicha autoridad o el servicio técnico no hayan recibido información suficiente del fabricante del vehículo para evaluar la ciberseguridad del tipo de vehículo.
- 5.2. La concesión, la extensión o la denegación de la homologación de un tipo de vehículo con arreglo al presente Reglamento se comunicará a las Partes contratantes en el Acuerdo de 1958 que apliquen el presente Reglamento por medio de un formulario que se ajuste al modelo que figura en su anexo 2.
- 5.3. Las autoridades de homologación no concederán ninguna homologación de tipo sin verificar que el fabricante haya establecido disposiciones y procedimientos satisfactorios para gestionar correctamente los aspectos de ciberseguridad contemplados en el presente Reglamento.
- 5.3.1. La autoridad de homologación y sus servicios técnicos se asegurarán de que, además de cumplir los criterios establecidos en el anexo 2 del Acuerdo de 1958, también cuentan con:
- a) personal competente con capacidades de ciberseguridad adecuadas y conocimientos específicos sobre evaluaciones de riesgos en el ámbito de la automoción <sup>(1)</sup>;
  - b) procedimientos para realizar la evaluación uniforme que se prevé en el presente Reglamento.

(1) Por ejemplo, ISO 26262-2018, ISO/PAS 21448 e ISO/SAE 21434.

- 5.3.2. Cada Parte contratante que aplique el presente Reglamento notificará e informará mediante su autoridad de homologación a otras autoridades de homologación de las Partes contratantes que apliquen el presente Reglamento de Naciones Unidas sobre el método y los criterios que la autoridad de notificación ha tomado como base para evaluar la idoneidad de las medidas adoptadas de acuerdo con el presente Reglamento, en particular con los puntos 5.1, 7.2 y 7.3.

Esta información se compartirá: a) únicamente antes de conceder por primera vez una homologación de conformidad con el presente Reglamento y b) cada vez que se actualicen el método o los criterios de evaluación.

El objeto de intercambiar esta información es recoger y analizar las mejores prácticas a fin de garantizar la aplicación convergente del presente Reglamento por parte de todas las autoridades de homologación que lo apliquen.

- 5.3.3. La información a que se refiere el punto 5.3.2 se incorporará, en inglés, a la base de datos segura de Internet «DETA» <sup>(2)</sup>, creada por la Comisión Económica para Europa de las Naciones Unidas, a su debido tiempo y a más tardar catorce días antes de que se conceda una homologación por primera vez con arreglo a los métodos y criterios de evaluación correspondientes. La información será suficiente para entender los niveles de rendimiento mínimos adoptados por la autoridad de homologación para cada requisito específico a que se refiere el punto 5.3.2, así como los procesos y las medidas que aplica para verificar que se cumplen dichos niveles <sup>(3)</sup>.
- 5.3.4. Las autoridades de homologación que reciben la información a que se refiere el punto 5.3.2 podrán formular observaciones a la autoridad de homologación notificante, incorporándolas a la base de datos DETA en los catorce días posteriores a la notificación.
- 5.3.5. Si la autoridad de homologación otorgante no puede tener en cuenta las observaciones recibidas de acuerdo con el punto 5.3.4, las autoridades de homologación que hayan enviado las observaciones y la autoridad de homologación otorgante solicitarán aclaraciones adicionales de conformidad con el anexo 6 del Acuerdo de 1958. El correspondiente Grupo de trabajo auxiliar <sup>(4)</sup> del Foro Mundial para la Armonización de la Reglamentación sobre Vehículos (WP.29) para el presente Reglamento acordará una interpretación común de los métodos y los criterios de evaluación <sup>(5)</sup>. Se aplicará dicha interpretación común y todas las autoridades de homologación expedirán en consecuencia homologaciones de tipo en virtud del presente Reglamento.
- 5.3.6. Cada autoridad de homologación que conceda una homologación de tipo con arreglo al presente Reglamento notificará a otras autoridades de homologación la homologación concedida. La autoridad de homologación incorporará la homologación de tipo junto con la documentación complementaria, en lengua inglesa, a la base de datos DETA en un plazo de catorce días a partir de la fecha de concesión de la homologación <sup>(6)</sup>.
- 5.3.7. Las Partes contratantes podrán estudiar las homologaciones concedidas sobre la base de la información incorporada con arreglo al punto 5.3.6. En caso de que haya opiniones divergentes entre las Partes contratantes, estas se resolverán de acuerdo con el artículo 10 y el anexo 6 del Acuerdo de 1958. Las Partes contratantes también informarán al correspondiente Grupo de trabajo auxiliar del Foro Mundial para la Armonización de la Reglamentación sobre Vehículos (WP.29) sobre las interpretaciones divergentes en el sentido del anexo 6 del Acuerdo de 1958. El Grupo de trabajo pertinente asistirá en la conciliación de las opiniones divergentes y podrá consultar con el WP.29 sobre este punto si fuera necesario.
- 5.4. A efectos del punto 7.2 del presente Reglamento, el fabricante velará por que se apliquen los aspectos de ciberseguridad contemplados en el presente Reglamento.

(2) <https://www.unece.org/trans/main/wp29/datasharing.html>

(3) Las orientaciones sobre la información detallada (p. ej., el método, los criterios y el nivel de rendimiento) que debe incorporarse, así como el formato, se facilitarán en el documento interpretativo que el Grupo de estudio sobre ciberseguridad y cuestiones de transmisión inalámbrica está elaborando para la séptima sesión del Grupo de trabajo sobre vehículos automatizados/autónomos y conectados (GRVA).

(4) El Grupo de trabajo sobre vehículos automatizados/autónomos y conectados (GRVA).

(5) Esta interpretación se reflejará en el documento interpretativo a que se refiere la nota a pie de página del punto 5.3.3.

(6) El GRVA elaborará más información sobre los requisitos mínimos de documentación durante su séptima sesión.

6. CERTIFICADO DE CONFORMIDAD DEL SISTEMA DE GESTIÓN DE LA CIBERSEGURIDAD
  - 6.1. Las Partes contratantes designarán una autoridad de homologación para que lleve a cabo la evaluación del fabricante y expida un certificado de conformidad del sistema de gestión de la ciberseguridad.
  - 6.2. La solicitud de un certificado de conformidad del sistema de gestión de la ciberseguridad será presentada por el fabricante del vehículo o por su representante debidamente acreditado.
  - 6.3. Dicha solicitud deberá ir acompañada de los documentos que se mencionan a continuación, por triplicado, así como de los elementos siguientes:
    - 6.3.1. documentos que describan el sistema de gestión de la ciberseguridad;
    - 6.3.2. una declaración firmada conforme al modelo definido en el apéndice 1 del anexo 1.
  - 6.4. En el contexto de la evaluación, el fabricante declarará haber utilizado el modelo definido en el apéndice 1 del anexo 1, y demostrará a satisfacción de la autoridad de homologación o de su servicio técnico que cuenta con los procesos necesarios para cumplir todos los requisitos del presente Reglamento en lo que respecta a la ciberseguridad.
  - 6.5. Cuando dicha evaluación se haya realizado de forma satisfactoria y se haya recibido una declaración firmada del fabricante conforme al modelo definido en el apéndice 1 del anexo 1, se otorgará al fabricante un certificado de conformidad del sistema de gestión de la ciberseguridad tal y como se describe en el anexo 4 del presente Reglamento.
  - 6.6. La autoridad de homologación o su servicio técnico utilizarán el modelo establecido en el anexo 4 del presente Reglamento para el certificado de conformidad del sistema de gestión de la ciberseguridad.
  - 6.7. El certificado de conformidad del sistema de gestión de la ciberseguridad tendrá una validez de un máximo de tres años a partir de la fecha de su expedición, a menos que sea retirado.
  - 6.8. La autoridad de homologación que haya concedido el certificado de conformidad del sistema de gestión de la ciberseguridad podrá verificar, en cualquier momento, que se siguen cumpliendo los requisitos para su concesión. La autoridad de homologación retirará dicho certificado si dejan de cumplirse los requisitos establecidos en el presente Reglamento.
  - 6.9. El fabricante informará a la autoridad de homologación o a su servicio técnico de cualquier modificación que afecte a la pertinencia del certificado de conformidad del sistema de gestión de la ciberseguridad. Tras consultar al fabricante, la autoridad de homologación o su servicio técnico decidirán si es necesario realizar nuevos controles.
  - 6.10. A su debido tiempo, permitiendo a la autoridad de homologación completar su evaluación antes del fin del período de validez del certificado de conformidad del sistema de gestión de la ciberseguridad, el fabricante solicitará uno nuevo o la extensión de un certificado existente. Tras una evaluación positiva, la autoridad de homologación expedirá un nuevo certificado de conformidad del sistema de gestión de la ciberseguridad o ampliará la validez del existente durante un periodo adicional de tres años. La autoridad de homologación verificará que el sistema de gestión de la ciberseguridad sigue cumpliendo los requisitos del presente Reglamento. La autoridad de homologación expedirá un nuevo certificado cuando ella o su servicio técnico hayan tenido conocimiento de cambios y dichos cambios se hayan reevaluado de forma positiva.
  - 6.11. El vencimiento o la retirada del certificado de conformidad del sistema de gestión de la ciberseguridad del fabricante se considerarán, en lo que respecta a los tipos de vehículos para los que es pertinente el sistema de gestión de la ciberseguridad, una modificación de la homologación a que se refiere el punto 8, que podrá incluir la retirada de la homologación si han dejado de cumplirse las condiciones para su concesión.

## 7. ESPECIFICACIONES

### 7.1. Especificaciones generales

7.1.1. Los requisitos del presente Reglamento no limitarán las disposiciones o los requisitos de otros Reglamentos de las Naciones Unidas.

### 7.2. Requisitos relativos al sistema de gestión de la ciberseguridad

7.2.1. Para la evaluación, la autoridad de homologación o su servicio técnico verificarán que el fabricante del vehículo cuenta con un sistema de gestión de la ciberseguridad, así como la conformidad de dicho sistema con el presente Reglamento.

7.2.2. El sistema de gestión de la ciberseguridad cubrirá los siguientes aspectos:

7.2.2.1. el fabricante del vehículo demostrará a una autoridad de homologación o servicio técnico que su sistema de gestión de la ciberseguridad se aplica a las siguientes fases:

- a) la fase de desarrollo;
- b) la fase de producción;
- c) la fase de posproducción.

7.2.2.2. El fabricante del vehículo demostrará que los procesos utilizados en su sistema de gestión de la ciberseguridad garantizan una consideración adecuada de la seguridad, incluidos los riesgos y las medidas de mitigación enumerados en el anexo 5. Se considerarán:

- a) los procesos utilizados en la organización del fabricante para gestionar la ciberseguridad;
- b) los procesos utilizados para detectar los riesgos para los tipos de vehículos. Dentro de dichos procesos, se tendrán en cuenta las amenazas indicadas en la parte A del anexo 5 y otras amenazas pertinentes;
- c) los procesos utilizados para la evaluación, la clasificación y el tratamiento de los riesgos detectados;
- d) los procesos existentes para verificar que los riesgos detectados se gestionan adecuadamente;
- e) los procesos utilizados para comprobar la ciberseguridad de un tipo de vehículo;
- f) los procesos utilizados para garantizar que la evaluación de riesgos se mantiene actualizada;
- g) los procesos utilizados para supervisar, detectar y responder a los ciberataques, las ciberamenazas y las vulnerabilidades que afectan a los tipos de vehículos, y los procesos utilizados para determinar si las medidas de ciberseguridad siguen siendo eficaces a la luz de nuevas las ciberamenazas y vulnerabilidades que se han detectado;
- h) los procesos utilizados para facilitar los datos pertinentes que respalden el análisis de los intentos de ciberataques o de los ciberataques consumados.

7.2.2.3. El fabricante del vehículo demostrará que los procesos utilizados en su sistema de gestión de la ciberseguridad garantizarán que, sobre la base de la clasificación a que se refiere el punto 7.2.2.2, letras c) y g), las ciberamenazas y las vulnerabilidades que requieren por su parte se mitigan en un plazo razonable.

7.2.2.4. El fabricante del vehículo demostrará que los procesos utilizados en el marco de su sistema de gestión de la ciberseguridad garantizarán que la supervisión a que se refiere el punto 7.2.2.2, letra g), sea continua. Esta condición:

- a) incluirá en la supervisión los vehículos después de la primera matriculación;
- b) incluirá la capacidad para analizar y detectar ciberamenazas, vulnerabilidades y ciberataques a partir de los datos del vehículo y de los registros del vehículo. Esta capacidad respetará el punto 1.3 y los derechos de privacidad de los propietarios o los conductores del vehículo, en particular en lo referente al consentimiento.

7.2.2.5. El fabricante del vehículo deberá mostrar la forma en que su sistema de gestión de la ciberseguridad gestionará las dependencias que puedan existir con proveedores contratados, proveedores de servicios o suborganizaciones del fabricante en lo que respecta a los requisitos del punto 7.2.2.2.

### 7.3. Requisitos relativos a los tipos de vehículos

7.3.1. El fabricante contará con un certificado de conformidad del sistema de gestión de la ciberseguridad válido pertinente para el tipo de vehículo sujeto a homologación.

No obstante, en el caso de homologaciones de tipo anteriores al 1 de julio de 2024, si el fabricante del vehículo puede demostrar que el tipo de vehículo no se pudo desarrollar de conformidad con el sistema de gestión de la ciberseguridad, deberá demostrar entonces que la ciberseguridad se tuvo en cuenta de forma adecuada durante la fase de desarrollo del tipo de vehículo en cuestión.

7.3.2. El fabricante del vehículo determinará y gestionará los riesgos relacionados con el proveedor para el tipo de vehículo sujeto a homologación.

7.3.3. El fabricante del vehículo determinará los elementos críticos del tipo de vehículo y realizará una evaluación de riesgos exhaustiva para dicho tipo y tratará o gestionará los riesgos detectados de forma adecuada. La evaluación de riesgos tendrá en cuenta los elementos individuales del tipo de vehículo y sus interacciones. La evaluación de riesgos tendrá en cuenta también las interacciones con cualquier otro sistema externo. Al evaluar los riesgos, el fabricante del vehículo tendrá en cuenta los riesgos relacionados con todas las amenazas a que se refiere la parte A del anexo 5, así como cualquier otro riesgo pertinente.

7.3.4. El fabricante del vehículo protegerá el tipo de vehículo contra los riesgos detectados en la evaluación de riesgos que haya realizado. Se adoptarán medidas de mitigación proporcionadas para proteger el tipo de vehículo. Las medidas de mitigación aplicadas incluirán todas las medidas de este tipo a que se refieren las partes B y C del anexo 5 que sean pertinentes para los riesgos detectados. No obstante, si una medida de mitigación mencionada en la parte A o B del anexo 5 no es pertinente o suficiente para el riesgo detectado, el fabricante del vehículo se asegurará de que se aplique otra medida de mitigación adecuada.

En particular, en el caso de las homologaciones de tipo anteriores al 1 de julio de 2024, el fabricante del vehículo se asegurará de que se aplique otra medida de mitigación adecuada si una medida de mitigación mencionada en las partes B o C del anexo 5 no es técnicamente viable. El fabricante facilitará a la autoridad de homologación la correspondiente evaluación de la viabilidad técnica.

7.3.5. El fabricante del vehículo adoptará medidas adecuadas y proporcionadas para garantizar entornos específicos seguros en el tipo de vehículo (si se incluyen) para el almacenaje y la ejecución del *software*, servicios, aplicaciones o datos postventa.

7.3.6. El fabricante del vehículo llevará a cabo, antes de la homologación de tipo, ensayos adecuados y suficientes para verificar la eficacia de las medidas de seguridad aplicadas.

7.3.7. El fabricante del vehículo aplicará medidas para el tipo de vehículo a fin de:

- a) detectar y prevenir ciberataques contra los vehículos del tipo de vehículo;
- b) respaldar la capacidad de supervisión del fabricante del vehículo en lo que respecta a la detección de amenazas, vulnerabilidades y ciberataques relacionados con el tipo de vehículo;
- c) proporcionar capacidad forense en relación con los datos a fin de permitir el análisis de los intentos de ciberataques o de los ciberataques consumados.

7.3.8. Los módulos criptográficos utilizados a los efectos del presente Reglamento estarán en consonancia con normas consensuadas. Si los módulos criptográficos utilizados no están en consonancia con normas consensuadas, el fabricante del vehículo deberá justificar su uso.

### 7.4. Disposiciones relativas a la notificación

7.4.1. El fabricante del vehículo notificará al menos una vez al año, o con más frecuencia si fuera pertinente, a la autoridad de homologación o al servicio técnico el resultado de sus actividades de supervisión definidas en el punto 7.2.2.2, letra g), incluida la información pertinente sobre nuevos ciberataques. El fabricante del vehículo también notificará y confirmará a la autoridad de homologación o al servicio técnico que las medidas de mitigación en materia de ciberseguridad aplicadas a sus tipos de vehículos siguen siendo eficaces, así como las medidas adicionales adoptadas.

7.4.2. La autoridad de homologación o el servicio técnico verificarán la información facilitada y, de ser necesario, exigirán al fabricante del vehículo que subsane cualquier ineficacia.

Si la notificación o la respuesta no son suficientes, la autoridad de homologación podrá decidir retirar el certificado de conformidad del sistema de gestión de la ciberseguridad de acuerdo con el punto 6.8.

## 8. MODIFICACIÓN DEL TIPO DE VEHÍCULO Y EXTENSIÓN DE LA HOMOLOGACIÓN DE TIPO

8.1. Toda modificación del tipo de vehículo que afecte a su rendimiento técnico en lo que respecta a la ciberseguridad o de la documentación exigida por el presente Reglamento se notificará a la autoridad de homologación que homologó el tipo de vehículo. Esta podrá entonces:

8.1.1. considerar que las modificaciones realizadas siguen cumpliendo los requisitos y la documentación de la homologación de tipo existente; o

8.1.2. proceder a la evaluación complementaria que sea necesaria en virtud del punto 5 y requerir, cuando proceda, otro informe de ensayo del servicio técnico responsable de la realización de los ensayos.

8.1.3. La confirmación, la extensión o la denegación de la homologación, especificando las alteraciones, se comunicará mediante un formulario de comunicación conforme al modelo que figura en el anexo 2 del presente Reglamento. La autoridad de homologación que expida la extensión de la homologación asignará un número de serie a dicha extensión e informará de ello a las demás Partes del Acuerdo de 1958 que apliquen el presente Reglamento por medio de un formulario de comunicación conforme al modelo que figura en el anexo 2 del presente Reglamento.

## 9. CONFORMIDAD DE LA PRODUCCIÓN

9.1. Los procedimientos de conformidad de la producción se ajustarán a los establecidos en el anexo 1 del Acuerdo de 1958 (E/ECE//TRANS/505/Rev.3) y cumplirán los requisitos que se exponen a continuación:

9.1.1. el titular de la homologación deberá garantizar que los resultados de los ensayos de conformidad de la producción se registran y que los documentos anejos están disponibles durante un período que se determinará de común acuerdo con la autoridad de homologación o su servicio técnico. Dicho período no será superior a diez años a partir del momento en que se produzca el cese definitivo de la producción;

9.1.2. la autoridad de homologación que haya concedido la homologación de tipo podrá verificar en cualquier momento los métodos de control de la conformidad aplicados en cada unidad de producción. La frecuencia normal de esas verificaciones será de una vez cada tres años.

## 10. SANCIONES POR FALTA DE CONFORMIDAD DE LA PRODUCCIÓN

10.1. La homologación concedida con respecto a un tipo de vehículo con arreglo al presente Reglamento podrá retirarse si no se cumplen los requisitos que figuran en él o si los vehículos de la muestra no cumplen los requisitos del presente Reglamento.

10.2. Cuando una autoridad de homologación retire una homologación que haya concedido previamente, informará de ello de forma inmediata a las demás Partes contratantes que apliquen el presente Reglamento mediante un formulario de comunicación conforme al modelo que figura en el anexo 2 del presente Reglamento.

- 
11. CESE DEFINITIVO DE LA PRODUCCIÓN
  - 11.1. Si el titular de una homologación cesa por completo de fabricar un tipo de vehículo homologado con arreglo al presente Reglamento, informará de ello a la autoridad que concedió la homologación. Tras recibir la correspondiente comunicación, dicha autoridad deberá informar de ello a las demás Partes contratantes del Acuerdo que apliquen el presente Reglamento mediante una copia del formulario de homologación al final de la cual figurará en grandes caracteres la indicación firmada y fechada «CESE DE LA PRODUCCIÓN».
  12. NOMBRES Y DIRECCIONES DE LOS SERVICIOS TÉCNICOS RESPONSABLES DE REALIZAR LOS ENSAYOS DE HOMOLOGACIÓN Y DE LAS AUTORIDADES DE HOMOLOGACIÓN DE TIPO
  - 12.1. Las Partes contratantes del Acuerdo que apliquen el presente Reglamento deberán comunicar a la Secretaría de las Naciones Unidas el nombre y la dirección de los servicios técnicos encargados de realizar los ensayos de homologación y de las autoridades de homologación de tipo que concedan la homologación y a las cuales deban remitirse los formularios expedidos en otros países que certifiquen la concesión, extensión, denegación o retirada de la homologación.
-



## ANEXO 1

**Ficha técnica**

La información que figura a continuación deberá presentarse, en su caso, por triplicado e ir acompañada de un índice de contenidos. Los planos que vayan a entregarse se presentarán a la escala adecuada, suficientemente detallados y en formato A4 o doblados de forma que se ajusten a dicho formato. Si se presentan fotografías, deberán ser suficientemente detalladas.

1. Marca (nombre comercial del fabricante): .....
2. Tipo y denominación(es) comercial(es) general(es): .....
3. Medio de identificación del tipo, si está marcado en el vehículo: .....
4. Ubicación de esa marca: .....
5. Categoría(s) de vehículo: .....
6. Nombre y dirección del fabricante o del representante del fabricante: .....
7. Nombre y dirección de la(s) planta(s) de montaje: .....
8. Fotografía(s) o plano(s) de un vehículo representativo: .....
9. Ciberseguridad
  - 9.1. Características generales de fabricación del tipo de vehículo, entre ellas:
    - a) los sistemas del vehículo que sean pertinentes para la ciberseguridad del tipo de vehículo;
    - b) los componentes de dichos sistemas que sean pertinentes para la ciberseguridad;
    - c) las interacciones de dichos sistemas con otros sistemas dentro del tipo de vehículo y las interfaces externas.
  - 9.2. Una representación esquemática del tipo de vehículo.
  - 9.3. El número del certificado de conformidad del sistema de gestión de la ciberseguridad: .....
  - 9.4. Documentos, relativos al tipo de vehículo cuya homologación se solicita, en los que se describe el resultado de la evaluación de riesgos y los riesgos detectados: .....
  - 9.5. Documentos, relativos al tipo de vehículo cuya homologación se solicita, en los que se describen las medidas de mitigación que se han aplicado en los sistemas enumerados o en el tipo de vehículo y la forma en que estas abordan los riesgos indicados: .....
  - 9.6. Documentos, relativos al tipo de vehículo cuya homologación se solicita, en los que se describe la protección de los entornos específicos previstos para el *software*, servicios, aplicaciones o datos postventa: .....
  - 9.7. Documentos, relativos al tipo de vehículo cuya homologación se solicita, en los que se describen los ensayos realizados para verificar la ciberseguridad del tipo de vehículo y sus sistemas, y el resultado de dichos ensayos: .....
  - 9.8. Descripción de la consideración de la cadena de suministro con respecto a la ciberseguridad: .....

*Apéndice 1 del Anexo 1***Modelo de la declaración de conformidad del sistema de gestión de la ciberseguridad del fabricante**

Declaración de conformidad del fabricante con los requisitos del sistema de gestión de la ciberseguridad

Nombre del fabricante: .....

Dirección del fabricante: .....

..... (*nombre del fabricante*) atestigua que se han instalado y se mantendrán los procesos necesarios para cumplir con los requisitos del sistema de gestión de la ciberseguridad establecidos en el punto 7.2 del Reglamento n.º 155 de las Naciones Unidas.....

Hecho en: ..... (*lugar*)

Fecha: .....

Nombre del firmante: .....

Cargo del firmante: .....

.....

(*Sello y firma del representante del fabricante*)

\_\_\_\_\_

## ANEXO 2

## Comunicación

[Formato máximo: A4 (210 × 297 mm)]



Expedida por:

Nombre de la administración:

.....

.....

.....

relativa a <sup>(2)</sup>

La concesión de la homologación

La extensión de la homologación

La retirada de la homologación con efecto a partir del dd/mm/aaaa

La denegación de la homologación

Cese definitivo de la producción

de un tipo de vehículo con arreglo al Reglamento n.º 155 de las Naciones Unidas

N.º de homologación: .....

N.º de extensión: .....

Motivos de la extensión: .....

1. Marca (nombre comercial del fabricante): .....

2. Tipo y denominación(es) comercial(es) general(es) .....

3. Medio de identificación del tipo, si está marcado en el vehículo: .....

3.1. Ubicación de esa marca: .....

4. Categoría(s) de vehículo: .....

5. Nombre y dirección del fabricante o del representante del fabricante: .....

6. Nombre y dirección de la(s) planta(s) de montaje: .....

7. Número del certificado de conformidad del sistema de gestión de la ciberseguridad: .....

8. Servicio técnico encargado de realizar los ensayos: .....

9. Fecha del informe de ensayo: .....

10. Número del informe de ensayo: .....

11. Observaciones: (en su caso). .....

12. Lugar: .....

13. Fecha: .....
14. Firma: .....
15. Se adjunta el índice del expediente de homologación en posesión de la autoridad de homologación, que puede obtenerse a petición del interesado:

(1) Táchese lo que no proceda.

(2) Número distintivo del país que ha concedido/extendido/denegado/retirado la homologación (véanse las disposiciones del Reglamento relativas a la homologación):

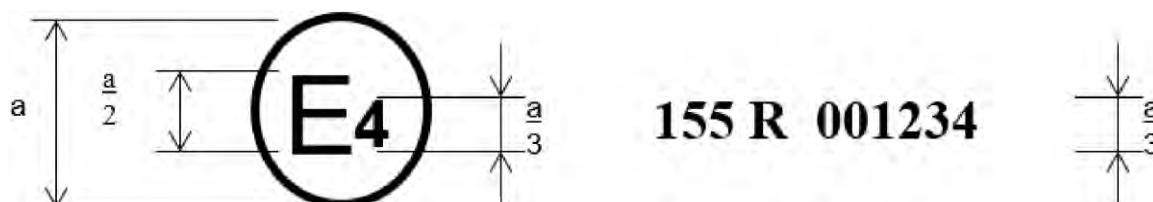
\_\_\_\_\_

## ANEXO 3

## Disposición de la marca de homologación

## MODELO A

(Véase el punto 4.2 del presente Reglamento)

 $a = 8 \text{ mm mín.}$ 

Esta marca de homologación colocada en un vehículo indica que el tipo de vehículo de carretera en cuestión ha sido homologado en los Países Bajos (E4), con arreglo al Reglamento n.º 155 y con el número de homologación 001234. Los dos primeros dígitos del número de homologación indican que esta fue concedida de conformidad con los requisitos del presente Reglamento en su forma original (00).

## ANEXO 4

**Modelo de certificado de conformidad del sistema de gestión de la ciberseguridad**

Certificado de conformidad del sistema de gestión de la ciberseguridad

con el Reglamento n.º 155 de las Naciones Unidas

Número del certificado [*Número de referencia*][..... *Autoridad de homologación*]

Certifica que

Fabricante: .....

Dirección del fabricante: .....

cumple con lo dispuesto en el punto 7.2 del Reglamento n.º 155

Los controles fueron realizados el día: .....

por (nombre y dirección de la autoridad de homologación o el servicio técnico): .....

Número del informe: .....

El certificado será válido hasta el [.....*fecha*]Hecho en [... ..*lugar*]el [... ..*fecha*][ .....*Firma*]

Anexos: descripción del sistema de gestión de la ciberseguridad por el fabricante.

---

## ANEXO 5

## Lista de amenazas y sus correspondientes medidas de mitigación

1. Este anexo consta de tres partes. En la parte A se describe la línea de base de las amenazas, las vulnerabilidades y los métodos de ataque. En la parte B se describen las medidas de mitigación de las amenazas previstas para los tipos de vehículos. En la parte C se describen las medidas de mitigación de las amenazas previstas para aspectos ajenos al vehículo, por ejemplo, en *back-ends* de TI.
2. La parte A, la parte B y la parte C se tendrán en cuenta para las evaluaciones de riesgos y las medidas de mitigación que aplicarán los fabricantes de los vehículos.
3. En la parte A se han indexado las vulnerabilidades de alto nivel con sus correspondientes ejemplos. Se hace referencia a la misma indexación en los cuadros de las partes B y C para vincular cada ataque/vulnerabilidad con una lista de medidas de mitigación correspondientes.
4. En el análisis de las amenazas también se tendrán en cuenta los posibles efectos de los ataques. Esto puede ayudar a determinar la gravedad de un riesgo y a detectar riesgos adicionales. Los posibles efectos de un ataque pueden ser:
  - a) afectación del funcionamiento seguro del vehículo;
  - b) interrupción del funcionamiento de las funciones del vehículo;
  - c) modificación del *software* y alteración del rendimiento;
  - d) alteración del *software* pero sin efectos en el funcionamiento;
  - e) violación de la integridad de los datos;
  - f) violación de la confidencialidad de los datos;
  - g) pérdida de disponibilidad de los datos;
  - h) otros, incluida la delincuencia.

## Parte A. Vulnerabilidad o método de ataque relacionados con las amenazas

1. En el cuadro A1 se ofrecen descripciones generales de las amenazas y de la vulnerabilidad o el método de ataque relacionados con ellas

## Cuadro A1

## Lista de vulnerabilidades o métodos de ataque relacionados con las amenazas

| Descripciones generales y específicas de vulnerabilidades/amenazas                                    |   |                                                                                                             | Ejemplo de vulnerabilidad o método de ataque |                                                                                                                                                                                                      |
|-------------------------------------------------------------------------------------------------------|---|-------------------------------------------------------------------------------------------------------------|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.3.1. Amenazas relativas a los servidores <i>back-end</i> en relación con vehículos sobre el terreno | 1 | Servidores <i>back-end</i> utilizados como medio para atacar un vehículo o extraer datos                    | 1.1                                          | Abuso de privilegios por parte del personal (ataque interno)                                                                                                                                         |
|                                                                                                       |   |                                                                                                             | 1.2                                          | Acceso no autorizado al servidor a través de Internet (posibilitado, por ejemplo, por <i>backdoors</i> , vulnerabilidades de un <i>software</i> del sistema sin parches, ataques SQL u otros medios) |
|                                                                                                       |   |                                                                                                             | 1.3                                          | Acceso físico no autorizado al servidor (por ejemplo, mediante memorias USB u otros medios de conexión al servidor)                                                                                  |
|                                                                                                       | 2 | Interrupción de los servicios del servidor <i>back-end</i> , lo que afecta al funcionamiento de un vehículo | 2.1                                          | El ataque al servidor <i>back-end</i> interrumpe su funcionamiento, por ejemplo evita que interactúe con los vehículos y les preste servicios de los que dependen                                    |

| Descripciones generales y específicas de vulnerabilidades/amenazas            |   |                                                                                                                                                                              | Ejemplo de vulnerabilidad o método de ataque |                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                               | 3 | Los datos relacionados con el vehículo que se almacenan en los servidores <i>back-end</i> se pierden o se ven comprometidos («violación de la seguridad de los datos»)       | 3.1                                          | Abuso de privilegios por parte del personal (ataque interno)                                                                                                                                                                    |
|                                                                               |   |                                                                                                                                                                              | 3.2                                          | Pérdida de información en la nube. Pueden perderse datos sensibles debido a ataques o accidentes cuando el almacenamiento de los datos corre a cargo de terceros proveedores de servicios en la nube                            |
|                                                                               |   |                                                                                                                                                                              | 3.3                                          | Acceso no autorizado al servidor a través de Internet (posibilitado, por ejemplo, por <i>backdoors</i> , vulnerabilidades de un <i>software</i> del sistema sin parches, ataques SQL u otros medios)                            |
|                                                                               |   |                                                                                                                                                                              | 3.4                                          | Acceso físico no autorizado al servidor (por ejemplo, mediante memorias USB u otros medios de conexión al servidor)                                                                                                             |
|                                                                               |   |                                                                                                                                                                              | 3.5                                          | Violación de la seguridad de los datos por un intercambio de datos no intencionado (p. ej., errores administrativos)                                                                                                            |
| 4.3.2. Amenazas a vehículos por lo que respecta a sus canales de comunicación | 4 | Falsificación de los mensajes o datos recibidos por el vehículo                                                                                                              | 4.1                                          | Falsificación de mensajes por suplantación de identidad (p. ej., 802.11p V2X durante la marcha en pelotón, mensajes GNSS, etc.)                                                                                                 |
|                                                                               |   |                                                                                                                                                                              | 4.2                                          | Ataque Sybil (a fin de suplantar la identidad de otros vehículos como si hubiera muchos vehículos en la carretera)                                                                                                              |
|                                                                               | 5 | Canales de comunicación utilizados para llevar a cabo una manipulación, eliminación u otras modificaciones no autorizadas del código o los datos almacenados por el vehículo | 5.1                                          | Los canales de comunicación permiten la introducción de un código, por ejemplo, se puede introducir un código binario de <i>software</i> manipulado en el flujo de comunicación                                                 |
|                                                                               |   |                                                                                                                                                                              | 5.2                                          | Los canales de comunicación permiten la manipulación de los datos o el código almacenados por el vehículo                                                                                                                       |
|                                                                               |   |                                                                                                                                                                              | 5.3                                          | Los canales de comunicación permiten sobrecribir los datos o el código almacenados por el vehículo                                                                                                                              |
|                                                                               |   |                                                                                                                                                                              | 5.4                                          | Los canales de comunicación permiten borrar los datos o el código almacenados por el vehículo                                                                                                                                   |
|                                                                               |   |                                                                                                                                                                              | 5.5                                          | Los canales de comunicación permiten introducir datos o el código en el vehículo (escritura de datos/código)                                                                                                                    |
|                                                                               | 6 | Los canales de comunicación permiten aceptar mensajes poco fiables o que no son de confianza o son vulnerables a secuestro de sesión o ataques de repetición                 | 6.1                                          | Aceptación de información de una fuente poco fiable o que no es de confianza                                                                                                                                                    |
|                                                                               |   |                                                                                                                                                                              | 6.2                                          | Ataque de intermediario / secuestro de sesión                                                                                                                                                                                   |
|                                                                               |   |                                                                                                                                                                              | 6.3                                          | Ataque de repetición, por ejemplo un ataque contra una pasarela de comunicación permite al atacante devolver a una versión anterior el <i>software</i> de una unidad de control electrónico o el <i>firmware</i> de la pasarela |



| Descripciones generales y específicas de vulnerabilidades/amenazas             |    |                                                                                                                                                                                      | Ejemplo de vulnerabilidad o método de ataque |                                                                                                                                                                                  |
|--------------------------------------------------------------------------------|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                | 7  | La información puede divulgarse fácilmente. Por ejemplo, mediante la interceptación de las comunicaciones o permitiendo el acceso no autorizado a archivos o carpetas confidenciales | 7.1                                          | Interceptación de la información / radiaciones interferentes / control de las comunicaciones                                                                                     |
|                                                                                |    |                                                                                                                                                                                      | 7.2                                          | Obtención de acceso no autorizado a archivos o datos                                                                                                                             |
|                                                                                | 8  | Ataques de denegación de servicio a través de canales de comunicación para alterar las funciones del vehículo                                                                        | 8.1                                          | Envío de una gran cantidad de datos inútiles al sistema de información del vehículo para que este no pueda prestar servicios de la forma habitual                                |
|                                                                                |    |                                                                                                                                                                                      | 8.2                                          | Ataque de agujero negro para interrumpir la comunicación entre vehículos; el atacante puede bloquear los mensajes entre los vehículos                                            |
|                                                                                | 9  | Un usuario sin privilegios puede obtener acceso privilegiado a los sistemas del vehículo                                                                                             | 9.1                                          | Un usuario sin privilegios puede obtener acceso privilegiado, por ejemplo acceso <i>root</i>                                                                                     |
|                                                                                | 10 | Los virus integrados en los medios de comunicación pueden infectar los sistemas del vehículo                                                                                         | 10.1                                         | Un virus integrado en los medios de comunicación infecta los sistemas del vehículo                                                                                               |
|                                                                                | 11 | Los mensajes recibidos por el vehículo (por ejemplo, mensajes X2V o mensajes de diagnóstico) o transmitidos en él contienen contenido malicioso                                      | 11.1                                         | Mensajes internos (p. ej., CAN) maliciosos                                                                                                                                       |
|                                                                                |    |                                                                                                                                                                                      | 11.2                                         | Mensajes V2X maliciosos, p. ej., mensajes de infraestructura a vehículo o de vehículo a vehículo (p. ej., CAM, DENM)                                                             |
|                                                                                |    |                                                                                                                                                                                      | 11.3                                         | Mensajes de diagnóstico maliciosos                                                                                                                                               |
|                                                                                |    |                                                                                                                                                                                      | 11.4                                         | Mensajes propietarios maliciosos (p. ej., los que normalmente se envían desde el fabricante de equipo original o el proveedor de componentes/sistemas/funciones)                 |
| 4.3.3. Amenazas a vehículos con respecto a sus procedimientos de actualización | 12 | Uso incorrecto o compromiso de los procedimientos de actualización                                                                                                                   | 12.1                                         | Compromiso de los procedimientos inalámbricos de actualización de <i>software</i> . Esto incluye la falsificación del programa de actualización del sistema o <i>firmware</i>    |
|                                                                                |    |                                                                                                                                                                                      | 12.2                                         | Compromiso de los procedimientos locales/físicos de actualización de <i>software</i> . Esto incluye la falsificación del programa de actualización del sistema o <i>firmware</i> |
|                                                                                |    |                                                                                                                                                                                      | 12.3                                         | El <i>software</i> se manipula antes del proceso de actualización (y está, por tanto, corrompido), aunque el proceso de actualización esté intacto                               |

| Descripciones generales y específicas de vulnerabilidades/amenazas                                     |                                                      |                                                                                                                                                                                                                                                             | Ejemplo de vulnerabilidad o método de ataque     |                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                        |                                                      |                                                                                                                                                                                                                                                             | 12.4                                             | Compromiso de las claves criptográficas del proveedor de <i>software</i> para permitir una actualización inválida                                                                                                                    |
|                                                                                                        | 13                                                   | Es posible denegar actualizaciones legítimas                                                                                                                                                                                                                | 13.1                                             | Ataque de denegación de servicio contra un servidor o red de actualización para impedir el lanzamiento de actualizaciones de <i>software</i> crítico o el desbloqueo de características específicas del cliente                      |
| 4.3.4. Amenazas a vehículos con respecto a acciones humanas involuntarias que facilitan un ciberataque | 15                                                   | Actores legítimos pueden actuar de forma que se facilita involuntariamente un ciberataque                                                                                                                                                                   | 15.1                                             | Se engaña a una víctima inocente (p. ej., un propietario, un operario o un ingeniero de mantenimiento) para que inicie una acción de tal manera que, de forma no intencionada, cargue <i>software</i> malicioso o permita un ataque  |
|                                                                                                        |                                                      |                                                                                                                                                                                                                                                             | 15.2                                             | No se siguen los procedimientos de seguridad definidos                                                                                                                                                                               |
| 4.3.5. Amenazas a vehículos con respecto a su conectividad externa y sus conexiones externas           | 16                                                   | La manipulación de la conectividad de las funciones del vehículo permite un ciberataque que puede incluir los sistemas telemáticos; los sistemas que permiten operaciones remotas; y los sistemas que utilizan comunicaciones inalámbricas de corto alcance | 16.1                                             | Manipulación de las funciones diseñadas para operar los sistemas a distancia, como una llave de control remoto, un inmovilizador y una estación de carga                                                                             |
|                                                                                                        |                                                      |                                                                                                                                                                                                                                                             | 16.2                                             | Manipulación de los sistemas telemáticos del vehículo (p. ej., manipulación de la medición de la temperatura de mercancías delicadas, desbloqueo remoto de puertas de carga)                                                         |
|                                                                                                        |                                                      |                                                                                                                                                                                                                                                             | 16.3                                             | Interferencia con sensores o sistemas inalámbricos de corto alcance                                                                                                                                                                  |
|                                                                                                        | 17                                                   | <i>Software</i> alojado por terceros, p. ej., aplicaciones de entretenimiento utilizadas como medio para atacar los sistemas de vehículo                                                                                                                    | 17.1                                             | Aplicaciones corruptas o aplicaciones con una mala seguridad de <i>software</i> utilizadas como método para atacar los sistemas del vehículo                                                                                         |
|                                                                                                        | 18                                                   | Dispositivos conectados a interfaces externas, p. ej., puertos USB, puerto OBD, utilizados como medio para atacar los sistemas del vehículo                                                                                                                 | 18.1                                             | Interfaces externas como puertos USB u otros puertos utilizadas como punto de ataque, por ejemplo, mediante la introducción de un código                                                                                             |
|                                                                                                        |                                                      |                                                                                                                                                                                                                                                             | 18.2                                             | Medios infectados con un virus conectados al vehículo                                                                                                                                                                                |
|                                                                                                        |                                                      |                                                                                                                                                                                                                                                             | 18.3                                             | Uso del acceso al diagnóstico (p. ej., mochilas en el puerto OBD) para facilitar un ataque, p. ej., para manipular los parámetros del vehículo (de manera directa o indirecta)                                                       |
|                                                                                                        | 4.3.6. Amenazas a los datos o el código del vehículo | 19                                                                                                                                                                                                                                                          | Extracción de los datos o el código del vehículo | 19.1                                                                                                                                                                                                                                 |
| 19.2                                                                                                   |                                                      |                                                                                                                                                                                                                                                             |                                                  | Acceso no autorizado a la información personal del propietario, como su identidad, información sobre cuentas de pago, información sobre sus contactos, información sobre la ubicación, identificación electrónica del vehículo, etc. |
| 19.3                                                                                                   |                                                      |                                                                                                                                                                                                                                                             |                                                  | Extracción de claves criptográficas                                                                                                                                                                                                  |

| Descripciones generales y específicas de vulnerabilidades/amenazas                                           |    |                                                                                         | Ejemplo de vulnerabilidad o método de ataque |                                                                                                                                                                                                                                     |
|--------------------------------------------------------------------------------------------------------------|----|-----------------------------------------------------------------------------------------|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                              | 20 | Manipulación de los datos o el código del vehículo                                      | 20.1                                         | Cambios ilícitos o no autorizados en la identificación electrónica del vehículo                                                                                                                                                     |
|                                                                                                              |    |                                                                                         | 20.2                                         | Fraude de identidad. Por ejemplo, si un usuario desea mostrar otra identidad cuando se comunica con sistemas de peaje, un <i>back-end</i> del fabricante                                                                            |
|                                                                                                              |    |                                                                                         | 20.3                                         | Acción para eludir los sistemas de supervisión (p. ej., piratear/manipular/bloquear mensajes como los datos del dispositivo de seguimiento ODR-Tracker o el número de ejecuciones)                                                  |
|                                                                                                              |    |                                                                                         | 20.4                                         | Manipulación de datos para falsificar los datos de conducción del vehículo (p. ej., kilometraje, velocidad de conducción, instrucciones de conducción, etc.)                                                                        |
|                                                                                                              |    |                                                                                         | 20.5                                         | Cambios no autorizados en los datos de diagnóstico del sistema                                                                                                                                                                      |
|                                                                                                              | 21 | Borrado de datos o de código                                                            | 21.1                                         | Borrado o manipulación no autorizados de los registros de eventos del sistema                                                                                                                                                       |
|                                                                                                              | 22 | Introducción de <i>software</i> malicioso                                               | 22.2                                         | Introducción de <i>software</i> malicioso o actividad de <i>software</i> malicioso                                                                                                                                                  |
|                                                                                                              | 23 | Introducción de <i>software</i> nuevo o sobreescritura de <i>software</i> ya existente  | 23.1                                         | Fabricación de <i>software</i> del sistema de control o del sistema de información del vehículo                                                                                                                                     |
|                                                                                                              | 24 | Alteración de sistemas u operaciones                                                    | 24.1                                         | Denegación del servicio, por ejemplo, esta acción puede desencadenarse en la red interna mediante la inundación de un bus CAN o la provocación de fallos en una unidad de control electrónico a través de una alta tasa de mensajes |
|                                                                                                              | 25 | Manipulación de los parámetros del vehículo                                             | 25.1                                         | Acceso no autorizado para falsificar los parámetros de configuración de las funciones clave del vehículo, como los datos de freno, el umbral de despliegue de los airbags, etc.                                                     |
|                                                                                                              |    |                                                                                         | 25.2                                         | Acceso no autorizado para falsificar los parámetros de carga, como la tensión de carga, la potencia de carga, la temperatura de la batería, etc.                                                                                    |
| 4.3.7. Posibles vulnerabilidades que podrían explotarse si no se protegen o se refuerzan de forma suficiente | 26 | Las tecnologías criptográficas pueden verse comprometidas o no se aplican lo suficiente | 26.1                                         | La combinación de claves de cifrado cortas y un período de validez largo permite al atacante descifrar las claves del sistema de cifrado                                                                                            |
|                                                                                                              |    |                                                                                         | 26.2                                         | Uso insuficiente de algoritmos criptográficos para proteger sistemas sensibles                                                                                                                                                      |
|                                                                                                              |    |                                                                                         | 26.3                                         | Uso de algoritmos criptográficos que ya están obsoletos o lo estarán pronto                                                                                                                                                         |

| Descripciones generales y específicas de vulnerabilidades/amenazas |    |                                                                                                | Ejemplo de vulnerabilidad o método de ataque |                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------|----|------------------------------------------------------------------------------------------------|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                    | 27 | Las piezas o los suministros podrían verse comprometidos y permitir el ataque de los vehículos | 27.1                                         | <i>Hardware</i> o <i>software</i> diseñados para permitir un ataque o que no cumplen los criterios de diseño para detener un ataque                                                                                                                                                                                                                                                                                                                                      |
|                                                                    | 28 | El desarrollo de <i>software</i> o <i>hardware</i> permite vulnerabilidades                    | 28.1                                         | Errores de <i>software</i> . La presencia de errores de <i>software</i> puede ser la base de posibles vulnerabilidades aprovechables. Esto se aplica sobre todo si el <i>software</i> no se ha probado para verificar que no contiene un mal código conocido o errores conocidos y reducir el riesgo de que contenga un mal código desconocido o errores desconocidos                                                                                                    |
|                                                                    |    |                                                                                                | 28.2                                         | El uso de restos de la fase de desarrollo (p. ej., puertos de depuración, puertos JTAG, microprocesadores, certificados de desarrollo, contraseñas de desarrolladores, etc.) puede permitir el acceso a unidades de control electrónico o permitir a los atacantes obtener mayores privilegios                                                                                                                                                                           |
|                                                                    | 29 | El diseño de la red introduce vulnerabilidades                                                 | 29.1                                         | Puertos de Internet que se dejan abiertos y dan acceso a sistemas de redes                                                                                                                                                                                                                                                                                                                                                                                               |
|                                                                    |    |                                                                                                | 29.2                                         | Eludir la separación de redes para obtener el control Un ejemplo específico es el uso de puntos de acceso o pasarelas no protegidas (como pasarelas camión-remolque) para eludir las protecciones y obtener acceso a otros segmentos de la red con vistas a llevar a cabo actos malintencionados, como enviar mensajes de bus CAN arbitrarios                                                                                                                            |
|                                                                    | 31 | Puede producirse una transmisión de datos no deseada                                           | 31.1                                         | Violación de la seguridad de los datos. Pueden filtrarse datos personales cuando el coche cambia de usuario (p. ej., cuando se vende o se usa como vehículo de alquiler con nuevos arrendatarios)                                                                                                                                                                                                                                                                        |
|                                                                    | 32 | La manipulación física de los sistemas puede posibilitar un ataque                             | 32.1                                         | Manipulación del <i>hardware</i> electrónico, p. ej., la instalación de <i>hardware</i> electrónico no autorizado en un vehículo para posibilitar un ataque de intermediario<br>Sustitución de <i>hardware</i> electrónico autorizado (p. ej., sensores) por <i>hardware</i> electrónico no autorizado<br>Manipulación de la información recogida por un sensor (por ejemplo, utilizando un imán para manipular el sensor de efecto Hall conectado a la caja de cambios) |

## Parte B. Medidas de mitigación de las amenazas dirigidas a vehículos

## 1. Medidas de mitigación para los «canales de comunicación del vehículo»

Las medidas de mitigación de las amenazas relacionadas con los «canales de comunicación del vehículo» se enumeran en el cuadro B1

Cuadro B1

**Medidas de mitigación de las amenazas relacionadas con los «canales de comunicación del vehículo»**

| Referencia al cuadro A1 | Amenazas para los «canales de comunicación del vehículo»                                                                                                                                                                         | Ref.      | Medida de mitigación                                                                                                                                                                                                                                                           |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.1                     | Falsificación de mensajes (p. ej., 802.11p V2X durante la marcha en pelotón, mensajes GNSS, etc.) mediante la suplantación de identidad                                                                                          | M10       | El vehículo verificará la autenticidad e integridad de los mensajes que recibe                                                                                                                                                                                                 |
| 4.2                     | Ataque Sybil (a fin de suplantar la identidad de otros vehículos como si hubiera muchos vehículos en la carretera)                                                                                                               | M11       | Se implantarán controles de seguridad para almacenar claves criptográficas (p. ej., uso de módulos de seguridad de <i>hardware</i> )                                                                                                                                           |
| 5.1                     | Los canales de comunicación permiten la introducción de un código en los datos o el código del vehículo, por ejemplo, se puede introducir un código binario de <i>software</i> en el flujo de comunicación                       | M10<br>M6 | El vehículo verificará la autenticidad e integridad de los mensajes que recibe<br>Los sistemas incorporarán seguridad desde el diseño para minimizar riesgos                                                                                                                   |
| 5.2                     | Los canales de comunicación permiten la manipulación de los datos o el código almacenados por el vehículo                                                                                                                        | M7        | Se aplicarán diseños y técnicas de control de acceso para proteger los datos y el código del sistema                                                                                                                                                                           |
| 5.3                     | Los canales de comunicación permiten sobrecribir los datos o el código almacenados por el vehículo                                                                                                                               |           |                                                                                                                                                                                                                                                                                |
| 5.4<br>21.1             | Los canales de comunicación permiten borrar los datos o el código almacenados por el vehículo                                                                                                                                    |           |                                                                                                                                                                                                                                                                                |
| 5.5                     | Los canales de comunicación permiten introducir datos o un código en los sistemas del vehículo (escribir código de datos)                                                                                                        |           |                                                                                                                                                                                                                                                                                |
| 6.1                     | Aceptación de información de una fuente poco fiable o que no es de confianza                                                                                                                                                     | M10       | El vehículo verificará la autenticidad e integridad de los mensajes que recibe                                                                                                                                                                                                 |
| 6.2                     | Ataque de intermediario / secuestro de sesión                                                                                                                                                                                    | M10       | El vehículo verificará la autenticidad e integridad de los mensajes que recibe                                                                                                                                                                                                 |
| 6.3                     | Ataque de repetición, por ejemplo, un ataque contra una pasarela de comunicación permite al atacante devolver a una versión anterior el <i>software</i> de una unidad de control electrónico o el <i>firmware</i> de la pasarela |           |                                                                                                                                                                                                                                                                                |
| 7.1                     | Interceptación de la información / radiaciones interferentes / control de las comunicaciones                                                                                                                                     | M12       | Se protegerán los datos confidenciales transmitidos al vehículo o desde este                                                                                                                                                                                                   |
| 7.2                     | Obtención de acceso no autorizado a archivos o datos                                                                                                                                                                             | M8        | Mediante el diseño del sistema y el control de acceso, no debe ser posible que el personal no autorizado acceda a datos personales o a los datos críticos del sistema. El Proyecto de seguridad de aplicaciones web abiertas (OWASP) ofrece ejemplos de controles de seguridad |

| Referencia al cuadro A1 | Amenazas para los «canales de comunicación del vehículo»                                                                                                         | Ref. | Medida de mitigación                                                                                        |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------------------------------|
| 8.1                     | Envío de un gran número de datos inútiles al sistema de información del vehículo para que este no pueda prestar servicios de la forma habitual                   | M13  | Se emplearán medidas para la detección y recuperación de un ataque de denegación de servicio                |
| 8.2                     | Ataque de agujero negro, interrupción de la comunicación entre vehículos mediante el bloqueo de la transmisión de mensajes a otros vehículos                     | M13  | Se emplearán medidas para la detección y recuperación de un ataque de denegación de servicio                |
| 9.1                     | Un usuario sin privilegios puede obtener acceso privilegiado, por ejemplo, acceso <i>root</i>                                                                    | M9   | Se emplearán medidas para prevenir y detectar accesos no autorizados                                        |
| 10.1                    | Un virus integrado en los medios de comunicación infecta los sistemas del vehículo                                                                               | M14  | Deben considerarse medidas para proteger los sistemas frente a virus o <i>software</i> malicioso integrados |
| 11.1                    | Mensajes internos maliciosos (p. ej., CAN)                                                                                                                       | M15  | Deben considerarse medidas para detectar actividad o mensajes internos maliciosos                           |
| 11.2                    | Mensajes V2X maliciosos, p. ej., mensajes de infraestructura a vehículo o de vehículo a vehículo (CAM, DENM)                                                     | M10  | El vehículo verificará la autenticidad e integridad de los mensajes que recibe                              |
| 11.3                    | Mensajes de diagnóstico maliciosos                                                                                                                               |      |                                                                                                             |
| 11.4                    | Mensajes propietarios maliciosos (p. ej., los que normalmente se envían desde el fabricante de equipo original o el proveedor de componentes/sistemas/funciones) |      |                                                                                                             |

## 2. Medidas de mitigación para el «proceso de actualización»

Las medidas de mitigación de las amenazas relacionadas con el «proceso de actualización» se enumeran en el cuadro B2

Cuadro B2

### Medidas de mitigación de las amenazas relacionadas con el «proceso de actualización»

| Referencia al cuadro A1 | Amenazas para el «proceso de actualización»                                                                                                                                      | Ref. | Medida de mitigación                                                     |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|--------------------------------------------------------------------------|
| 12.1                    | Compromiso de los procedimientos inalámbricos de actualización de <i>software</i> . Esto incluye la falsificación del programa de actualización del sistema o <i>firmware</i>    | M16  | Se emplearán procedimientos seguros de actualización del <i>software</i> |
| 12.2                    | Compromiso de los procedimientos locales/físicos de actualización de <i>software</i> . Esto incluye la falsificación del programa de actualización del sistema o <i>firmware</i> |      |                                                                          |
| 12.3                    | El <i>software</i> se manipula antes del proceso de actualización (y está, por tanto, corrompido), aunque el proceso de actualización esté intacto                               |      |                                                                          |

| Referencia al cuadro A1 | Amenazas para el «proceso de actualización»                                                                                                                                                                     | Ref. | Medida de mitigación                                                                                                                                                                                                                                                                               |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.4                    | Compromiso de las claves criptográficas del proveedor de <i>software</i> para permitir una actualización inválida                                                                                               | M11  | Se aplicarán controles de seguridad para almacenamiento de claves criptográficas                                                                                                                                                                                                                   |
| 13.1                    | Ataque de denegación de servicio contra un servidor o red de actualización para impedir el lanzamiento de actualizaciones de <i>software</i> crítico o el desbloqueo de características específicas del cliente | M3   | Se aplicarán controles de seguridad a los sistemas de <i>back-end</i> . Cuando los servidores <i>back-end</i> son esenciales para la prestación de los servicios, existen medidas de recuperación en caso de interrupción del sistema. El proyecto OWASP ofrece ejemplos de controles de seguridad |

### 3. Medidas de mitigación para las «acciones humanas involuntarias que facilitan un ciberataque»

Las medidas de mitigación de las amenazas relacionadas con las «acciones humanas involuntarias que facilitan un ciberataque» se enumeran en el cuadro B3.

*Cuadro B3*

#### Medidas de mitigación de las amenazas relacionadas con las «acciones humanas involuntarias que facilitan un ciberataque»

| Referencia al cuadro A1 | Amenazas relacionadas con «acciones humanas involuntarias»                                                                                                                                                                          | Ref. | Medida de mitigación                                                                                                                                                                                          |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 15.1                    | Se engaña a una víctima inocente (p. ej., un propietario, un operario o un ingeniero de mantenimiento) para que inicie una acción de tal manera que, de forma no intencionada, cargue <i>software</i> malicioso o permita un ataque | M18  | Se aplicarán medidas para definir y controlar las funciones de usuario y los privilegios de acceso, sobre la base del principio del mínimo privilegio de acceso                                               |
| 15.2                    | No se siguen los procedimientos de seguridad definidos                                                                                                                                                                              | M19  | Las organizaciones garantizarán la definición y el cumplimiento de los procedimientos de seguridad, incluido el registro de actividades y el acceso relacionados con la gestión de las funciones de seguridad |

### 4. Medidas de mitigación para «la conectividad externa y las conexiones externas»

Las medidas de mitigación de las amenazas relacionadas con «la conectividad externa y las conexiones externas» se enumeran en el cuadro B4

*Cuadro B4*

#### Medidas de mitigación de las amenazas relacionadas con «la conectividad externa y las conexiones externas»

| Referencia al cuadro A1 | Amenazas para «la conectividad externa y las conexiones externas»                                                                                                            | Ref. | Medida de mitigación                                                        |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-----------------------------------------------------------------------------|
| 16.1                    | Manipulación de las funciones diseñadas para operar los sistemas a distancia, como una llave de control remoto, un inmovilizador y una estación de carga                     | M20  | Se aplicarán controles de seguridad a los sistemas que tienen acceso remoto |
| 16.2                    | Manipulación de los sistemas telemáticos del vehículo (p. ej., manipulación de la medición de la temperatura de mercancías delicadas, desbloqueo remoto de puertas de carga) |      |                                                                             |

| Referencia al cuadro A1 | Amenazas para «la conectividad externa y las conexiones externas»                                                                                                              | Ref. | Medida de mitigación                                                                                                                                                                                                                                                                       |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 16.3                    | Interferencia con sensores o sistemas inalámbricos de corto alcance                                                                                                            |      |                                                                                                                                                                                                                                                                                            |
| 17.1                    | Aplicaciones corruptas, o aplicaciones con una mala seguridad de <i>software</i> utilizadas como método para atacar los sistemas del vehículo                                  | M21  | Se evaluará la seguridad del software, se autenticará y se protegerá su integridad. Se aplicarán controles de seguridad para minimizar el riesgo procedente del <i>software</i> de terceros que está destinado a ser alojado en el vehículo o es susceptible de ser alojado en el vehículo |
| 18.1                    | Interfaces externas como puertos USB u otros puertos utilizadas como punto de ataque, por ejemplo, mediante la introducción de un código                                       | M22  | Se aplicarán controles de seguridad a las interfaces externas                                                                                                                                                                                                                              |
| 18.2                    | Medios infectados con virus conectados al vehículo                                                                                                                             |      |                                                                                                                                                                                                                                                                                            |
| 18.3                    | Uso del acceso al diagnóstico (p. ej., mochilas en el puerto ODB) para facilitar un ataque, p. ej., para manipular los parámetros del vehículo (de manera directa o indirecta) | M22  | Se aplicarán controles de seguridad a las interfaces externas                                                                                                                                                                                                                              |

#### 5. Medidas de mitigación para los «objetivos potenciales de un ataque o motivaciones para un ataque»

Las medidas de mitigación de las amenazas relacionadas con los «objetivos potenciales de un ataque o motivaciones para un ataque» se enumeran en el cuadro B5.

Cuadro B5

#### Medidas de mitigación de las amenazas relacionadas con los «objetivos potenciales de un ataque o motivaciones para un ataque»

| Referencia al cuadro A1 | Amenazas relacionadas con «objetivos potenciales de un ataque o motivaciones para un ataque»                                                                                                                                         | Ref. | Medida de mitigación                                                                                                                                                                                                               |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 19.1                    | Extracción de <i>software</i> patentado o protegido con derechos de autor de los sistemas del vehículo (piratería)                                                                                                                   | M7   | Se aplicarán diseños y técnicas de control de acceso para proteger los datos o el código del sistema. El proyecto OWASP ofrece ejemplos de controles de seguridad                                                                  |
| 19.2                    | Acceso no autorizado a la información personal del propietario, como su identidad, información sobre cuentas de pago, información sobre sus contactos, información sobre la ubicación, identificación electrónica del vehículo, etc. | M8   | Mediante el diseño del sistema y el control de acceso, no debe ser posible que el personal no autorizado acceda a datos personales o a los datos críticos del sistema. El proyecto OWASP ofrece ejemplos de controles de seguridad |
| 19.3                    | Extracción de claves criptográficas                                                                                                                                                                                                  | M11  | Se implantarán controles de seguridad para el almacenaje de claves criptográficas, p. ej., uso de módulos de seguridad                                                                                                             |
| 20.1                    | Cambios ilícitos o no autorizados en la identificación electrónica del vehículo                                                                                                                                                      | M7   | Se aplicarán diseños y técnicas de control de acceso para proteger los datos o el código del sistema. El proyecto OWASP ofrece ejemplos de controles de seguridad                                                                  |
| 20.2                    | Fraude de identidad. Por ejemplo, si un usuario desea mostrar otra identidad cuando se comunica con sistemas de peaje o <i>back-end</i> del fabricante                                                                               |      |                                                                                                                                                                                                                                    |
| 20.3                    | Acción para eludir los sistemas de supervisión (p. ej., piratear/manipular/bloquear mensajes como los datos del dispositivo de seguimiento ODR-Tracker o el número de ejecuciones)                                                   | M7   | Se aplicarán diseños y técnicas de control de acceso para proteger los datos o el código del sistema. El proyecto OWASP ofrece ejemplos de controles de seguridad.                                                                 |



| Referencia al cuadro A1 | Amenazas relacionadas con «objetivos potenciales de un ataque o motivaciones para un ataque»                                                                                                                                        | Ref. | Medida de mitigación                                                                                                                                               |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 20.4                    | Manipulación de datos para falsificar los datos de conducción del vehículo (p. ej., kilometraje, velocidad de conducción, instrucciones de conducción, etc.)                                                                        |      | Los ataques de manipulación de datos en sensores o datos transmitidos podrían mitigarse correlacionando los datos de diferentes fuentes de información             |
| 20.5                    | Cambios no autorizados en los datos de diagnóstico del sistema                                                                                                                                                                      |      |                                                                                                                                                                    |
| 21.1                    | Borrado o manipulación no autorizados de los registros de eventos del sistema                                                                                                                                                       | M7   | Se aplicarán diseños y técnicas de control de acceso para proteger los datos o el código del sistema. El proyecto OWASP ofrece ejemplos de controles de seguridad. |
| 22.2                    | Introducción de <i>software</i> malicioso o actividad de <i>software</i> malicioso                                                                                                                                                  | M7   | Se aplicarán diseños y técnicas de control de acceso para proteger los datos o el código del sistema. El proyecto OWASP ofrece ejemplos de controles de seguridad. |
| 23.1                    | Fabricación de <i>software</i> del sistema de control o del sistema de información del vehículo                                                                                                                                     |      |                                                                                                                                                                    |
| 24.1                    | Denegación del servicio, por ejemplo, esta acción puede desencadenarse en la red interna mediante la inundación de un bus CAN o la provocación de fallos en una unidad de control electrónico a través de una alta tasa de mensajes | M13  | Se emplearán medidas para la detección y recuperación de un ataque de denegación de servicio                                                                       |
| 25.1                    | Acceso no autorizado para falsificar los parámetros de configuración de las funciones clave del vehículo, como los datos de freno, el umbral de despliegue de los airbags, etc.                                                     | M7   | Se aplicarán diseños y técnicas de control de acceso para proteger los datos o el código del sistema. El proyecto OWASP ofrece ejemplos de controles de seguridad  |
| 25.2                    | Acceso no autorizado para falsificar los parámetros de carga, como la tensión de carga, la potencia de carga, la temperatura de la batería, etc.                                                                                    |      |                                                                                                                                                                    |

6. Medidas de mitigación para las «posibles vulnerabilidades que podrían ser aprovechadas si no se protegen o se refuerzan de forma suficiente»

Las medidas de mitigación de las amenazas relacionadas con las «posibles vulnerabilidades que podrían ser aprovechadas si no se protegen o se refuerzan de forma suficiente» se enumeran en el cuadro B6.

Cuadro B6

**Medidas de mitigación de las amenazas relacionadas con las «posibles vulnerabilidades que podrían ser aprovechadas si no se protegen o se refuerzan de forma suficiente»**

| Referencia al cuadro A1 | Amenazas para las «posibles vulnerabilidades que podrían ser aprovechadas si no se protegen o se refuerzan de forma suficiente»          | Ref. | Medida de mitigación                                                                                      |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------|------|-----------------------------------------------------------------------------------------------------------|
| 26.1                    | La combinación de claves de cifrado cortas y un período de validez largo permite al atacante descifrar las claves del sistema de cifrado | M23  | Se seguirán las mejores prácticas de ciberseguridad en el desarrollo de <i>software</i> y <i>hardware</i> |

| Referencia al cuadro A1 | Amenazas para las «posibles vulnerabilidades que podrían ser aprovechadas si no se protegen o se refuerzan de forma suficiente»                                                                                                                                                                                                                | Ref. | Medida de mitigación                                                                                                                                                                                                       |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 26.2                    | Uso insuficiente de algoritmos criptográficos para proteger sistemas sensibles                                                                                                                                                                                                                                                                 |      |                                                                                                                                                                                                                            |
| 26.3                    | Uso de algoritmos criptográficos obsoletos                                                                                                                                                                                                                                                                                                     |      |                                                                                                                                                                                                                            |
| 27.1                    | <i>Hardware</i> o <i>software</i> diseñados para permitir un ataque o que no cumplen los criterios de diseño para detener un ataque                                                                                                                                                                                                            | M23  | Se seguirán las mejores prácticas de ciberseguridad en el desarrollo de <i>software</i> y <i>hardware</i>                                                                                                                  |
| 28.1                    | La presencia de errores de <i>software</i> puede ser la base de posibles vulnerabilidades aprovechables. Esto se aplica sobre todo si el <i>software</i> no se ha probado para verificar que no contiene un mal código conocido o errores conocidos y reducir el riesgo de que contenga un mal código desconocido o errores desconocidos       | M23  | Se seguirán las mejores prácticas de ciberseguridad en el desarrollo de <i>software</i> y <i>hardware</i> .<br>Ensayos de ciberseguridad con una cobertura adecuada                                                        |
| 28.2                    | El uso de restos de la fase de desarrollo (p. ej., puertos de depuración, puertos JTAG, microprocesadores, certificados de desarrollo, contraseñas de desarrolladores, etc.) puede permitir a un atacante acceder a las unidades de control electrónico u obtener mayores privilegios                                                          |      |                                                                                                                                                                                                                            |
| 29.1                    | Puertos de Internet que se dejan abiertos y dan acceso a sistemas de redes                                                                                                                                                                                                                                                                     |      |                                                                                                                                                                                                                            |
| 29.2                    | Eludir la separación de redes para obtener el control. Un ejemplo específico es el uso de puntos de acceso o pasarelas no protegidas (como pasarelas camión-remolque) para eludir las protecciones y obtener acceso a otros segmentos de la red con vistas a llevar a cabo actos malintencionados, como enviar mensajes de bus CAN arbitrarios | M23  | Se seguirán las mejores prácticas de ciberseguridad en el desarrollo de <i>software</i> y <i>hardware</i> .<br>Se seguirán las mejores prácticas de ciberseguridad para el diseño de sistemas y la integración de sistemas |

#### 7. Medidas de mitigación para la «pérdida de datos/violación de la seguridad de los datos del vehículo»

Las medidas de mitigación de las amenazas relacionadas con la «pérdida de datos / violación de la seguridad de los datos del vehículo» se enumeran en el cuadro B7.

Cuadro B7

#### Medidas de mitigación de las amenazas relacionadas con la «pérdida de datos / violación de la seguridad de los datos del vehículo»

| Referencia al cuadro A1 | Amenazas relacionadas con la «pérdida de datos / violación de la seguridad de los datos del vehículo»                                                                                                                | Ref. | Medida de mitigación                                                                                                                                 |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| 31.1                    | Violación de la seguridad de los datos. Se puede violar la seguridad de los datos personales cuando el coche cambia de usuario (p. ej., cuando se vende o se usa como vehículo de alquiler con nuevos arrendatarios) | M24  | Para el almacenamiento de datos personales se seguirán las mejores prácticas para la protección de la integridad y la confidencialidad de los datos. |

## 8. Medidas de mitigación para la «manipulación física de los sistemas para permitir un ataque»

Las medidas de mitigación de las amenazas relacionadas con la «manipulación física de los sistemas para permitir un ataque» se enumeran en el cuadro B8.

Cuadro B8

**Medidas de mitigación de las amenazas relacionadas con la «manipulación física de los sistemas para permitir un ataque»**

| Referencia al cuadro A1 | Amenazas relacionadas con la «manipulación física de los sistemas para permitir un ataque»                                                                                                | Ref. | Medida de mitigación                                                 |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|----------------------------------------------------------------------|
| 32.1                    | La manipulación del <i>hardware</i> del fabricante de equipo original, p. ej., la instalación de <i>hardware</i> no autorizado en un vehículo para posibilitar un ataque de intermediario | M9   | Se emplearán medidas para prevenir y detectar accesos no autorizados |

## Parte C. Medidas de mitigación de las amenazas externas al vehículo

1. Medidas de mitigación para los «servidores *back-end*»

Las medidas de mitigación de las amenazas relacionadas con los «servidores *back-end*» se enumeran en el cuadro C1

Cuadro C1

**Medidas de mitigación de las amenazas relacionadas con los «servidores *back-end*»**

| Referencia al cuadro A1 | Amenazas para «servidores <i>back-end</i> »                                                                                                                                                          | Ref. | Medida de mitigación                                                                                                                                                                                                                                                                             |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.1 y 3.1               | Abuso de privilegios por parte del personal (ataque interno)                                                                                                                                         | M1   | Se aplican controles de seguridad a los sistemas de <i>back-end</i> para minimizar el riesgo de un ataque interno                                                                                                                                                                                |
| 1.2 y 3.3               | Acceso no autorizado al servidor a través de Internet (posibilitado, por ejemplo, por <i>backdoors</i> , vulnerabilidades de un <i>software</i> del sistema sin parches, ataques SQL u otros medios) | M2   | Se aplican controles de seguridad a los sistemas de <i>back-end</i> para minimizar accesos no autorizados. El proyecto OWASP ofrece ejemplos de controles de seguridad                                                                                                                           |
| 1.3 y 3.4               | Acceso físico no autorizado al servidor (por ejemplo, mediante memorias USB u otros medios de conexión al servidor)                                                                                  | M8   | Mediante el diseño del sistema y el control de acceso, no debe ser posible que el personal no autorizado acceda a datos personales o a los datos críticos del sistema                                                                                                                            |
| 2.1                     | El ataque al servidor <i>back-end</i> interrumpe su funcionamiento, por ejemplo evita que interactúe con los vehículos y les preste servicios de los que dependen                                    | M3   | Se aplican controles de seguridad a los sistemas de <i>back-end</i> . Cuando los servidores <i>back-end</i> son esenciales para la prestación de los servicios, existen medidas de recuperación en caso de interrupción del sistema. El proyecto OWASP ofrece ejemplos de controles de seguridad |
| 3.2                     | Pérdida de información en la nube. Pueden perderse datos sensibles debido a ataques o accidentes cuando el almacenamiento de los datos corre a cargo de terceros proveedores de servicios en la nube | M4   | Se aplican controles de seguridad para minimizar los riesgos asociados a la computación en la nube. En el proyecto OWASP y en las orientaciones sobre computación en la nube del Centro de Ciberseguridad Nacional (NCSC) pueden encontrarse ejemplos de controles de seguridad                  |
| 3.5                     | Violación de la seguridad de los datos por un intercambio de datos no intencionado (p. ej., errores administrativos y almacenamiento de datos en servidores situados en garajes)                     | M5   | Se aplican controles de seguridad a los sistemas de <i>back-end</i> para evitar violaciones de la seguridad de los datos. El proyecto OWASP ofrece ejemplos de controles de seguridad                                                                                                            |

## 2. Medidas de mitigación para las «acciones humanas involuntarias»

Las medidas de mitigación de las amenazas relacionadas con las «acciones humanas involuntarias» se enumeran en el cuadro C2.

Cuadro C2

**Medidas de mitigación de las amenazas relacionadas con las «acciones humanas involuntarias»**

| Referencia al cuadro A1 | Amenazas relacionadas con «acciones humanas involuntarias»                                                                                                                                                                          | Ref. | Medida de mitigación                                                                                                                                                                                          |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 15.1                    | Se engaña a una víctima inocente (p. ej., un propietario, un operario o un ingeniero de mantenimiento) para que inicie una acción de tal manera que, de forma no intencionada, cargue <i>software</i> malicioso o permita un ataque | M18  | Se aplicarán medidas para definir y controlar las funciones de usuario y los privilegios de acceso, sobre la base del principio del mínimo privilegio de acceso                                               |
| 15.2                    | No se siguen los procedimientos de seguridad definidos                                                                                                                                                                              | M19  | Las organizaciones garantizarán la definición y el cumplimiento de los procedimientos de seguridad, incluido el registro de actividades y el acceso relacionados con la gestión de las funciones de seguridad |

## 3. Medidas de mitigación para la «pérdida física de datos»

Las medidas de mitigación de las amenazas relacionadas con la «pérdida física de datos» se enumeran en el cuadro C3.

Cuadro C3

**Medidas de mitigación de las amenazas relacionadas con la «pérdida física de datos»**

| Referencia al cuadro A1 | Amenazas para la «pérdida física de datos»                                                                                                                                                     | Ref. | Medida de mitigación                                                                                                                                                                                                        |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 30.1                    | Daños causados por un tercero. Pueden perderse datos sensibles o verse comprometidos debido a daños físicos en caso de accidentes de tráfico o robos                                           | M24  | Para el almacenamiento de datos personales se seguirán las mejores prácticas para la protección de la integridad y la confidencialidad de los datos. En la norma ISO/SC27/WG5 se ofrecen ejemplos de controles de seguridad |
| 30.2                    | Pérdida derivada de conflictos en la gestión de derechos digitales. Pueden borrarse datos de usuario por cuestiones relativas a la gestión de derechos digitales                               |      |                                                                                                                                                                                                                             |
| 30.3                    | La integridad de los datos sensibles se puede perder debido al desgaste de componentes informáticos, lo que puede provocar problemas en cascada (en caso de alteración de claves, por ejemplo) |      |                                                                                                                                                                                                                             |



**Proposal for the Interpretation  
Document for UN Regulation No.  
[155] on uniform provisions  
concerning the approval of  
vehicles with regards to cyber  
security and cyber security  
management system**

## **Proposal for the Interpretation Document for UN Regulation No. [155] on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system**

The text reproduced below was prepared by the Informal Working Group on Cyber Security and Over-the-Air issues and endorsed by the Working Party on Automated/Autonomous and Connected Vehicles (GRVA). It is submitted for review and endorsement by the World Forum for Harmonization of Vehicle Regulations (WP.29). At the request of WP.29, this document could be distributed with an official symbol at the March 2021 session of WP.29.

### **1. Preamble**

- 1.1. The purpose of this document is to help clarify the requirements of paragraphs 5, 7 and 8 and Annex 1 of the UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system (UN Regulation No. 155) and provide information on what may be used to evidence those requirements. The target audience for this document are vehicle manufacturers submitting systems for test and the Technical Services / Approval Authorities assessing those systems. The outcome should be that this document is able to help harmonise evaluations between different Technical Services/ Approval Authorities.

### **2. Note regarding evidencing the requirements**

- 2.1. This document is only guidance. It provides information on what information might/would be acceptable for the Technical Services/ Approval Authorities and what level of information might be supplied. It is not intended to be exhaustive. The standards referenced are intended as examples, not mandatory. Nevertheless, a coherence-check (see section 6 “Link with ISO/SAE DIS 21434 (E)”) has shown that especially the ISO/SAE DIS 21434 can be very supportive in implementing the requirements on the CSMS to the organizations along the supply chain. It should be noted that the clauses of ISO/SAE DIS 21434 referred to may change during later edition of the standard, but it is expected that the standard will still be relevant to those requirements. Depending on the vehicle type defined by the vehicle manufacturer and the practices and procedures they use alternative and/or equivalent information may be supplied.
- 2.2. For all the requirements in the regulation, demonstration that they are met may be achieved via documentation/presentation and/or audit. The format of what documentation is supplied is open but should be agreed between the vehicle manufacturer and Technical Service/ Approval Authority prior to testing/audit. A demonstration may be provided through an overview, diagrams and experience. Argument that the requirements are met needs to be logical, understandable and convincing. Documents need not necessarily be large documents.
- 2.3. The wording used in this document seeks to respect the ISO/IEC Directives, Part 2, Principles and rules for the structure and drafting of ISO

and IEC documents (ISBN 978-92-67-10603-8) described in section 7 of the 8th edition 2018.

### **3. Guidance on the requirements of the Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system (UN Regulation No. 155)**

Note. The paragraphs referred to below refer to the paragraphs of the on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system.

#### **A. Paragraphs 1. to 4. of the Regulation**

“1. Scope”

*No guidance included in this document with regards this requirement*

“2. Definitions”

*No guidance included in this document with regards this requirement*

“3. Application for Approval”

*No guidance included in this document with regards this requirement*

“4. Marking”

*No guidance included in this document with regards this requirement*

#### **B. Paragraph 5. to 5.3.**

“5. Approval”

“5.3. Approval Authorities shall not grant any type approval without verifying that the manufacturer has put in place satisfactory arrangements and procedures to manage properly the cyber security aspects as covered by this Regulation.”

*Explanation of the requirement*

In addition to the conditions referred to in paragraph 5.1., the Approval Authority is bound to verify if all the requirements quoted in section 7 of the Regulation have been effectively fulfilled. This includes the Cyber Security Management System referred to in paragraphs 7.2. and 7.3.1.

#### **C. Paragraph 5.3.1., part a)**

“5.3.1. The Approval Authority and its Technical Services shall ensure, in addition to the criteria laid down in Schedule 2 of the 1958 Agreement that they have:

- (a) Competent personnel with appropriate cyber security skills and specific automotive risk assessments knowledge;”

*Explanation of the requirement*

The requirement would imply that the authority or the Technical Service (the organisation) have at their disposal, in a sufficient number, the following categories of personnel:

- (a) Personnel competent and experienced in application of the Cyber Security Regulation, as well as of any national or organisation's rules, standards and procedures necessary for its implementation and application. Applicable standards may include ISO 21434 and ISO 27001 for the content and aspects of ISO 19011 and ISO PAS 5112 for the audit processes;
- (b) Personnel competent and experienced in application of methods of cyber security laboratory testing, such as, pen-, fuzz- and side channel-testing, in relation to cyber security of the vehicle.

This competence should be demonstrated by appropriate qualifications or other equivalent training records.

The Regulation does not impose any specific contractual relation between the Approval Authority/Technical Service and the personnel concerned. These might be employment (labour) contracts, services contracts etc.

The number of personnel concerned must be proportionate to the actual workload.

The internal procedures of the organisation should ensure that the tasks under the Regulation are performed or effectively controlled by the personnel having relevant skills.

#### **D. Paragraph 5.3.1., part b)**

- “(b) Implemented procedures for the uniform evaluation according to this Regulation.”

##### *Explanation of the requirement*

The organisation should have in place procedures ensuring that evaluation of every vehicle type is conducted according to the same scheme. If necessary, the evaluation may include variants. Application of variants is determined by clear criteria set out and explained in the internal documentation of the organisation.

In case the Approval Authority has designated several Technical Services, it needs to ensure uniformity of evaluation between different Technical Services, notably by arranging regular meetings where the experience is exchanged.

The organisation should have processes installed for secure storage and transmission of confidential information.

The Technical Services should have processes to assure that the integrity of the personnel involved in assessments is appropriate to the risks involved.

The requirement of the Regulation cannot be discharged by mere establishment of the required processes and procedures. It also requires their effective application, implying the necessity for adequate training and effective quality control.

##### *Examples of documents/evidence proving correct implementation*

Interpretation documents of the Technical Services

Best practice guidelines of the Approval Authority. These are the consolidated interpretations of the Technical Services.

Minutes of exchange of experience meetings of Approval Authority and Technical Services.

#### **E. Paragraph 5.3.2.**

- “5.3.2. Each Contracting Party applying this Regulation shall notify and inform by its Approval Authority other Approval Authorities about the method and criteria taken as a basis by the notifying Authority to assess the



appropriateness of the measures taken in accordance with this regulation and in particular with paragraphs 5.1., 7.2. and 7.3.

This information shall be shared only before granting an approval according to this Regulation for the first time and each time the method or criteria for assessment is updated.

This information is intended to be shared for the purposes of collection and analysis of the best practice and in view of ensuring the convergent application of this Regulation by all Approval Authorities applying this Regulation.”

*Explanation of the requirement*

This requirement aims at convergence across the Contracting Parties in the manner the requirements of paragraphs 5.1., 7.2. and 7.3. are applied. Importantly, the following subparagraphs must be interpreted in the manner permitting to achieve this objective. Additionally, the exchange should permit mutual learning and building of a pool of best practices which may be inspiration for further works on the amendment of UN Regulation No. [155] in the future.

As it can be understood from joint reading of paragraphs 5.3.2. and 5.3.3., information about methods and criteria should contain:

- (a) minimum performance levels that the Approval Authority will require to be met with regard to the specifications provided for under paragraphs 7.2. and 7.3.;
- (b) measures and processes the Approval Authorities/their Technical Services will follow when assessing the compliance following an application for a type approval.

In particular, the information should include:

- (c) the characteristics and the minimum performance criteria that processes referred to in paragraph 7.2.2.2. must meet, including the information on the criteria used to establish if the risks referred to in paragraph 7.2.2.2.(d) are “appropriately managed”;
- (d) the criteria that the Approval Authority will apply to assess if these processes ensure that cyber threats and vulnerabilities referred to in paragraph 7.2.2.3. shall be mitigated within a reasonable timeframe, including the information on the conditions for these threats and vulnerabilities to be considered as mitigated and on the understanding of “reasonable timeframe”;
- (e) the criteria that the Approval Authority will apply to assess that the processes meet the requirement referred to in paragraph 7.2.2.4.;
- (f) the criteria that the approval authority will apply to assess if the manufacturer has demonstrated that the CSMS manages dependencies referred to in paragraph 7.2.2.5.;
- (g) the criteria that the Approval Authority will apply to assess whether the CSMS certificate to be considered relevant for the vehicle type under approval;
- (h) for type approvals prior to 1 July 2024, the criteria that the Approval Authority will apply to assess if cyber security was adequately considered during the development phase of the vehicle type to the effect that it results in an equivalent cybersecurity performance;
- (i) the criteria that the Approval Authority will apply to assess whether the manufacturer has taken sufficient measures to identify and manage, for the vehicle type being approved, supplier-related risks, including the required standards for such risk management;
- (j) the criteria that the Approval Authority will apply to assess if the vehicle manufacturer has identified the critical elements of the vehicle type, including the

definition of “critical elements” that the authority has adopted to this effect;

- (k) the criteria that the Approval Authority will apply to assess if the vehicle manufacturer has performed an exhaustive risk assessment for the vehicle type, as required under subparagraph 7.3.3. of the Regulation;
- (l) the criteria that the Approval Authority will apply to assess if the vehicle type is protected against risks identified in the vehicle manufacturer’s risk assessment;
- (n) the criteria that the Approval Authority will apply to assess if the mitigations applied by the manufacturer are proportionate, including the explanation of the interpretation of the term “proportionate”;
- (o) the criteria that the approval authority will apply to assess if the mitigations referred to in Annex 5, Part B or C, are not relevant, not sufficient for the risk identified or not feasible;
- (p) the criteria that the approval authority will apply to assess if “another mitigation” implemented by the manufacturer pursuant to subparagraph 7.3.4. is “appropriate”;
- (q) the criteria that the Approval Authority will apply to assess if the testing performed by the manufacturer to verify the effectiveness of the security measures implemented were “appropriate” and “sufficient”;
- (r) the criteria that the Approval Authority will apply to assess if measures put in place by the manufacturer to secure dedicated environments on the vehicle type for the storage and execution of aftermarket software, services, applications or data, are “appropriate” and “proportionate”, including the explanation of the interpretation of the term “proportionate” in this context;
- (s) the documents that the Approval Authority will require to check if the vehicle manufacturer has taken the necessary measures referred to in subparagraph 5.1.1.;
- (t) the tests that the Approval Authority or Technical Services will perform and the testing strategy it will apply to verify that that the vehicle manufacturer has implemented the cyber security measures they have documented;
- (u) the internal procedures that the Approval Authority will apply in the process of assessment under section 5 of the Regulation.

It is important to stress that the Approval Authorities of the Parties are implicitly obliged to follow the methods and requirements which are subject to sharing and assessment.

#### **F. Paragraph 5.3.3.**

- “5.3.3. The information referred to in paragraph 5.3.2. shall be uploaded in English language to the secure internet database established by the United Nations Economic Commission for Europe (DETA) in due time and no later than 14 days before an approval is granted for the first time under the methods and criteria of assessment concerned. The information shall be sufficient to understand what minimum performance levels the Approval Authority adopted for each specific requirement referred to in paragraph 5.3.2. as well as the processes and measures it applies to verify that these minimum performance levels are met.”

##### *Explanation of the requirement*

Information uploaded must be objectively sufficient to understand the minimal performance levels that an authority adopted to consider that the requirements of the Regulation are complied with. This is of crucial importance, given the high-level nature and the frequent use of general clauses in formulation of these requirements.

Although the obligation to share the information, as referred to in paragraph 5.3.3., is an obligation of result and must always be met by the Approval Authority, the latter should discharge this obligation mindful of the need to avoid putting at risk the cyber security of a vehicle type approved in accordance with this Regulation.

Preferably, the information should be shared with other authorities well in advance (i.e. long before the first assessment conducted under these methods and criteria), so as to permit other authorities to examine them and, if necessary, obtain additional clarification, so as to fully achieve the objectives. However, under no circumstances can an Approval authority grant a type approval based on such methods and criteria within less than 14 days from the moment when the information was shared via DETA.

*Examples of documents/evidence that could be provided*

Please refer to Annex 1, which provides a template for data exchange via DETA in accordance with paragraph 5.3.

## **G. Paragraph 5.3.4.**

“5.3.4. Approval Authorities receiving the information referred to in paragraph 5.3.2. may submit comments to the notifying Approval Authority by uploading them to DETA within 14 days after the day of notification.”

*Explanation of the requirement*

Approval Authorities of other Contracting Parties are given the possibility, but are under no obligation, to provide comments on the information shared.

The 14-day time limit applies also in case where the information referred to in line with paragraph 5.3.2. has been shared earlier than 14 days before the approval decision. Ideally, comments of other authorities should be discussed and, if legitimate/useful, taken into account before the methods and criteria shared through DETA are applied for the first time. Therefore, interested approval authorities should react as quickly as possible by transmitting their views to the Approval authority.

## **H. Paragraph 5.3.5.**

“5.3.5. If it is not possible for the granting Approval Authority to take into account the comments received in accordance with paragraph 5.3.4., the Approval Authorities having sent comments and the granting Approval Authority shall seek further clarification in accordance with Schedule 6 to the 1958 Agreement. The relevant subsidiary Working Party of the World Forum for Harmonization of Vehicle Regulations (WP.29) for this Regulation shall agree on a common interpretation of methods and criteria of assessment. That common interpretation shall be implemented and all Approval Authorities shall issue type approvals under this Regulation accordingly.”

*Explanation of the requirement*

Possible comments of Approval Authorities of other Contracting Parties have no suspensive effect on the issuance of a type approval by the Approval Authority. However, if the latter decides not to take the comments on board, the Approval Authorities having made comments and the Approval Authority having issued a decision are bound to initiate a discussion before the GRVA on the methods and criteria submitted and the comments received. Although the obligation to seek further clarification is on both authorities, it is not necessary for the procedure under Schedule 6 to start that both the Authority having submitted information and the Authority having made comments take formal steps to this effect. Under Schedule 6 paragraph 3, the Chair of the GRVA is required to “identify the issues arising from diverging interpretations” of the Cyber Security Regulation.

The interpretation of the GRVA should be guided by the purpose of the consultation

procedure, as specified under paragraph 5.3.2., hence ensuring convergence in the application of the Regulation. Therefore, it should contain elements permitting to clearly establish whether the minimum performance levels and processes applied by the Approval Authority are sufficient/adequate to verify if the requirements of the Regulation have been complied with. Once the GRVA agrees on the interpretation, this interpretation of the Regulation must be applied by all approval authorities, in all future assessment procedures (for type approvals, modifications and extensions) under the Regulation. This may require updates of the existing methods and criteria by Approval Authorities of certain or all Contracting Parties.

## **I. Paragraph 5.3.6.**

“5.3.6. Each Approval Authority granting a type approval pursuant to this Regulation shall notify other Approval Authorities of the approval granted. The type approval together with the supplementing documentation shall be uploaded in English language by the Approval Authority within 14 days after the day of granting the approval to DETA.”

### *Explanation of the requirement*

This requirement is distinct from and additional to the requirement of notification based on a standard form included in paragraph 5.2. The type approval must be notified together with supplementing documentation which is not specified in paragraph 5.3.6. The objective of sharing is not explicitly stated in the Regulation, but can be inferred from paragraph 5.3.7. it is to allow the approval authorities to “study” the approvals and possibly address “diverging views” in compliance with, notably, Schedule 6. Therefore, the supplementing documentation should include all elements (including test reports) sufficient to permit the approval authorities to understand if and how the methods and criteria referred to in previous paragraphs have been applied in the context of an individual approval decision.

The information must be uploaded to the DETA database. A template for uploading information to the database is provided in section 5.

The obligation of notification in the first sentence of paragraph 5.3.6. is not dependant on possibility to reconcile the requirement of uploading the information to DETA with its obligations under national law pertaining to security and possible confidentiality of the notified information. In the situation where uploading the information to DETA might conflict with such other obligations, the approval authority must find a way to notify the information in a secure manner.

## **J. Paragraph 5.3.7.**

“5.3.7. The Contracting Parties may study the approvals granted based on the information uploaded according to paragraph 5.3.6. In case of any diverging views between Contracting Parties this shall be settled in accordance with Article 10 and Schedule 6 of the 1958 Agreement. The Contracting Parties shall also inform the relevant subsidiary Working Party of the World Forum for Harmonization of Vehicle Regulations (WP.29) of the diverging interpretations within the meaning of Schedule 6 to the 1958 Agreement. The relevant Working Party shall support the settlement of the diverging views and may consult with WP.29 on this if needed.”

### *Explanation of the requirement*

In case of “diverging views” regarding the information on the type approval among the Approval Authorities, reference is made to Article 10 of the Agreement and to Schedule 6. The procedure under Article 10 is reserved for cases where there is dispute on the interpretation of the Agreement. By contrast, any dispute, arising in the context of the

type approval, which concerns the application or interpretation of the Regulation (hence also the application of the methods and criteria referred to in paragraph 5.3.3.) must be solved pursuant to Schedule 6, paragraph 2.

#### **K. Paragraphs 6. to 7.1.1.**

“6. Certificate of Compliance for Cyber Security Management System”

*No guidance included in this document with regards this requirement*

“7. Specifications

7.1. General specifications

7.1.1. The requirements of this Regulation shall not restrict provisions or requirements of other UN Regulations.”

*Explanation of the requirement*

The requirements of this Regulation shall not restrict provisions or requirements of other UN Regulations as well as national or regional legislations as described in points 1.3. and 1.4. of the scope of this Regulation.

#### **L. Paragraphs 7.2. to 7.2.1.**

“7.2. Requirements for the Cyber Security Management System

7.2.1. For the assessment the Approval Authority or its Technical Service shall verify that the vehicle manufacturer has a Cyber Security Management System in place and shall verify its compliance with this Regulation.”

*Explanation of the requirement*

The intention of this requirement is that the Technical Service or Approval Authority shall verify that:

- (a) The vehicle manufacturer has a CSMS;
- (b) The presented CSMS complies to the requirements listed below in this regulation.

For this requirement the focus is on the manufacturer’s processes and assessing if they are in place, in order to get an overview of the capability of the manufacturer to fulfil the requirements of the CSMS.

*The follow clarifications should be noted:*

- (c) The CSMS may be a part of the organization’s Quality Management System or be independent of it;
- (d) If the CSMS is part of the organization’s QMS it should be clearly identifiable.

*Examples of documents/evidence that could be provided*

The following standards may be applicable:

- (e) ISO/SAE 21434 may be used as the basis for evidencing and evaluating the CSMS. Clauses 5 “Overall cybersecurity management”, 6 “Project dependent cybersecurity management”, and 7 “Continuous cybersecurity activities” could be used to evaluate the CSMS in general;
- (f) ISO 18045, ISO 15408, ISO 27000 series, ISO 31000 series may be applicable to relevant parts of the CSMS.

#### **M. Paragraphs 7.2.2. to 7.2.2.1.**

- “7.2.2. The Cyber Security Management System shall cover the following aspects:
- 7.2.2.1. The vehicle manufacturer shall demonstrate to an Approval Authority or Technical Service that their Cyber Security Management System applies to the following phases:
- Development phase;
  - Production phase;
  - Post-production phase.”

*Explanation of the requirement*

The intention of this requirement is that the cybersecurity management system should be able to demonstrate how a manufacturer will handle cybersecurity during the operational life of vehicles produced under a vehicle type. This includes evidencing that there are procedures and processes implemented to cover the three phases. The different phases of the lifecycle may have specific activities to be performed in each of them.

7.2.2.1. describes the different phases of the vehicle type to be considered in the CSMS and 7.2.2.2. applies to all these phases if not stated otherwise. The phases also apply to 7.2.2.4.

The CSMS may include active and/or reactive processes or procedures covering the end of support for a vehicle type and how this is implemented or triggered. It may include the possibility to disconnect non-mandatory functions/systems and under what conditions this might happen.

The operational life (use phase) of an individual vehicle will commence during the production phase of the vehicle type. It will end during either the production phase or post-production phase of the vehicle type.

*Examples of documents/evidence that could be provided*

The following standards may be applicable:

- (a) ISO/SAE 21434 can be used as the basis for evidencing and evaluating the required phases of the CSMS. Clauses 9 “Concept Phase”, 10 “Product Development”, and 11 “Cybersecurity validation” could be used to evaluate the Development phase of the CSMS. Clause 12 “Production” could be used to evaluate the Production phase of the CSMS. Clauses 7 “Continuous cybersecurity activities”, 13 “Operations and maintenance”, and 14 “Decommissioning” could be used to evaluate the Post-production phase of the CSMS;
- (b) Other standards that may be applicable to 7.2.2. and its sub-requirements include: ISO 18045, ISO 15408, ISO 27000 series, ISO 31000 series.

**N. Paragraph 7.2.2.2., part a)**

- “7.2.2.2. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System ensure security is adequately considered, including risks and mitigations listed in Annex 5. This shall include:
- a) The processes used within the manufacturer’s organization to manage cyber security;”

*Explanation of the requirement*

The aim of this requirement is to ensure that the organization has processes to manage the implementation of the CSMS. Its scope is limited to processes that are relevant for the cyber security of the vehicle types and not other aspects of the organization. For example, the scope of this requirement is not intended to cover the entire Information Security

Management System of an organization.

The following could be used to show the range of activities performed by the manufacturer to manage the cyber security of the development, production and post-production phases of a vehicle type:

- (a) Organizational structure used to address cyber security;
- (b) Roles and Responsibilities regarding cybersecurity management incl. accountability.

*Examples of documents/evidence that could be provided*

- (c) ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-05-01], [RQ-05-02], [RQ-05-07], [RQ-05-08];
- (d) BSI PAS 1885 could be used to help evidence this requirement. National certification schemes, like the UK Cyber Essentials, could be used to evidence a manufacturer's organizational processes.

*The requirement should be considered unfulfilled if one of the following statements is true*

- 1. Processes are absent or incomplete.
- 2. Processes are not applied universally or consistently.
- 3. Processes are often or routinely circumvented to achieve business objectives.
- 4. The vehicle manufacturer's security governance and risk management approach has no bearing on its processes.
- 5. System security is totally reliant on users' careful and consistent application of manual security processes.
- 6. Processes have not been reviewed in response to major changes (e.g. technology or regulatory framework), or within a suitable period.
- 7. Processes are not readily available to staff, too detailed to remember, or too hard to understand.

*The requirement may be considered fulfilled if all the following statements are true*

- 1. The vehicle manufacturer fully documents its overarching security governance and risk management approach, technical security practice and specific regulatory compliance. Cyber security is integrated and embedded throughout these processes and key performance indicators are reported to its executive management.
- 2. The vehicle manufacturer's processes are developed to be practical, usable and appropriate for its policies and technologies.
- 3. Processes that rely on user behaviour are practical, appropriate and achievable.
- 4. The vehicle manufacturer reviews and updates processes at suitably regular intervals to ensure they remain relevant. This is in addition to reviews following a major cyber security incident.
- 5. Any changes to the essential function or the threat it faces triggers a review of processes.
- 6. The vehicle manufacturer's systems are designed so that they are, and remain, secure even when user security policies and processes are not always followed. For such claim a justification should be provided.

#### **O. Paragraph 7.2.2.2., part b)**

- “b) The processes used for the identification of risks to vehicle types. Within these processes, the threats in Annex 5, Part A, and other relevant threats

shall be considered.”

*Explanation of the requirement*

The aim of this requirement is for a manufacturer to demonstrate the processes and procedures they use to identify risks to vehicle types.

Processes implemented should consider all probable sources of risk. This shall include risks identified Annex 5 of the Cyber Security Regulation e.g. risks arising from connected services or dependencies external to the vehicle.

Sources for risk identification may be stated. These may include:

- (a) Vulnerability/ Threats sharing platforms;
- (b) Lessons learned regarding risks and vulnerabilities.

*Examples of documents/evidence that could be provided*

The following standards may be applicable:

- (c) ISO/SAE 21434, especially based on [RQ-08-01], [RQ-08-02], [RQ-08-08], [RQ-08-09].

*The processes may consider:*

- (d) Identification the relevance of a system to cybersecurity;
- (e) Description of the overall system with respect to:
  - (i) Definition of the system/function;
  - (ii) Boundaries and interactions with other systems;
  - (iii) Architecture;
  - (iv) Environment of operation of the system (context, constraints and assumptions).
- (f) Identification of assets;
- (g) Identification of threats;
- (h) Identification of vulnerabilities.

*The requirement should be considered unfulfilled if one of the following statements is true*

1. Risk identification is not based on a clearly defined set of assumptions.
2. Risk identification for vehicle types are a "one-off" activity (or not done at all).
3. Vehicle types are assessed in isolation, without consideration of dependencies and interactions with other systems. (e.g. interactions between IT and OT environments).

*The requirement may be considered fulfilled if all the following statements are true*

1. The vehicle manufacturer’s organisational process ensures that security risks to vehicle types are identified, analysed, prioritised, and managed.
2. The vehicle manufacturer’s approach to risk is focused on the possibility of adverse impact to its vehicle types, leading to a detailed understanding of how such impact might arise as a consequence of possible attacker actions and the security properties of its networks and systems.
3. The vehicle manufacturer’s risk identification is based on a clearly understood set of assumptions, informed by an up-to-date understanding of security threats to its vehicle types and its sector.
4. The vehicle manufacturer’s risk identification is informed by an understanding of the vulnerabilities in its vehicle types.



5. The vehicle manufacturer performs detailed threat analysis and understand how this applies to your its organisation in the context of the threat to its vehicle types and its sector.

**P. Paragraph 7.2.2.2., part c)**

- “c) The processes used for the assessment, categorization and treatment of the risks identified;”

*Explanation of the requirement*

The aim of this requirement is that the manufacturer demonstrates the processes and rules they use to assess, categorize and treat risks identified.

*Examples of documents/evidence that could be provided*

The following standards may be applicable:

- (a) ISO/SAE 21434, especially based on [RQ-08-11], [RQ-08-04], [RQ-08-06], [RQ-08-10], [RQ-08-12], [RQ-09-07], [RQ-05-06], [RQ-09-08];
- (b) BSI PAS 11281:2018 may be applicable for the consideration of safety and security.

*The processes may consider:*

- (c) Assessing the associated impact related to the risks identified in requirement 7.2.2.2. b);
- (d) Identification of potential attack paths related to risks identified in requirement 7.2.2.2. b);
- (e) Determination of feasibility/likelihood of attack for every attack paths identified above;
- (f) Calculation and categorization of risks;
- (g) Treatment options of those identified and categorized risks.

*The requirement should be considered unfulfilled if one of the following statements is true*

1. Risk assessment outputs are too complex or unwieldy to be consumed by decision-makers and are not effectively communicated in a clear and timely manner.
2. Security requirements and mitigation techniques are arbitrary or are applied from a control catalogue without consideration of how they contribute to the security of vehicle types.
3. Only certain domains or types of asset are documented and understood. Dependencies between assets are not understood (such as the dependencies between IT and OT).
4. Inventories of assets relevant to vehicle types are incomplete, non-existent, or inadequately detailed.
5. Asset inventories are neglected and out of date.
6. Systems are assessed in isolation, without consideration of dependencies and interactions with other systems (e.g. interactions between IT and OT environments).
7. Risk assessments are not based on a clearly defined set of assumptions.
8. Risk assessments for vehicle types are a "one-off" activity (or not done at all).

*The requirement may be considered fulfilled if all the following statements are true*

1. The output from the vehicle manufacturer's risk management process is a clear set of security requirements that will address the risks in line with its organisational

approach to security.

2. All assets relevant to the secure operation of its vehicle types are identified and inventoried (at a suitable level of detail).
3. The inventory is kept up-to-date.
4. Dependencies on supporting infrastructure are recognised and recorded.
5. The vehicle manufacturer has prioritised assets according to their importance to the operation of its vehicle types.
6. The vehicle manufacturer's risk identification is based on a clearly understood set of assumptions, informed by an up-to-date understanding of security threats to its vehicle types and its sector.
7. The vehicle manufacturer's risk identification is informed by an understanding of the vulnerabilities in its vehicle types.
8. The manufacturer can demonstrate the effectiveness and repeatability of their processes for their categorisation and treatment of risk.

**Q. Paragraph 7.2.2.2., part d)**

- “d) The processes in place to verify that the risks identified are appropriately managed;”

*Explanation of the requirement*

The aim of this requirement is that the manufacturer demonstrates the processes and rules they use to decide how to manage the risks. This can include the decision criteria for risk treatment, e.g. the process for selecting what controls to implement and when to accept a risk.

The results of the process for risks identification and assessment should feed into selecting the appropriate treatment category options to address those risks. The outcome of this process should be that the residual risk (risks remaining after treatment) is within the manufacturer's stated tolerance of risks (i.e. within stated acceptable limits).

Mitigations identified in Annex 5 of the Cyber Security Regulation shall be considered in the processes.

*Examples of documents/evidence that could be provided*

The following standards may be applicable:

- (a) ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-09-09];
- (b) ISO 31000 may be applicable if adapted for product related risks.

*The processes may consider:*

- (c) Appropriate and proportional risk treatment methodologies;
- (d) Treatment of critical elements (with safety and environment) to ensure the risks to them are appropriately mitigated and proportionately based on the safety or environmental goal of dependent vehicle systems;
- (e) Ensuring the residual risk remains within acceptable limits for components or the overall vehicle type;
- (f) Detailing any cases where the organization would accept justification for non-adherence to their stated risk tolerance.

*The requirement should be considered unfulfilled if one of the following statements is true*

1. The security elements of projects or programmes are solely dependent on the completion of a risk management assessment without any regard to the outcomes.
2. There is no systemic process in place to ensure that identified security risks are managed effectively.
3. Risks remain unresolved on a register for prolonged periods of time awaiting senior decision-making or resource allocation to resolve.

*The requirement may be considered fulfilled if all the following statements are true*

1. Significant conclusions reached in the course of the vehicle manufacturer's risk management process are communicated to key security decision-makers and accountable individuals.
2. The effectiveness of the vehicle manufacturer's risk management process is reviewed periodically, and improvements made as required.

## **R. Paragraph 7.2.2.2., part e)**

“e) The processes used for testing the cyber security of a vehicle type;”

*Explanation of the requirement*

The aim of this requirement is to ensure the manufacturer has appropriate capabilities and processes for testing the vehicle type throughout its development and production phases.

Testing processes in the production phase may be different to the ones used during the development phase.

*Examples of documents/evidence that could be provided*

The following standards may be applicable:

- (a) ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-09-10], [RQ-10-01], [RQ-11-01], [RQ-11-02], [RQ-12-01];
- (b) BSI PAS 11281:2018 may be utilised for considering the interaction of safety and security and processes for evidencing security outcomes are met.

*The processes may consider:*

Development Phase:

- (c) Organization specific rules for testing during development;
- (d) Processes for creation and execution of test strategies;
- (e) Processes for cybersecurity testing planning;
- (f) Processes for cybersecurity system design testing;
- (g) Processes for cybersecurity software unit testing;
- (h) Processes for cybersecurity hardware testing;
- (i) Processes for cybersecurity integration testing;
- (j) Processes for documentation of the results of testing;
- (k) Processes for handling vulnerabilities identified during testing;
- (l) Justification and requirements for cybersecurity tests, like Functional (requirement-based, positive and negative) testing, Interface testing, Penetration testing, Vulnerability scanning, Fuzz testing but not limited to the same.

Production Phase:

- (m) Processes for testing to ensure the produced system has the cybersecurity

requirements, controls and capabilities outlined in the production plan;

- (n) Processes for testing to ensure the produced item meets the cybersecurity specifications which are in accordance with the system in the development phase;
- (o) Processes for testing to assure that cybersecurity controls and configuration as cybersecurity specifications are enabled in the produced item;
- (p) Processes for documenting the test results and findings handling.

*The requirement should be considered unfulfilled if one of the following statements is true*

- 1. A particular product or service is seen as a "silver bullet" and vendor claims are taken at face value.
- 2. Assurance methods are applied without appreciation of their strengths and limitations, such as the risks of penetration testing in operational environments.
- 3. Assurance is assumed because there have been no known problems to date.

*The requirement may be considered fulfilled if all the following statements are true*

- 1. The vehicle manufacturer validates that the security measures in place to protect systems are effective and remain effective until the end-of-life of all vehicles under the vehicle types for which they are needed.
- 2. The vehicle manufacturer understands the assurance methods available to it and chooses appropriate methods to gain confidence in the security of vehicle types.
- 3. The vehicle manufacturer's confidence in the security as it relates to its technology, people, and processes can be justified to, and verified by, a third party.
- 4. Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way.
- 5. The methods used for assurance are reviewed to ensure they are working as intended and remain the most appropriate method to use.

#### **S. Paragraph 7.2.2.2., part f)**

“f) The processes used for ensuring that the risk assessment is kept current;”

*Explanation of the requirement*

The aim of this requirement is to ensure the risk assessment is kept current. This should include processes to identify if the risks to a vehicle type have changed and how this will be considered within the risk assessment.

Sources for risk identification may be stated. These may include:

- (a) Vulnerability/ Threats sharing platforms;
- (b) Lessons learned regarding risks and vulnerabilities;
- (c) Conferences.

It is noted that requirements 7.2.2.2. parts f) to h) may have overlaps in terms of the processes used and therefore the same evidence may be applicable to demonstrating that these requirements are met.

*Examples of documents/evidence that could be provided*

- (d) ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-11-03], [RQ-06-08], [RQ-07-05], [RQ-07-06].

*The requirement should be considered unfulfilled if one of the following statements is true*

- 1. No processes are in place which require the risk assessment to be updated.

*The requirement may be considered fulfilled if all the following statements are true*

1. The vehicle manufacturer conducts risk assessments when significant events potentially affect vehicle types, such as replacing a system or a change in the cyber security threat.
2. The vehicle manufacturer's risk assessments are dynamic and updated in the light of relevant changes which may include technical changes to vehicle types, change of use and new threat information.

#### **T. Paragraph 7.2.2.2., part g)**

- “g) The processes used to monitor for, detect and respond to cyber-attacks, cyber threats and vulnerabilities on vehicle types and the processes used to assess whether the cyber security measures implemented are still effective in the light of new cyber threats and vulnerabilities that have been identified;”

##### *Explanation of the requirement*

The aim of this requirement is to ensure that the manufacturer has processes to monitor for cyber-attacks, threats or vulnerability to vehicles that the manufacturer has had type approved, i.e. are in the post-production or production phase, and that they have established processes that would permit them to respond in an appropriate and timely manner.

It is noted that requirements 7.2.2.2. parts f) to h) may have overlaps in terms of the processes used and therefore the same evidence may be applicable to demonstrating that these requirements are met.

##### *Examples of documents/evidence that could be provided*

The following standards may be applicable:

- (a) ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-07-01], [RQ-07-02], [RQ-07-03], [RQ-07-04], [RQ-07-05], [RQ-15-04], [RQ-15-05], [RC-15-03], [RQ-13-01], [RQ-13-02], [RQ-13-03].

##### *The following could be used to evidence the processes used:*

- (b) Cyber security monitoring processes for post-production vehicles. This may include processes that will collect information that may or may not be pertinent to the manufacturer's vehicle/system;
- (c) Cyber security information assessment processes. These will be processes for the identification of the relevance of the information collected with respect to the system/vehicle of the manufacturer;
- (d) Processes for risk determination/assessment for the relevant information;
- (e) Incident response procedures for both vehicles already registered and yet to be registered of the vehicle types covered by the CSMS, which may include evidence of procedures for:
  - (i) Interaction with authorities;
  - (ii) Identified or stated triggers that would lead to an escalation or action;
  - (iii) Determining what response options might be implemented for which condition;
  - (iv) Handling any dependencies and interactions with suppliers.
- (f) Evidence that the response procedures would work, for example through exercising and verification that planning assumptions remain valid under test.

*The requirement should be considered unfulfilled if one of the following statements is true*

1. The vehicle manufacturer has no sources of threat intelligence.
2. The vehicle manufacturer does not apply updates in a timely way, after receiving them.
3. The vehicle manufacturer does not evaluate the usefulness of its threat intelligence or share feedback with providers, authorised aftermarket service providers or other users.
4. There are no staff who perform a monitoring function.
5. Monitoring staff do not have the correct specialist skills.
6. Monitoring staff are not capable of reporting against governance requirements.
7. Security alerts relating to vehicle types are not prioritised.

*The requirement may be considered fulfilled if all the following statements are true*

1. Data relating to the security and operation of vehicle types is collected.
2. Alerts from third parties are investigated, and action taken.
3. Some logging datasets can be easily queried with search tools to aid investigations.
4. The resolution of alerts to an asset or system is performed regularly.
5. Security alerts relating to vehicle types are prioritised.
6. The vehicle manufacturer applies updates in a timely way.
7. The vehicle manufacturer has processes to monitor for, detect and respond to cyber-attacks, cyber threats and vulnerabilities which are relevant to its business needs, or specific threats in its sector.
8. The vehicle manufacturer knows how effective its processes are (e.g. by tracking how they helps it identify security problems).
9. Monitoring staff have appropriate investigative skills and a basic understanding of the data they need to work with.
10. Monitoring staff can report to other parts of the organisation (e.g. security directors, resilience managers).
11. The vehicle manufacturer successfully demonstrates the processes to evaluate whether the cyber security measures implemented are robust enough to conclude whether they are still effective.

#### **U. Paragraph 7.2.2.2., part h)**

- “h) The processes used to provide relevant data to support analysis of attempted or successful cyber-attacks;”

##### *Explanation of the requirement*

The intention of this requirement is to ensure that a process has been established to provide the data required for analysis and associated responsibilities for handling the data and analysis.

- (a) ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-07-03].

##### *Examples of documents/evidence that could be provided*

The following could be used to evidence the processes used:

- (b) Procedure for implementing Security Incident Response Team activities (incidents);

- (c) Field monitoring (obtaining information on incidents and vulnerabilities);
- (d) Procedure when an incident occurs (including an overview of what information is passed to the analyst in what steps);
- (e) Procedure when a vulnerability is discovered (including an overview of what information is passed to the analyst in what steps).

## **V. Paragraph 7.2.2.3.**

“7.2.2.3. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that, based on categorization referred to in paragraph 7.2.2.2. (c) and 7.2.2.2. (g), cyber threats and vulnerabilities which require a response from the vehicle manufacturer shall be mitigated within a reasonable timeframe.”

### *Explanation of the requirement*

The intention of this requirement is to ensure that after the identified risks have been classified, a process has been established to determine the response time limit based on the classification results.

It is necessary to set the response deadline by processes such as triage and explain the monitoring process to see if it is executed within the deadline.

The timeframes provided by the manufacturers should be able to be justified and explained. There may be a set of timeframes covering different possible situations. This should include timeframes for deciding and implementing possible reactions or responses.

ISO/SAE 21434 can be used as the basis for evidencing the required processes, especially based on [RQ-05-02] b).

### *Examples of documents/evidence that could be provided*

The following could be used to evidence the processes used:

- (a) Procedure for implementing cyber security incident response activities, including:
  - (i) Field monitoring (obtaining information on incidents and vulnerabilities);
  - (ii) Procedure for incident handling, including how the timeframe to respond is determined;
  - (iii) Procedures for discovering vulnerabilities.
- (b) Demonstration of how the procedures are implemented.

## **W. Paragraph 7.2.2.4.**

“7.2.2.4. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that the monitoring referred to in paragraph 7.2.2.2. (g) shall be continual. This shall:

- (a) Include vehicles after first registration in the monitoring;
- (b) Include the capability to analyse and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs. This capability shall respect paragraph 1.3. and the privacy rights of car owners or drivers, particularly with respect to consent.”

### *Explanation of the requirement*

The intention of this requirement is to ensure that processes of monitoring for cyber-attacks, cyber threats and vulnerabilities on vehicle types are continual and apply to all

registered vehicles of the manufacturer that fall within the scope of their Cyber Security Management System and use:

- a) the information on monitoring acquired in accordance with 7.3.7. in addition to other sources of information on monitoring acquired in accordance with 7.2.2.2. (g) (such as social media).

It is noted that paragraph 1.3., and compliancy with data privacy laws, are particularly relevant to this requirement,

ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on 7.3 “Cybersecurity Monitoring”, 7.4 “Cybersecurity event assessment”, 7.5 “Vulnerability analysis.

*Examples of documents/evidence that could be provided*

The following could be used to evidence the processes used:

- (b) Procedure for implementing cyber security incident response activities, including:
  - (i) Field monitoring (obtaining information on incidents and vulnerabilities)
  - (ii) Procedure for incident handling
  - (iii) Procedures for discovering vulnerabilities
- (c) Demonstration of how the procedures are implemented.

## **X. Paragraph 7.2.2.5.**

“7.2.2.5. The vehicle manufacturer shall be required to demonstrate how their Cyber Security Management System will manage dependencies that may exist with contracted suppliers, service providers or manufacturer’s sub-organizations in regards of the requirements of paragraph 7.2.2.2.”

*Explanation of the requirement*

The intention of this requirement is to ensure that it can be shown that risks from suppliers are able to be known and can be managed within the processes described in the CSMS. The steps taken should be proportionate to the risks from what is supplied.

The final implementation of the processes may be incorporated into bilateral agreement between the vehicle manufacturer and their suppliers.

Within the CSMS there may be processes to:

- (a) identify risks associated with parts, components, systems or services provided by suppliers;
- (b) manage risks to the vehicle coming from service providers providing connectivity functions or services that a vehicle may rely on, this may include for example cloud providers, telecom providers, internet providers and authorised aftermarket service providers;
- (c) ensure contracted suppliers and/or service providers are able to evidence how they have managed risks associated with them. The processes may include consideration of validation or testing requirements that may be used to evidence that risks are appropriately managed;
- (d) delegate relevant requirements to relevant departments or sub-organisations of the manufacturer, in order to manage risks identified.

It is noted that it is possible to put requirements on Tier1 suppliers and to require they cascade it to Tier 2 suppliers. However, it may be difficult for a manufacturer to cascade requirements further down in the supply chain (especially legally binding requirements).



*Examples of documents/evidence that could be provided*

The following standards may be applicable:

- (e) ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-06-09], [RQ-15-03], [RC-15-02].

*The following could be used to evidence the processes used:*

- (f) Contractual agreements in place or evidence of such agreements;
- (g) Evidenced arguments for how their processes will ensure suppliers / service providers will be considered in the risk assessment process;
- (h) Procedures/Methods of sharing information on risk between suppliers and manufacturers;
- (i) Existing solutions / contracts like ISMS (Information Security Management System) regulation can be used for evidence. This may be evidenced by certificates based on ISO/IEC 27001 or TISAX (Trusted Information Security Assessment eXchange).

*The requirement should be considered unfulfilled if one of the following statements is true*

1. Relevant contracts with suppliers and service providers do not have cyber security requirements.

*The requirement may be considered fulfilled if all the following statements are true*

1. The vehicle manufacturer has a deep understanding of its supply chain, including sub-contractors and the wider risks it faces. The vehicle manufacturer considers factors such as supplier's partnerships, competitors, nationality and other organisations with which they sub-contract. This informs its risk assessment and procurement processes.
2. The vehicle manufacturer's approach to supply chain risk management considers the risks to its vehicle types arising from supply chain subversion by capable and well-resourced attackers.
3. The vehicle manufacturer has confidence that information shared with suppliers that is essential to the operation of your vehicle types is appropriately protected from sophisticated attacks.
4. The vehicle manufacturer can clearly express the security needs it places on suppliers in ways that are mutually understood and are laid in contracts. There is a clear and documented shared-responsibility model.
5. All network connections and data sharing with third parties is managed effectively and proportionately.
6. When appropriate, the vehicle manufacturer's incident management process and that of its suppliers provide mutual support in the resolution of incidents.

**Y. Paragraphs 7.3. to 7.3.1.**

"7.3. Requirements for vehicle types

7.3.1. The manufacturer shall have a valid Certificate of Compliance for the Cyber Security Management System relevant to the vehicle type being approved.

However, for type approvals prior to 1 July 2024, if the vehicle manufacturer can demonstrate that the vehicle type could not be developed in compliance with the CSMS, then the vehicle manufacturer shall demonstrate that cyber security was adequately considered during the development phase of the vehicle type concerned."

*Explanation of the requirement*

The intention of this requirement is to ensure that there is a valid Certificate of Compliance for CSMS to enable type approval to be given for any new vehicle type and that it is appropriate to the vehicle type.

*The following clarification should be noted:*

- (a) "relevant to the vehicle type being approved." means the CSMS should be applicable to the vehicle type being approved.

*Examples of documents/evidence that could be provided*

The following could be used to evidence the validity of the CSMS certificate:

- (b) The Certificate of Compliance for CSMS to demonstrate it is still valid;
- (c) Confirmation that the CSMS is appropriately applied to the vehicle type and any information required to provide assurance.

**Z. Paragraph 7.3.2.**

“7.3.2. The vehicle manufacturer shall identify and manage, for the vehicle type being approved, supplier-related risks”

*Explanation of the requirement*

This requirement specifically references gaining sufficient information from the supply chain and is linked to 7.2.2.5. The intention of this requirement is to ensure that information presented (together with that from the manufacturer) is sufficient to allow an assessment to be conducted of the requirements 7.3.3. to 7.3.6.

*The following clarification should be noted:*

- (a) "supplier-related risks" - The aim is that it can be shown that risks from suppliers are able to be known and can be managed. It is accepted that it is difficult to cascade requirements down in the supply chain beyond Tier 2 suppliers and ensure they are legally binding.

*Examples of documents/evidence that could be provided*

The following standards may be applicable:

- (b) ISO/SAE 21434.

The following could be used to evidence the processes used:

- (c) Evidence in the form of contract sections with suppliers that deal with the requirements of this regulation.

**AA. Paragraph 7.3.3.**

“7.3.3. The vehicle manufacturer shall identify the critical elements of the vehicle type and perform an exhaustive risk assessment for the vehicle type and shall treat/manage the identified risks appropriately. The risk assessment shall consider the individual elements of the vehicle type and their interactions. The risk assessment shall further consider interactions with any external systems. While assessing the risks, the vehicle manufacturer shall consider the risks related to all the threats referred to in Annex 5, Part A, as well as any other relevant risk.”

*Explanation of the requirement*

The intention of this requirement is that the vehicle manufacturers shall identify the

critical elements of a vehicle type with respect to cyber security and provide justification for how risks related to them are managed.

The manufacturer should be able to provide justification for why they have identified elements of a vehicle type as critical (or not).

*The following clarifications should be noted*

- (a) Critical elements may be elements contributing to vehicle safety, environment protection or theft protection. They could be parts which provide connectivity. They may also be parts of the vehicle architecture which are critical for sharing information or cyber security (e.g. gateways could be also considered critical);
- (b) The intention of this requirement is to ensure that risks shall be appropriately processed / managed by considering all threats including Annex 5, Part A and judging the necessity of countermeasures based on the results of risk analysis and risk evaluation;
- (c) The intention of this requirement is to allow the vehicle manufacturer to demonstrate the application of the relevant process in requirements 7.2.2.2. and 7.2.2.4. of the CSMS to the vehicle type;
- (d) The approval authority or technical service shall refer to Annex 5 of the Cyber Security Regulation to aid their assessment of the manufacturer's risk assessment;
- (e) The consideration of risks should consider the requirements of 7.3.4. and the requirement for proportionate mitigations;
- (f) The consideration of the threats and mitigations of Annex 5 within a risk assessment may lead to ratings like "not relevant" or "negligible risks".

*Examples of documents/evidence that could be provided*

The following standards may be applicable:

- (g) ISO/SAE 21434 describes the way to define the concept. This also includes the consideration of critical elements based on risk treatment decisions. The results are documented in "Cybersecurity goals" and "Cybersecurity concept". It further describes exhaustive risk assessment in clause 8 "Risk assessment methods". This is documented in Threat analysis and risk assessment;
- (h) ETSI TS 103 645 may be used for demonstrating the security of Internet of Things elements of a vehicle;
- (i) BSI PAS 1885 may be used.

The following could be used to evidence this requirement:

- (j) The vehicle type claimed;
- (k) An explanation of why elements within the vehicle type are critical;
- (l) What security measures are implemented, including information on how they work;
- (m) Information on any security measures should permit the Technical Service/ Approval Authority to both be assured that they do what the manufacturer intends and that vehicles in production will use the same measure as presented to the Approval Authority/Technical Service for the vehicle type. Confidentiality of specifics and how these are handled should be agreed and recorded.

## **AB. Paragraph 7.3.4.**

"7.3.4. The vehicle manufacturer shall protect the vehicle type against risks identified in the vehicle manufacturer's risk assessment. Proportionate mitigations shall be implemented to protect the vehicle type. The

mitigations implemented shall include all mitigations referred to in Annex 5, Part B and C which are relevant for the risks identified. However, if a mitigation referred to in Annex 5, Part B or C, is not relevant or not sufficient for the risk identified, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented.

In particular, for type approvals prior to 1 July 2024, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented if a mitigation measure referred to in Annex 5, Part B or C is technically not feasible. The respective assessment of the technical feasibility shall be provided by the manufacturer to the approval authority.”

#### *Explanation of the requirement*

The intention of this requirement is to ensure that vehicle manufacturers implement appropriate mitigation measures in accordance with the results of their risk assessment.

The manufacturer should provide reasoned arguments and evidence for the mitigations they have implemented in the design of the vehicle type and why they are sufficient. This may include any assumptions made, for example about external systems that interact with the vehicle.

The technical mitigations from Annex 5, Parts B and C shall be considered wherever applicable to the risks to be mitigated. The Manufacturer may present a rationale not only for a listed mitigation from Annex 5 being “not relevant or not sufficient”, but also may present a rationale, that another mitigation other than the ones listed in Annex 5 is appropriate to the respective risk. That rationale may be substantiated by a risk assessment and risk rating showing the appropriateness of the alternative mitigation. This is to allow the adoption of new or improved defensive technologies.

#### *The following clarifications should be noted:*

- (a) The design decisions of the manufacturer should be linked to the risk assessment and risk management strategy. The manufacturer should be able to justify the strategy implemented;
- (b) The term “proportionate” should be considered when choosing whether to implement a mitigation and what mitigation should be implemented. If the risk is negligible then it may be argued that a mitigation would not be necessary;
- (c) Protection from identified risks means to mitigate the risk.

#### *Examples of documents/evidence that could be provided*

The following standards may be applicable:

- (d) ISO/SAE 21434 describes the identification of risk and the deduced Cybersecurity goals and concept based on the identified risks. The results are documented in [WP-09-04] Cybersecurity goals and [WP-09-07] Cybersecurity concept;
- (e) BSI PAS 11281: 2018 and other standards regarding claims, arguments and evidence may be used to justify the design decisions of the manufacturer.

The following could be used to evidence the mitigations used:

- (f) Evidence that mitigation measures were introduced according to the necessity of measures, this includes:
  - (i) the reason, if mitigation measures other than Annex 5 Part B and C are applied;
  - (ii) the reason, if mitigations listed in Annex 5 are not applied;
  - (iii) the reason, if mitigation measures are determined to be unnecessary.

## **AC. Paragraph 7.3.5.**

“7.3.5. The vehicle manufacturer shall put in place appropriate and proportionate measures to secure dedicated environments on the vehicle type (if provided) for the storage and execution of aftermarket software, services, applications or data.”

*The following clarifications should be noted:*

- (a) "appropriate and proportionate measures" requires that the manufacturer is able to justify how risks associated with any dedicated environment, as defined in their risk assessment, are managed;
- (b) Dedicated environments can be on the vehicle. If the vehicle interacts with servers or services located off the vehicle (for example in the cloud) then the risks to the vehicle originating from them, with respect to their cyber security, should be considered.

*Examples of documents/evidence that could be provided*

The following standards may be applicable:

- (c) ISO/SAE 21434 describes on a process base steps to make conclusion for the architecture. This aspect is to be considered in [WP-08-03] Threat scenarios.

The following could be used to evidence this requirement:

- (d) A description of the dedicated environment;
- (e) What security measures are implemented, including information on how they work;
- (f) Information on any security measures should permit the Approval Authority/Technical Service to both be assured that they do what the manufacturer intends and that vehicles in production will use the same measure as presented to the Approval Authority/Technical Service for the vehicle type. Confidentiality of specifics and how these are handled should be agreed and recorded;
- (g) Annex 5 of the cyber security Regulation shall be referred to.

## **AD. Paragraph 7.3.6.**

“7.3.6. The vehicle manufacturer shall perform, prior to type approval, appropriate and sufficient testing to verify the effectiveness of the security measures implemented.”

*Explanation of the requirement*

The test results should be valid at time of type approval. The Technical Service may perform security tests to confirm the results.

*The following clarifications should be noted:*

- (a) The aim of any security measures will be to reduce the risks. Testing should support justification for the security measures implemented.

*Examples of documents/evidence that could be provided*

The following standards may be applicable:

- (b) Manufacturers may describe the verification and validation measure implemented in accordance with ISO/SAE 21434 in form of [WP-09-08] Verification report of cybersecurity concept, [WP-10-03] Verification report for the refined cybersecurity specification, [WP-11-02] Validation report.

The following could be used to evidence this requirement:

- (c) What is tested and why (e.g. what measures of success for the test look like);
- (d) Methodology used and why (e.g. this may include notes on the extent and effort contained within the testing);
- (e) Who has performed the tests and why (e.g. in-house, a supplier or an external organization and any relevant information regarding their qualification/experience);
- (f) Confirmation of its successful outcome (this may include the pass/fail criteria and result of the test).

## **AE. Paragraph 7.3.7.**

“7.3.7. The vehicle manufacturer shall implement measures for the vehicle type to:

- (a) detect and prevent cyber-attacks against vehicles of the vehicle type;
- (b) support the monitoring capability of the vehicle manufacturer with regards to detecting threats, vulnerabilities and cyber-attacks relevant to the vehicle type;
- (c) provide data forensic capability to enable analysis of attempted or successful cyber-attacks.”

### *Explanation of the requirement*

The intention of this requirement is to ensure that there are specific measures implemented for the vehicle type to monitor for changes in the threat landscape, detect and prevent cyber-attacks and have the capability to forensically support the analysis of any attempted or successful attack.

### *The following clarifications should be noted:*

- (a) Measures with regard to this clause may be implemented on the vehicle type or in its operational environment, e.g. the backend, the mobile network “for the vehicle type”;
- (b) Measures should primarily look to prevent cyber-attacks being successful, with reference to 7.3.4. and 7.3.5. to protect against risks identified in the risk assessment;
- (c) Measures to prevent cyber-attacks being successful against all vehicles of a vehicle type may additionally be delivered asynchronously, i.e. after the actual event of a cyber-attack and its analysis;
- (d) Data forensic capability may include the ability to provide and analyse log data, diagnostic error codes, vehicle operational information, backend information to investigate cyber-attacks;
- (e) Data forensic capability may include a circular buffer of persisting log data that supports investigatory procedures.

It is noted that paragraph 1.3., and compliancy with data privacy laws, are particularly relevant to this requirement.

### *Examples of documents/evidence that could be provided*

The following standards may be applicable:

- (f) ISO/SAE 21434. A list of sources for cybersecurity monitoring is provided in clause 7.3. The results of analysis and how to document it is described in [WP-07-04] Vulnerability analysis.

The following could be used to evidence this requirement:

- (g) Attack prevention measures applied to the vehicle type;
- (h) Demonstration of how a vehicle type's preventive measures and monitoring activities perform;
- (i) Demonstration of how forensic analysis is performed.

#### **AF. Paragraph 7.3.8.**

“7.3.8. Cryptographic modules used for the purpose of this Regulation shall be in line with consensus standards. If the cryptographic modules used are not in line with consensus standards, then the vehicle manufacturer shall justify their use.”

*The following clarifications should be noted:*

A consensus standard may be an internationally recognised standard, or it may be a national standard that is commonly used, e.g. FIPS.

*Explanation of the requirement*

The intent of this requirement is to ensure encryption methods used can be justified.

*Examples of documents/evidence that could be provided*

Where encryption measures are implemented, based on the results of risk analysis and risk assessment, the manufacturer should be able to:

- (a) Explain whether the encryption algorithm or measure complies with a current consensus standard; and
- (b) Explain the reason for the choice of encryption and why it adequately mitigates the risk identified.

#### **AG. Paragraph 7.4.**

“7.4. Reporting provisions

7.4.1. The vehicle manufacturer shall report at least once a year, or more frequently if relevant, to the Approval Authority or the Technical Service the outcome of their monitoring activities, as defined in paragraph 7.2.2.2.(g), this shall include relevant information on new cyber-attacks. The vehicle manufacturer shall also report and confirm to the Approval Authority or the Technical Service that the cyber security mitigations implemented for their vehicle types are still effective and any additional actions taken.”

*Explanation of the requirement*

The main purpose of this requirement is to confirm that the aspects of the CSMS related to the cyber security monitoring activities, as defined in paragraph 7.2.2.2.(g), continue to be applied properly after Development Phase and that the relevant cyber security mitigations implemented continue to be effective.

The manufacturer shall at least annually report to the Type Approval Authority who granted the type approval or the Technical Service who verified the compliance of its CSMS with this Regulation. The reporting should be more frequent if events such as new cyber-attacks are observed, especially to report on any actions taken.

*Examples of documents/evidence that could be provided*

The following standards may be applicable:

- (a) ISO/SAE 21434 defines [WP-07-02] Results from the triage of cybersecurity information and [WP-07-04] Vulnerability Analysis. Both can be used as the

baseline for the required reporting.

**AH. Paragraph 7.4.2.**

“7.4.2. The Approval Authority or the Technical Service shall verify the provided information and, if necessary, require the vehicle manufacturer to remedy any detected ineffectiveness.

If the reporting or response is not sufficient the Approval Authority may decide to withdraw the CSMS in compliance with paragraph 6.8.”

*No guidance included in this document with regards this requirement*

**AI. Paragraph 8.**

“8. Modification and extension of the vehicle type”

*Examples of documents/evidence that could be provided*

The following table gives some examples for modifications of E/E architectures and the potential impact on the vehicle type with regard to this regulation.

Note, the examples given are indicative of what may be considered but should not be viewed as limiting. When applied the example of changes given may result in a different outcome.



|                            | Possible <b>changes</b> in the E/E Architecture | Impact on type                                                                                                                                                                                        | Examples                                                                                                                                                                                                                                  |
|----------------------------|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| New type                   |                                                 | Development of an E/E Architecture requires a <b>new type</b> .                                                                                                                                       | Development of an E/E Architecture requires a <b>new type</b> .                                                                                                                                                                           |
|                            |                                                 | Requires a <b>new type</b> , since security in existing subsystem is being influenced.                                                                                                                | <ul style="list-style-type: none"> <li>• Adding new external interfaces (NFC Near Field Communication) for new services such as personalization</li> <li>• Change of network topology by adding a new gateway</li> </ul>                  |
| Extension of existing type |                                                 | Replacing an existing subsystem or adding a new subsystem, and this introduces some minor changes to the cybersecurity of the resulting E/E architecture, and <b>thus requires a type extension</b> . | <ul style="list-style-type: none"> <li>• Replacing a UMTS communication unit by a 5G communication unit -&gt; additional communication possible</li> <li>• Replacing an ECU by a new one with a HSM (hardware security module)</li> </ul> |
|                            |                                                 |                                                                                                                                                                                                       |                                                                                                                                                                                                                                           |
| No impact                  |                                                 | Replacing an existing subsystem, and this does not change the cybersecurity of the resulting E/E architecture, and thus does <b>not require a type extension. This is the usual situation.</b>        | Replacing an ECU:<br>new state of the art processor, more memory, no                                                                                                                                                                      |

**AJ. Paragraphs 9. to 12.**

- “9. Conformity of production
- 10. Penalties for non-conformity of production
- 11. Production definitively discontinued
- 12. Names and addresses of Technical Services responsible for conducting approval test, and of Type Approval Authorities”

*No guidance included in this document with regards this requirement*

## **4. Guidance regarding Annex 1, the Information Document**

### **A. Paragraphs 9. to 9.1.**

- “9. Cyber Security
- 9.1. General construction characteristics of the vehicle type, including:
- (a) The vehicle systems which are relevant to the cyber security of the vehicle type;
  - (b) The components of those systems that are relevant to cyber security;
  - (c) The interactions of those systems with other systems within the vehicle type and external interfaces.”

*Examples of documents/evidence that could be provided*

Shall be a written description of the E/E architecture

### **B. Paragraph 9.2.**

- “9.2. Schematic representation of the vehicle type”

*Examples of documents/evidence that could be provided*

Shall be a schematic of the E/E architecture – e.g. circuit diagram

### **C. Paragraphs 9.3. to 9.8.**

- “9.3. The number of the Certificate of Compliance for CSMS:
- 9.4. Documents for the vehicle type to be approved describing the outcome of its risk assessment and the identified risks:
- 9.5. Documents for the vehicle type to be approved describing the mitigations that have been implemented on the systems listed, or to the vehicle type, and how they address the stated risks:
- 9.6. Documents for the vehicle type to be approved describing protection of dedicated environments for aftermarket software, services, applications or data:
- 9.7. Documents for the vehicle type to be approved describing what tests have been used to verify the cyber security of the vehicle type and its systems and the outcome of those tests:
- 9.8. Description of the consideration of the supply chain with respect to cyber security:”

*No guidance included in this document with regards this requirement*

## 5. Template for data exchange via DETA in accordance with paragraph 5.3.

### Important Note:

Information obtained through DETA for the purpose of information sharing scheme which is defined in the UN Regulation shall be protected in a secure manner. This information shall not be used for other purposes rather than vehicle type approval and certification of cyber security management system for vehicle type.

### 5.1. Description of CSMS auditing

For the description of the CSMS audit the approval authority shall provide the following information to DETA.

#### 5.1.1. Auditing process

Contact data of the approval authority and its organisational unit responsible for the audit process shall be provided.

The audit process should be documented in a process flow chart, including possible iterative steps and remediation workflow.

(Flow chart)

The chronological workflow of the audit should be documented in table format.

| Audit phase                                                                                                                               | Start date / time span | Resource requirement<br>(in man-days) |
|-------------------------------------------------------------------------------------------------------------------------------------------|------------------------|---------------------------------------|
| Pre-audit, if required<br><i>e.g. involvement of auditors in productive processes, planning of audit, adaptation of audit workflow</i>    |                        |                                       |
| Document handover                                                                                                                         |                        |                                       |
| Preparation for audit activities<br><i>Including document review, e.g. sort, check for completeness, audit of contents</i>                |                        |                                       |
| Conducting the on-site audit                                                                                                              |                        |                                       |
| Assessment of rectification efforts<br><i>e.g. rectifications completed by auditee during the audit may address findings of the audit</i> |                        |                                       |
| Preparation and distribution of the audit report                                                                                          |                        |                                       |
| Findings from the audit                                                                                                                   |                        |                                       |
| Review of findings and rectifications by applicant (where applicable)                                                                     |                        |                                       |
| Audit completion                                                                                                                          |                        |                                       |

If deemed necessary additional information concerning the audit phases can be documented in the table below.

| Audit-phase | Remarks |
|-------------|---------|
|             |         |

The information shall also include the workflow for verification measures according to UN Regulation No. 155, paragraphs 6.8. and 6.10. and re-audit according to UN Regulation No. 155, paragraph 6.10.

#### 5.1.1.1. Conducting the On-site audit

If on-site assessments of the CSMS of applicants are part of the audit process, then the workflow and basic principles (rationale) of these shall be described.

#### 5.1.1.2. Handling of findings and rectification efforts

This chapter describes the workflow associated with the rectification efforts of the auditee to address the audit findings.

(The respective workflow should be included in the flow chart in 5.1.1.)

#### 5.1.1.3. Samples of application forms

A sample form for the application, for CSMS certification shall be documented.

#### 5.1.1.4. References to standards and specifications

Any standard, specification or other external document on which (parts of) the audit process and assessment criteria are based shall be referenced.

#### 5.1.2. Qualification requirements and auditing team setup

Here the minimum requirements of the approval authority on technical services and auditors conducting CSMS assessments shall be laid down. The positions in a potential auditing team shall be listed. Qualifications shall be attributed to auditing team position.

##### 5.1.2.1. Potential auditing team setup

| Position<br><i>Examples</i> | Staffing requirement<br><i>Examples</i> | Tasks/remarks<br><i>Examples</i>                                                                  |
|-----------------------------|-----------------------------------------|---------------------------------------------------------------------------------------------------|
| Lead auditor                | 1                                       | Manage audit process; accountable and responsible                                                 |
| CS process expert           | 2                                       | Responsible for process audit; ideally personal staffing overlap with type approval assessor team |
| Product expert              | 1                                       | ...                                                                                               |
| ...                         | ...                                     |                                                                                                   |
| Documentation Management    |                                         |                                                                                                   |

##### 5.1.2.2. Qualification requirements

| Qualification            | Concerned Positions                                | Minimum requirement                                                                                    | Evidence                                |
|--------------------------|----------------------------------------------------|--------------------------------------------------------------------------------------------------------|-----------------------------------------|
| Educational achievements | <i>Example:</i><br>Lead auditor, CS process expert | <i>Example:</i> University degree in computer science, mathematics, physics, engineering or similar.   | <i>Example:</i> Diploma or certificate. |
| Work experience          |                                                    | <i>Example:</i> Five years of job experience including two years in the field of information security. | <i>Example:</i> Job reference.          |
| Practical experience     |                                                    |                                                                                                        |                                         |
| Further trainings        |                                                    |                                                                                                        |                                         |
| Accreditations           |                                                    |                                                                                                        |                                         |

### 5.1.3. Auditing requirements

In this chapter auditing requirements shall be listed. These shall be the evidence deemed sufficient by the approval authority to prove that all requirements as listed in paragraphs 7.2.2.1. to 7.2.2.5. are met by the manufacturer. (Including type approvals prior to 1 July 2024).

Requirements should include the prospective rational to decide if cyber security was adequately considered during the development phase of the vehicle type.

#### 5.1.3.1. Formal requirements

In case formal requirements are set by the approval authority these shall be listed here. Formal requirements include the requirement for certifications, permits and licences for example.

| Formal requirement                   | Version / edition, date |
|--------------------------------------|-------------------------|
| For example: ISO 27001 certification |                         |
|                                      |                         |
|                                      |                         |

#### 5.1.3.2. Required information

In this Chapter a structured list of the documentation which the auditing body requires from the audited entity should be provided. Any formal requirements on the documentation shall be stated here.

*Note: This could contain a list of topics that need to be addressed. A reference to documentation requirements from standard certifications like ISO/SAE 21434 is also possible.*

#### 5.1.3.3. Assessment of documentation

In this chapter details on the assessment rationale for the received documentation should be provided. There will be some general assessment criteria that apply to all documentation, e.g. that they are controlled, being used, are accessible, being reviewed, etc.

| No. | Title | Description | Remarks | Assessment rationale                                                                                                                                                                                                   |
|-----|-------|-------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   |       |             |         | Note: This should contain the different levels of rationales. The level of the integration of the procedures (to assure that procedures are relevant to each other) rationales related to requirements and rationales. |
| 2   |       |             |         |                                                                                                                                                                                                                        |

#### 5.1.3.4. Auditing Questionnaire

<Focus Area 1 (e.g. *threat analysis*)>

| Requirement | Audit question | Intent/purpose of question | Minimum performance criteria | Best practice | Additional information/context <sup>1</sup> |
|-------------|----------------|----------------------------|------------------------------|---------------|---------------------------------------------|
|             |                |                            |                              |               |                                             |
|             |                |                            |                              |               |                                             |
|             |                |                            |                              |               |                                             |

<Focus Area 2 (e.g. *risk management*)>

| Requirement | Audit question | Intent/purpose of question | Minimum performance criteria | Best practice | Additional information/context <sup>1</sup> |
|-------------|----------------|----------------------------|------------------------------|---------------|---------------------------------------------|
|             |                |                            |                              |               |                                             |
|             |                |                            |                              |               |                                             |
|             |                |                            |                              |               |                                             |

## 5.2. Description of type approval

### 5.2.1. Approval process

Contact data of the approval authority and its organisational unit responsible for the type approval process shall be provided.

The approval process should be documented in a process flow chart.

(Flow chart)

### 5.2.2. Qualification requirements and assessor team setup

Here the minimum requirements of the approval authority on technical services assessing the type approval requirements shall be laid down. The positions in a potential assessment team shall be listed. Qualifications shall be attributed to team position.

#### 5.2.2.1. Potential auditing team setup

| Position<br><i>Examples</i>     | Staffing requirement | Tasks/remarks                                                                                                                                                      |
|---------------------------------|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Lead assessor</i>            | <i>1</i>             | <i>Manage assessment process; accountable and responsible</i>                                                                                                      |
| <i>CS process expert</i>        | <i>1</i>             | <i>Responsible for transferring CSMS knowledge and understanding to the assessment of the vehicle type; ideally personal staffing overlap with CSMS audit team</i> |
| <i>CS Product expert</i>        | <i>2</i>             |                                                                                                                                                                    |
| <i>Penetration tester</i>       | <i>1-2</i>           |                                                                                                                                                                    |
| <i>...</i>                      |                      |                                                                                                                                                                    |
| <i>Documentation Management</i> |                      |                                                                                                                                                                    |

<sup>1</sup> If relevant, the circumstances in which the question can be asked or omitted or possible variations depending on the context etc.)

### 5.2.2.2. Qualification requirements

| Assessor qualification   | Concerned positions                           | Minimum requirement                                                                                                               | Evidence                                  |
|--------------------------|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| Educational achievements | <i>Example: lead assessor, product expert</i> | <i>Example: University degree in computer science, mathematics, physics, engineering or similar.</i>                              | <i>Example: Diploma or certificate.</i>   |
| Work experience          |                                               | <i>Example: Five years of job experience including two years in the field of information security.</i>                            | <i>Example: Job reference.</i>            |
| Practical experience     |                                               | <i>Example: Experience with automobile E/E architectures and experience with cybersecurity assessment and penetration testing</i> | <i>Example: Job or project reference.</i> |
| Further trainings        |                                               |                                                                                                                                   |                                           |
| Accreditations           |                                               |                                                                                                                                   |                                           |

### 5.2.3. Assessment requirements

In this chapter measures fit for assessing if the vehicle manufacturer has taken the necessary measures referred to in subparagraph 5.1.1.

#### 5.2.3.1. General assessment measures

These shall be the measures deemed sufficient by the approval authority to verify that:

- (a) the CSMS certificate is relevant for the vehicle type under approval.

#### *Risk Management*

- (b) the vehicle manufacturer has taken sufficient measures to identify and manage, for the vehicle type being approved, supplier-related risks, including the required standards for such risk management.

#### *Risk Identification*

- (c) the vehicle manufacturer has identified the critical elements of the vehicle type;
- (d) the definition of “critical elements”;
- (e) the vehicle manufacturer has performed an exhaustive risk assessment for the vehicle type, as required under subparagraph 7.3.3. of the Regulation.

#### *Risk Mitigation*

- (f) the vehicle type is protected against risks identified in the vehicle manufacturer’s risk assessment;
- (g) the mitigations applied by the manufacturer are proportionate, including the explanation of the interpretation of the term “proportionate”;
- (h) the reasons to support that the mitigations referred to in Annex 5, Part B or C are not relevant, not sufficient for the risk identified or not feasible;
- (i) “another mitigation” implemented by the manufacturer pursuant to subparagraph 7.3.4. is “appropriate”.

#### *Monitoring and response*

- (j) the principles was laid out in the respective CSMS to monitor threats and respond to possible incidents have been thoroughly applied to the vehicle type and are effectively in place;
- (k) effectiveness and efficiency of implemented mitigation measures has been tested and will be monitored.

The approval authority shall comprehensively lay down the evaluation standards used for the above verification.

### 2.3.2. Documentation requirements



Required documentation and expected main content of the documents shall be listed. The documentation shall be fit to assess the requirements as listed in 2.3.1.

### 2.3.3. Technical assessment

The technical assessment strategy shall be laid out. This shall include the tests and testing strategy envisaged/applied to verify that the vehicle manufacturer has implemented the cyber security measures as required by the regulation and documented by the manufacturer. The testing strategy shall consider tests executed by third parties. *E.g. tests executed by specialized technical services or service providers, manufacturer's subcontractors or research institutions, as either initiated by the manufacturer or approval authorities.*

The strategy used for replicating manufacturer tests shall also be included.

*Note: while the assessment measures in 2.3.1. are thought to include the assessment of past tests as documented by the manufacturer, the replication strategy shall lay down the rationale for choosing test which to replicate and how to replicate them.*

## 6. Link with ISO/SAE DIS 21434 (E)

The following table provides a summary of the link between the requirements of the Regulation and the relevant paragraphs of ISO/SAE DIS 21434.

| Paragraph                                                                                                                                                                                                                                                                                                            | Clauses from ISO/SAE DIS 21434                                                                                                                    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| 7.2.1. For the assessment the Approval Authority or its Technical Service shall verify that the vehicle manufacturer has a Cyber Security Management System in place and shall verify its compliance with this Regulation.                                                                                           |                                                                                                                                                   |
| Verify that a Cyber Security Management System is in place                                                                                                                                                                                                                                                           | <i>Not applicable</i>                                                                                                                             |
| 7.2.2.1. The vehicle manufacturer shall demonstrate to an Approval Authority or Technical Service that their Cyber Security Management System applies to the following phases: <ul style="list-style-type: none"> <li>- Development phase;</li> <li>- Production phase;</li> <li>- Post-production phase.</li> </ul> |                                                                                                                                                   |
| Development phase                                                                                                                                                                                                                                                                                                    | Clauses 9, 10, 11, 15                                                                                                                             |
| Production phase                                                                                                                                                                                                                                                                                                     | Clause 12                                                                                                                                         |
| Post-production phase                                                                                                                                                                                                                                                                                                | Clauses 7, 13, 14, 15                                                                                                                             |
| 7.2.2.2. (a) The processes used within the manufacturer's organization to manage cyber security                                                                                                                                                                                                                      |                                                                                                                                                   |
| Organization-wide cyber security policy                                                                                                                                                                                                                                                                              | [RQ-05-01], [RQ-05-03]                                                                                                                            |
| Management of cyber security relevant processes                                                                                                                                                                                                                                                                      | [RQ-05-02], [RQ-05-09]                                                                                                                            |
| (a3) Establishment and Maintenance of cyber security culture and awareness                                                                                                                                                                                                                                           | [RQ-05-07], [RQ-05-08]                                                                                                                            |
| 7.2.2.2. (b) The processes used for the identification of risks to vehicle types. Within these processes, the threats in Annex 5, Part A, and other relevant threats shall be considered.                                                                                                                            |                                                                                                                                                   |
| (b1) Process for identifying cyber security risks to vehicle types established across development, production, and post-production                                                                                                                                                                                   | [RQ-08-01], [RQ-08-02], [RQ-08-03], [RQ-08-08], [RQ-08-09].<br>The threats in Annex 5 of UN Regulation No. 155. are out of scope of ISO/SAE 21434 |
| 7.2.2.2. (c) The processes used for the assessment, categorization and treatment of the risks identified                                                                                                                                                                                                             |                                                                                                                                                   |

|                                                                                                                                                                                                                                                                                                                              |                                                |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| (c1) Is a process established to assess and categorize cyber security risks for vehicle types across development, production and post-production?                                                                                                                                                                            | [RQ-08-11], [RQ-08-04], [RQ-08-06], [RQ-08-10] |
| (c2) Is a process established to treat cyber security risks for vehicle types across development, production and post-production?                                                                                                                                                                                            | [RQ-08-12], [RQ-09-07], [RQ-05-06], [RQ-09-08] |
| 7.2.2.2. (d) The processes in place to verify that the risks identified are appropriately managed                                                                                                                                                                                                                            |                                                |
| (d1) Is a process established to verify appropriateness of risk management?                                                                                                                                                                                                                                                  | [RQ-09-09]                                     |
| (e) The processes used for testing the cyber security of a vehicle type                                                                                                                                                                                                                                                      |                                                |
| (e1) Is a process established to specify cyber security requirements?                                                                                                                                                                                                                                                        | [RQ-09-10], [RQ-10-01]                         |
| (e2) Is a process established to validate the cyber security requirements of the item during development phase?                                                                                                                                                                                                              | [RQ-11-01], [RQ-11-02]                         |
| (e3) Is a process established to validate the cyber security requirements of the item during production phase?                                                                                                                                                                                                               | [RQ-12-01]                                     |
| 7.2.2.2. (f) The processes used for ensuring that the risk assessment is kept current                                                                                                                                                                                                                                        |                                                |
| (f1) Is a process established to keep the cyber security risk assessment current?                                                                                                                                                                                                                                            | [RQ-11-03], [RQ-06-08], [RQ-07-05], [RQ-07-06] |
| 7.2.2.2. (g) The processes used to monitor for, detect and respond to cyber-attacks, cyber threats and vulnerabilities on vehicle types and the processes used to assess whether the cyber security measures implemented are still effective in the light of new cyber threats and vulnerabilities that have been identified |                                                |
| (g1) Is a process established to monitor for cyber security information?                                                                                                                                                                                                                                                     | [RQ-07-01]                                     |
| (g2) Is a process established to detect cyber security events?                                                                                                                                                                                                                                                               | [RQ-07-02]                                     |
| (g3) Is a process established to assess cyber security events and analyze cyber security vulnerabilities?                                                                                                                                                                                                                    | [RQ-07-03], [RQ-07-04]                         |
| (g4) Is a process established to manage identified cyber security vulnerabilities?                                                                                                                                                                                                                                           | [RQ-07-05], [RQ-15-04], [RQ-15-05], [RC-15-03] |
| (g5) Is a process established to respond on cyber security incidents?                                                                                                                                                                                                                                                        | [RQ-13-01], [RQ-13-02], [RQ-13-03]             |
| (g6) Is a process established to validate effectiveness of the response?                                                                                                                                                                                                                                                     | [RQ-11-01], [RQ11-03], [RQ-11-04]              |
| (h) The processes used to provide relevant data to support analysis of attempted or successful cyber-attacks.                                                                                                                                                                                                                |                                                |
| Is a process given to provide relevant data to support analysis?                                                                                                                                                                                                                                                             | [RQ-07-03]                                     |
| 7.2.2.3. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that, based on categorization referred to in point 7.2.2.2. (c) and 7.2.2.2. (g), cyber threats and                                                                                    |                                                |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| vulnerabilities which require a response from the vehicle manufacturer shall be mitigated within a reasonable timeframe.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                    |
| Mitigation within reasonable timeframe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | No timeframe defined by ISO/SAE DIS 21434 (E)                                                      |
| <p>7.2.2.4. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that the monitoring referred to in point 7.2.2.2. (g) shall be continual. This shall:</p> <ul style="list-style-type: none"> <li>(a) Include vehicles after first registration in the monitoring;</li> <li>(b) Include the capability to analyse and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs. This capability shall respect paragraph 1.3. and the privacy rights of car owners or drivers, particularly with respect to consent.</li> </ul> |                                                                                                    |
| Monitoring after first registration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Clause 7.3 “Cybersecurity Monitoring”                                                              |
| Capability to analyse and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Not explicitly mentioned in ISO/SAE DIS 21434 (E), but could be seen as Cybersecurity Information. |
| Respecting privacy rights of car owners or drivers, particularly with respect to consent                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Out of scope of ISO/SAE 21434, so not applicable                                                   |
| <p>7.2.2.5. The vehicle manufacturer shall be required to demonstrate how their Cyber Security Management System will manage dependencies that may exist with contracted suppliers, service providers or manufacturer’s sub-organizations in regards of the requirements of paragraph 7.2.2.2.</p>                                                                                                                                                                                                                                                                                                                                       |                                                                                                    |
| Dependencies that may exist with contracted suppliers                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | [RQ-06-09], [RQ-15-03], [RC-15-02]                                                                 |
| Dependencies that may exist with contracted service providers                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | [RQ-06-09], [RQ-15-03], [RC-15-02]                                                                 |
| Dependencies that may exist with manufacturer’s sub-organizations                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | [RQ-06-09], [RQ-15-03], [RC-15-02]                                                                 |



# **Normalización en ciberseguridad para la movilidad conectada y automatizada de vehículos y su entorno**

# Normalización en Ciberseguridad para la Movilidad Conectada y Automatizada de vehículos y su entorno



## Agradecimientos

---

Los organismos públicos, asociaciones y empresas privadas que forman parte del Grupo de estudio CTN 320/GT CAV "Ciberseguridad en Ámbito del Vehículo" y que han participado en la elaboración de este Informe son:

COITT - Colegio Oficial de Ingenieros Técnicos de Telecomunicación (promotor del grupo CTN 320/GT CAV)

UNE - Asociación Española de Normalización (coordinador del CTN 320/GT CAV)

Abertis Autopistas España S.A. Unipersonal

Aenor Internacional S.A.

Alter Technology Tuv Nord S.A.

AMETIC - Asociación de Empresas de Electrónica, Tecnologías de la Información, Telecomunicaciones y Contenidos Digitales

COIT - Colegio Oficial de Ingenieros de Telecomunicación

DEKRA Testing and Certification S.A.U.

ECIX Group S.L

Enigmedia S.L.

FORLOPD, Seguridad y Privacidad de Datos S.L.

Fundación Tecnalía Research & In

GMV, Soluciones Globales Internet S.A.U.

Grupo CFI - Construyendo Futuro Informático S.L.

jtsec Beyond IT Security S.L.

Knowledge Development for POF S.L.

LGAi Technological Center S.A.. Applus+ Laboratories, España

MAPFRE S.A.

Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC)

Renfe Operadora

Sistemas Informáticos Abiertos S.A. (SIA)

TELEFÓNICA S.A.

Universidad Carlos III de Madrid

Universidad de Navarra

Universidad Nacional de Educación a Distancia

Universidad Rey Juan Carlos

Vicomtech, Fundación centro de Tecnologías de Interacción Visual y Comunicaciones



# Índice

|     |                                                                                                                        |    |
|-----|------------------------------------------------------------------------------------------------------------------------|----|
| 1   | Objeto.....                                                                                                            | 4  |
| 2   | Antecedentes .....                                                                                                     | 4  |
| 3   | Ecosistema de Ciberseguridad en la Movilidad Conectada y Automatizada (CAM) .....                                      | 8  |
| 4   | Tecnologías de comunicación y conectividad para Vehículos Conectados y Automatizados (CAVs).....                       | 13 |
| 4.1 | Tecnologías de conectividad 5G hacia vehículos autónomos .....                                                         | 16 |
| 4.2 | Modelo híbrido .....                                                                                                   | 17 |
| 4.3 | Algunas conclusiones sobre la estandarización de los sistemas de conectividad .....                                    | 18 |
| 5   | Ciberseguridad y Privacidad en la movilidad inteligente .....                                                          | 19 |
| 5.1 | Ciberseguridad en el ámbito de Vehículos Conectados y Automatizados (CAVs) .....                                       | 20 |
| 5.2 | Ciberseguridad en el ámbito de Sistemas Inteligentes de Transporte (ITS) .....                                         | 22 |
| 6   | Ciberseguridad en las comunicaciones intra-vehiculares .....                                                           | 23 |
| 6.1 | Seguridad en CAN-BUS .....                                                                                             | 24 |
| 6.2 | Seguridad en Ethernet.....                                                                                             | 25 |
| 6.3 | Ejemplos de redes vehiculares.....                                                                                     | 26 |
| 7   | Regulaciones y certificaciones de Ciberseguridad en el ecosistema de la Movilidad Conectada y Automatizada (CAM) ..... | 27 |
| 7.1 | Seguridad del vehículo conectado y la operación de servicios y procesos en el ecosistema CAM .....                     | 28 |
| 7.2 | Primeras iniciativas en certificación del vehículo autónomo conectado.....                                             | 28 |
| 7.3 | Primeras iniciativas de certificación de los procesos de fabricación, desarrollo y operación del vehículo .....        | 30 |
| 7.4 | Primeras iniciativas de certificación de productos (componentes) del vehículo .....                                    | 30 |
| 7.5 | Normas y Certificaciones en los sistemas de comunicaciones del vehículo conectado .....                                | 33 |
| 7.6 | Esquemas de certificación de la criptografía en el vehículo conectado .....                                            | 41 |
| 7.7 | Regulaciones .....                                                                                                     | 41 |
| 8   | Futuros trabajos .....                                                                                                 | 44 |
|     | ANEXO I Referencias de algunas amenazas de ciberseguridad del vehículo .....                                           | 45 |
|     | ANEXO II Documentos de referencia en las tecnologías de comunicación y conectividad para vehículos conectados .....    | 46 |

# 1 Objeto

Este documento tiene por objeto identificar los órganos técnicos de normalización, estándares, proyectos e iniciativas más relevantes, relativos a la Ciberseguridad y Privacidad, en el ámbito general de la industria de la Movilidad Conectada y Automatizada (CAM)<sup>1</sup>, en particular de los Vehículos Conectados y Automatizados (CAVs)<sup>2</sup>, Sistemas Inteligentes de Transporte (ITS)<sup>3</sup> y las tecnologías de comunicación y conectividad involucradas.

## 2 Antecedentes

El reto social de la movilidad inteligente<sup>4</sup> es lograr un sistema de transporte que sea eficiente en cuanto a recursos, respetuoso con el clima y el medio ambiente, esto se consigue trabajando sobre las premisas de 0 accidentes, 0 contaminación y 0 emisiones siendo requisito esencial que funcione de manera segura y sin problemas en beneficio de todos los ciudadanos, la economía y la sociedad. La IoT es una tecnología clave que permite resolver este desafío.

Un vehículo moderno contiene más de 100 millones de líneas de código y puede tener entre 8 y 70 o más ECUs o computadoras de a bordo que generan más de 25 GB de datos a la hora destinados a gestionar diversos aspectos de la funcionalidad del automóvil, desde la velocidad del vehículo hasta la temperatura de su interior. Estos números ilustran la observación de que un vehículo no es un único dispositivo de IoT, sino que es más apropiado pensar en él como un mega dispositivo de IoT o, más formalmente, un sistema de sistemas de dispositivos de IoT o una plataforma móvil hiperconectada. Dentro de este sistema de sistemas, las restricciones son el empleo de un protocolo no orientado a la ciberseguridad como CAN BUS, el coste de componentes, la potencia de computación y las limitaciones de ancho de banda y consumo eléctrico; las restricciones físicas son usualmente menos críticas en el ambiente de un auto.

En la actualidad existen varias tendencias relativas a la digitalización del automóvil, lo que da lugar al vehículo conectado, cuando sus sistemas se comunican con sistemas fuera del ámbito del propio vehículo; al vehículo inteligente, que ofrece información acerca de la situación del vehículo y su entorno al conductor y otros ocupantes; e incluso al vehículo autónomo, en el que el vehículo es capaz de tomar decisiones automáticas y accionar actuadores que le permiten operar reduciendo la interacción con el piloto en una situación controlada.

Un automóvil conectado está invariablemente equipado con acceso a Internet, y por lo general también con una red de área local inalámbrica. Esto permite que el automóvil comparta el acceso a Internet con otros dispositivos tanto dentro como fuera del vehículo.

El despliegue satisfactorio y seguro de vehículos conectados en diferentes escenarios de uso, utilizando información e inteligencia local y distribuida, es una tarea difícil<sup>5</sup> que requiere el uso de plataformas de IoT fiables y en tiempo real que gestionen servicios críticos para la seguridad de los vehículos, sensores y accionadores avanzados, tecnología de navegación y toma de decisiones cognitivas, interconectividad entre vehículos (V2V) y comunicación entre vehículos e infraestructura (V2I). Los vehículos conectados permitirán el desarrollo de ecosistemas de servicios basados en la información recogida (por ejemplo, mantenimiento, seguros personalizados e incluso entretenimiento personalizado en el vehículo).

---

1 Más comúnmente conocida por sus siglas en inglés CAM, *Connected and Automated Mobility*.

2 Más comúnmente conocida por sus siglas en inglés CAVs, *Connected and Automated Vehicles*.

3 Más comúnmente conocida por sus siglas en inglés ITS, *Intelligent Transportation Systems*.

4 <https://ec.europa.eu/programmes/horizon2020/en/h2020-section/smart-green-and-integrated-transport>

5 Report: AIOTI WG 9 – Smart Mobility, 2015





Como con todos los dispositivos de IoT, la funcionalidad adicional que ofrece un vehículo conectado conlleva riesgos y consecuencias potencialmente fatales dado que ejecuta una función crítica que puede causar daños físicos y personales. Los investigadores ya han demostrado que los vehículos modernos e informatizados pueden ser secuestrados con sólo un ordenador portátil, un hardware de bajo coste y un software fácil de obtener. Los piratas informáticos han demostrado que pueden mostrar lecturas falsas en el salpicadero, controlar a distancia la dirección si esta es electrónica y desactivar los frenos, y apagar el motor a distancia cuando el vehículo está en movimiento<sup>6</sup>.

ENISA<sup>7</sup> identifica buenas prácticas para garantizar la seguridad de los vehículos inteligentes contra las ciberamenazas, clasificando estas prácticas en medidas políticas, organizativas y técnicas. Las medidas políticas incluyen la adhesión a la reglamentación y el establecimiento de responsabilidades; las medidas organizativas incluyen la designación de un equipo de seguridad dedicado dentro de los actores organizativos de la industria automovilística conectada, el desarrollo de un Sistema de Gestión de la Seguridad de la Información (SGSI) dedicado y adaptado a las necesidades de la industria, y la introducción de controles de seguridad y privacidad en la fase de diseño; y las medidas técnicas incluyen comunicaciones cifradas de extremo a extremo, normas de vanguardia para la criptografía y la generación de números aleatorios, Módulos de Seguridad de Hardware (HSM) dedicados y auditados independientemente, y prácticas de gestión de claves seguras; también se incluyen las actualizaciones y parcheos de software y firmware, entre otras. ENISA recomienda también que se mejore el intercambio de información entre las partes interesadas de la industria, así como que se aclare la responsabilidad de los agentes de la industria.

Además de los peligros para la seguridad y la protección, los conductores y los pasajeros se enfrentan a amenazas a la privacidad. Los datos privados de los teléfonos inteligentes, como el correo electrónico, los mensajes de texto, los contactos y otros datos personales, podrían ser robados por los piratas informáticos a través del vehículo si dichos datos pasan por sus sistemas de información. La información sobre la ubicación de los vehículos puede utilizarse para determinar cuándo están ausentes los ocupantes de una casa, lo que da a los ladrones una oportunidad.

Se han puesto en marcha varias iniciativas para abordar los problemas de seguridad inherentes a los vehículos conectados. La Alianza para la Innovación en IoT de la Comisión Europea (AIOTI) tiene un grupo de trabajo dedicado a la movilidad inteligente, que incluye casos de uso de IoT relacionados con la industria del automóvil. La iniciativa eCall<sup>8</sup>, tiene por objeto prestar asistencia rápida a los automovilistas en caso de accidente comunicando la ubicación y la dirección del vehículo a los servicios de emergencia; el sistema eCall es obligatorio para todos los automóviles nuevos vendidos en la UE desde abril de 2018. Los grupos de Sistemas Inteligentes de Transporte (ITS) de todo el mundo, en particular ERTICO<sup>9</sup> en Europa, participan en varios proyectos piloto en el área de la movilidad inteligente. ERTICO también ha publicado recomendaciones<sup>10</sup> sobre tecnologías de comunicación para futuros escenarios de ITS cooperativos (C-ITS). El Foro Americano sobre el Futuro de la Privacidad<sup>11</sup> y la Asociación Nacional de Concesionarios de Automóviles (NADA) han publicado una guía para el consumidor<sup>12</sup> en la que se destacan los tipos de datos que recogen y transmiten los automóviles conectados.

---

6 <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>

7 Cyber Security and Resilience of Smart Cars, ENISA, Dec 2016  
<https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars>

8 <https://ec.europa.eu/digital-single-market/en/news/ecall-all-new-cars-april-2018>

9 <http://ertico.com/>

10 <http://erticonetwork.com/ertico-releases-guide-about-technologies-for-future-c-its-service-scenarios/>

11 <https://fpf.org/>

12 <https://fpf.org/2017/01/25/fpf-and-nada-launch-guide-to-consumer-privacy-in-the-connected-car/>

El Sistema de Administración de Credenciales de Seguridad (SCMS) del Departamento de Transporte de los Estados Unidos es una solución de seguridad de mensajes de prueba de concepto (POC)<sup>13</sup> para la comunicación de vehículo a vehículo (V2V) y de vehículo a infraestructura (V2I). Utiliza un enfoque basado en la infraestructura de clave pública (PKI) que emplea la encriptación y la gestión de certificados para facilitar una comunicación fiable. Los participantes autorizados del sistema utilizan certificados digitales emitidos por el SCMS para autenticar y validar los mensajes de seguridad y movilidad que constituyen la base de los vehículos conectados. Para proteger la privacidad de los propietarios de los vehículos, estos certificados no contienen ninguna información personal o de identificación del equipo, sino que sirven como credenciales del sistema, de modo que los demás usuarios del sistema pueden confiar en la fuente de cada mensaje. El SCMS también protege el contenido de cada mensaje identificando y eliminando los dispositivos con comportamiento erróneo, manteniendo al mismo tiempo la privacidad.

## Datos y Vehículos conectados



*Figura 1: Vehículo conectado con diferentes funciones  
(Fuente: Foro sobre el Futuro de la Privacidad, modificado)*

<sup>13</sup> <https://www.its.dot.gov/resources/scms.htm>



Figura 2: Enfoque de Diseño, Construcción y Conducción de IBM<sup>14</sup>  
(Fuente: IBM)

## Riesgos de ciberseguridad

A continuación, se señalan algunos de los principales riesgos identificados y que han servido para poner de manifiesto la necesidad urgente de estandarizar y armonizar normativas y regulaciones de seguridad que permitan gestionar los riesgos de seguridad y privacidad una forma eficiente, consensuada, transparente y confiable.

## Riesgos de ciberseguridad en sistemas de telecomunicaciones de vehículos

El uso de cada vez más vehículos de sistemas de comunicación remota mediante unidades de control telemático (TCUs), o soluciones de gestión de flota, implica que cada vez más vehículos podrían sufrir ataques de forma remota, al estar conectados estos elementos por comunicaciones móviles de propósito general (3G/4G, o alternativas como NB-IoT...), redes específicas de IoT (SigFox, LoRa...) o conectados a teléfonos móviles vía WiFi o Bluetooth.

Dado que dichas unidades de control se encuentran conectados en las redes internas de los vehículos, se podrían producir ataques por dichos elementos, como puedan ser denegaciones de servicio (tipo *ransomware*), robos de vehículos de la flota, o incluso ataques terroristas, mediante por ejemplo la activación de los pirotécnicos del vehículo (airbags).

La falta de regulación, normativa y certificación de esta clase de elementos pone en riesgo a los usuarios de las flotas de alquiler, a los profesionales que operan los vehículos monitorizados, y a todos los usuarios de la vía pública.

14 Informe ejecutivo de IBM "Driving security: Cyber assurance for next-generation vehicles".

Entre las iniciativas de la industria, IBM aboga por su filosofía "Design, Build, Drive" (Diseñar, Construir, Conducir) que tiene como objetivo asegurar cada fase del ciclo de vida del automóvil conectado. En particular, IBM reconoce la necesidad de diseñar una infraestructura segura además de un vehículo seguro, dado que los ataques basados en la infraestructura, como las condiciones de tráfico falsificadas, podrían causar estragos al provocar desvíos y frenazos inesperados. El enfoque también hace hincapié en la necesidad de una cadena de suministro y un ecosistema de mantenimiento fiables.

## Riesgos de ciberseguridad en sistemas de comunicaciones de vehículos autónomos

La introducción de interfaces de telecomunicaciones inalámbricas en los vehículos (independientemente del sistema tecnológico subyacente) supone la introducción de un vector de ataque importante en los vehículos, cuyos riesgos deberán ser manejados y contrarrestados de forma efectiva para la implementación segura de los sistemas V2X (*vehicle-to-everything*, “vehículo a todo”).

Dado que un ataque contra esta clase de elementos supondría una posible pérdida de vida, es imperativo que se preparen los sistemas de forma que estos sean resilientes, teniendo en consideración los requisitos de ciberseguridad desde las primeras fases de desarrollo. Para ello, los organismos de estandarización técnica deberán de regular unos requisitos mínimos de seguridad de acuerdo con el estado del arte de la protección de sistemas.

En cualquier caso, la seguridad en el desarrollo de los sistemas es necesario que se soporte en estándares que cubran todo el ciclo completo de vida de los productos, y que son comúnmente conocidos como SDLC (*Systems Development Life Cycle*).

Los requisitos regulatorios definidos en el comité UNECE para implantar un sistema de gestión de la seguridad en los procesos de desarrollo y fabricación de los vehículos, es un primer paso en esta línea y es esperable que en el futuro veamos mayores avances y armonización de requisitos en este sentido.

Finalmente, es importante no olvidarse que los requisitos no han de ser usados como una barrera artificial de entrada al mercado, ni como una excusa para eliminar los derechos de los consumidores de poder llevar a cabo reparaciones en sus sistemas, por lo que se tiene que garantizar la interoperabilidad de los sistemas, así como la homologación y regularización de componentes de “*aftermarket*” para soluciones avanzadas personales y profesionales.

## 3 Ecosistema de Ciberseguridad en la Movilidad Conectada y Automatizada (CAM)

La industria de la Movilidad Conectada y Automatizada (CAM) se basa en un amplio ecosistema de actores que cubren las diferentes áreas de la cadena de valor desde I + D y fabricación, venta minorista y prestación de servicios, operaciones, mantenimiento y gestión de infraestructuras y flotas, así como todo el marco de los organismos reguladores y de normalización del sector.

Y por ello es fácil ver que la seguridad del vehículo conectado, no depende únicamente del propio vehículo, sino que los riesgos y amenazas para el mismo se extienden a lo largo de todo el ecosistema CAM.

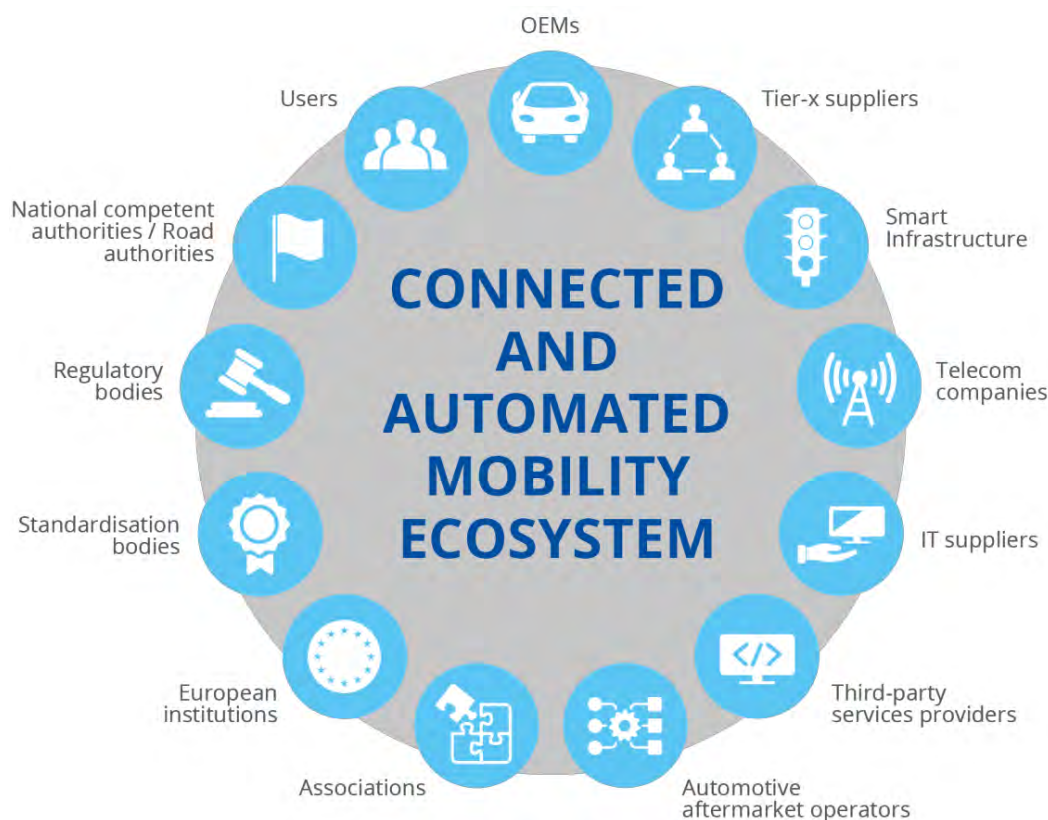
ENISA en un reciente estudio, publicado en noviembre 2020 titulado: *Inventario de ciberseguridad en el Ecosistema CAM*<sup>15</sup>, analiza en detalle la composición de este ecosistema y las implicaciones para la ciberseguridad de cada una de las partes que los conforman.

---

15 <https://www.enisa.europa.eu/publications/cybersecurity-stocktaking-in-the-cam>



A continuación, se resumen los principales actores y partes interesadas de este ecosistema CAM según han sido consideradas en dicho estudio.



Fuente: ENISA report Cybersecurity stocktaking in the CAM

## Fabricantes de equipos originales (OEM)

En el sector automotriz, el término OEM se refiere a cualquier empresa que fabrica piezas para su uso en vehículos, incluido hardware y software (también conocidos como proveedores de nivel 1 y nivel 2) y quién se encarga del montaje final del vehículo (OEM propiamente dicho).

## Proveedores de nivel 1 y nivel 2

Un proveedor de nivel 1 se centra en proporcionar sistemas y piezas a los OEM que son sus clientes directos, y un proveedor de nivel 2 en subcomponentes de los sistemas y piezas proporcionados por el proveedor de nivel 1 sin una relación directa con los OEM.

## Operadores de Infraestructuras Inteligentes

En el ecosistema CAM, las partes interesadas dentro de la categoría de infraestructura inteligente son multifacéticas. Las infraestructuras inteligentes comprenden varios operadores de diferentes dominios de actividad, como energía, transporte público, gestión de carreteras, seguridad pública.



En el contexto particular de la CAM, los Sistemas Inteligentes de Transporte (ITS) se definen como “Sistemas que sin incorporar la inteligencia como tal tienen como objetivo brindar servicios innovadores relacionados con diferentes modos de transporte y gestión del tráfico y permitir que varios usuarios estén mejor informados y hacer un uso más seguro, coordinado y 'más inteligente' de las redes de transporte” y de los operadores de Smart City que son “ciudades que utilizan soluciones tecnológicas para mejorar la gestión y eficiencia del entorno urbano”.

Dentro de la infraestructura inteligente, los vehículos conectados y automatizados interactúan con todo el ecosistema (V2X), lo que en parte es posible gracias a la interacción con la infraestructura vial inteligente y urbana que se basa en Internet de las Cosas, aprendizaje automático, *big data* y movilidad bajo demanda (V2I, I2V, V2N e I2N).

La interacción de un vehículo con su entorno y entre las infraestructuras que constituyen el entorno es crucial para el correcto despliegue de CAM.

## Empresas de telecomunicaciones

Las empresas de telecomunicaciones son parte muy importante dentro del ecosistema CAM, ya que garantizan la conectividad y la transferencia de datos desde y hacia los vehículos y la infraestructura inteligente (V2N e I2N).

Una evolución muy importante para el futuro cercano de la CAM es la aparición de las redes de comunicación 5G V2X, que son mucho más sofisticadas y ofrecen un mayor ancho de banda para mejorar la conectividad en comparación con las redes 3G / 4G actuales.

El Plan de Acción 5G<sup>16</sup> de la Comisión Europea de 2016, se propuso garantizar que para 2025, “todas las áreas urbanas y las principales rutas de transporte terrestre tengan una cobertura 5G ininterrumpida”.

El Plan de Acción también pide disminuir la fragmentación entre los Estados miembros para garantizar la continuidad del servicio (es decir, infraestructura 5G alineada y coordinada), que es crucial para los vehículos conectados, especialmente en la UE, donde la movilidad transfronteriza es un fenómeno cotidiano.

## Proveedores de IT y Servicios Cloud

Los proveedores de IT proporcionan software, hardware y funcionalidades en la nube seguros. Al igual que las empresas de telecomunicaciones, la conectividad confiable (estable) es una necesidad absoluta para CAM.

Los proveedores de IT también cubren la provisión de tecnologías emergentes como plataformas de IT en la nube (Amazon AWS, Microsoft Azure, Google Cloud, etc.), plataformas de software para conectividad y movilidad automotriz (por ejemplo, Waymo, Yandex, etc.), IA (Inteligencia Artificial) e IoT (Internet de las Cosas).

---

16 5G for Europe Action Plan. (last updated 2019). European Commission.  
<https://ec.europa.eu/digital-single-market/en/5g-europe-action-plan>



## Proveedor de servicios de terceros

Los proveedores de servicios de terceros proporcionan, por ejemplo, contenido, mapas, datos de tráfico, reproductor de música, monitor meteorológico y aplicaciones móviles para vehículos.

Los proveedores de navegación por satélite también están incluidos en este grupo de partes interesadas, ya que es un elemento clave de los vehículos automatizados dentro del ecosistema CAM.

## Operadores del mercado de repuestos y accesorios del automóvil

Los operadores del mercado de repuestos para automóviles son proveedores de servicios independientes. También son productores independientes de repuestos, distribuidores de repuestos, reparadores independientes, editores de información técnica, fabricantes de equipos de herramientas, reparadores de carreteras, compañías de leasing y compañías de seguros, según se define en el Reglamento (UE) 2018/858<sup>17</sup>.

## Asociaciones y consorcios industriales

En el ecosistema CAM las asociaciones y consorcios industriales tienen un papel clave como agrupadores y transmisores de los intereses de la industria. En particular en el ecosistema CAM son especialmente relevante las asociaciones y consorcios industriales representando a los grupos de: fabricación de piezas, *testing* y evaluación de seguridad de los componentes C-ITS, inspección técnica de vehículos, evaluación de carreteras, soluciones de software de conducción automatizada, representación de mayoristas y minoristas, lobbies industriales, etc.

Las asociaciones son, por tanto, un componente clave del ecosistema CAM, ya que sus competencias y, en ocasiones, sus esfuerzos de lobby a menudo resultan en cambios importantes en el mundo del transporte, a nivel nacional, europeo e internacional.

## Instituciones europeas

Las instituciones europeas que actúan en el ecosistema CAM son principalmente la Comisión Europea y las Agencias. La Comisión Europea tiene como objetivo adoptar políticas y legislaciones de varios niveles para liderar la transformación del ecosistema. ENISA, la agencia europea de ciberseguridad, es especialmente relevante en el ecosistema CAM para ayudar a mejorar la cooperación entre los estados miembros, en materia de ciberseguridad del vehículo autónomo y los C-ITS.

Un aspecto especialmente importante en Europa es la colaboración entre los Estados miembros, que la Comisión coordina en su Estrategia sobre sistemas de transporte inteligentes cooperativos (C-ITS)<sup>18</sup>.

---

17 *Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles.* <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32018R0858>

18 Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre una estrategia europea sobre sistemas de transporte inteligentes cooperativos, un hito hacia la movilidad cooperativa, conectada y automatizada. 30 de noviembre de 2016. Obtenido de: [https://ec.europa.eu/transport/sites/transport/files/com20160766\\_en.pdf](https://ec.europa.eu/transport/sites/transport/files/com20160766_en.pdf)

El Centro Común de Investigación<sup>19</sup> de la Comisión Europea ha definido la Infraestructura de clave pública<sup>20</sup> de seguridad en toda la UE como la característica más relevante de C-ITS y V2X y ha establecido estos sistemas como una infraestructura crítica en la UE.

## Organismos de normalización y estandarización

Los organismos de estandarización, dentro del ecosistema CAM, están a cargo de garantizar la seguridad e interoperabilidad a largo plazo de la industria.

Las normas técnicas y estándares internacionales cumplen diferentes objetivos, que incluyen por un lado estructurar y unificar los conceptos, unidades y sistemas de medidas que se utilicen en el ecosistema CAM, y por otro definir de forma transparente y abierta requisitos de ciberseguridad estandarizados para los diferentes elementos y componentes de la CAM. Por su parte, las normas de sistemas de gestión tienen por objetivo definir los procedimientos de calidad y seguridad necesarios para homogeneizar los procesos de diseño, desarrollo, operación y mantenimiento de productos, servicios y procesos.

Las normas técnicas ofrecen un terreno común para el desarrollo tecnológico, especialmente si se impulsan como un requisito legislativo.

## Organismos reguladores

Los organismos reguladores proponen regulaciones y condiciones marco para abordar los cambios necesarios provocados por CAM, que incluyen, por ejemplo, cuestiones éticas y de responsabilidad y privacidad, ciberseguridad y seguridad.

Como ejemplo, podemos mencionar como la Comisión Económica de las Naciones Unidas para Europa (CEPE) adoptó el reglamento de ciberseguridad WP29 en junio de 2020, que exige a todos los fabricantes de automóviles que adopten unas medidas mínimas de ciberseguridad para la homologación de los vehículos conectados.

A nivel europeo, la Comisión Europea es la encargada de transponer los textos definidos por UNECE, que tienen en cuenta las necesidades de todos los actores de la CAM.

Dado que el ritmo del desarrollo tecnológico es más rápido que el proceso legislativo que lo acompaña, los organismos reguladores son los encargados de crear una estructura dinámica de gobernanza para desarrollar una legislación técnica eficiente.

A nivel nacional, cada estado puede desarrollar regulaciones específicas para el ecosistema CAM.

---

19 Centro Común de Investigación, más conocido por JRC (en inglés *Joint Research Centre*).

20 Infraestructura de Clave Pública, más conocido por PKI (en inglés *Public Key Infrastructure*).





## Autoridades nacionales competentes / autoridades viales

En todos los niveles nacionales, el apoyo político es necesario para impulsar el desarrollo del ecosistema de la CAM. En los estados miembros de la UE, los gobiernos tienen diferentes instancias sobre el desarrollo, la prueba y el despliegue de CAM, en los que las autoridades nacionales competentes / autoridades viales desempeñan un papel muy importante.

El papel de estos organismos puede abarcar desde proporcionar experiencia en materia de seguridad, hasta tener una visión general de los objetivos a largo plazo de una ciudad específica, o incluso agencias independientes que cooperan con los sectores público y privado en asuntos relacionados con el transporte y las comunicaciones.

## Usuarios

Los usuarios se definen como conductores y pasajeros, así como peatones. La puesta en marcha de la CAM muestra cómo la digitalización afecta cada vez a más ámbitos de la sociedad.

# 4 Tecnologías de comunicación y conectividad para Vehículos Conectados y Automatizados (CAVs)

Los avances en tecnologías de comunicaciones clave han llevado a grandes mejoras y expectativas en el mercado automotriz, particularmente en los campos de automatización, Vehículos Conectados y Automatizados (CAVs), y Sistemas Inteligentes de Transporte (ITS).

Grupos de trabajo de la industria como "SAE International" (previamente conocido como Sociedad de Ingenieros de Automoción) y 3GPP (*3rd Generation Partnership Project*) han definido un sistema de clasificación de seis niveles para identificar las diferentes etapas de automatización hacia una conducción totalmente autónoma.

La siguiente imagen muestra los niveles de conducción autónoma, desde el nivel 0: Sin automatización hasta el nivel 5: Automatización completa).

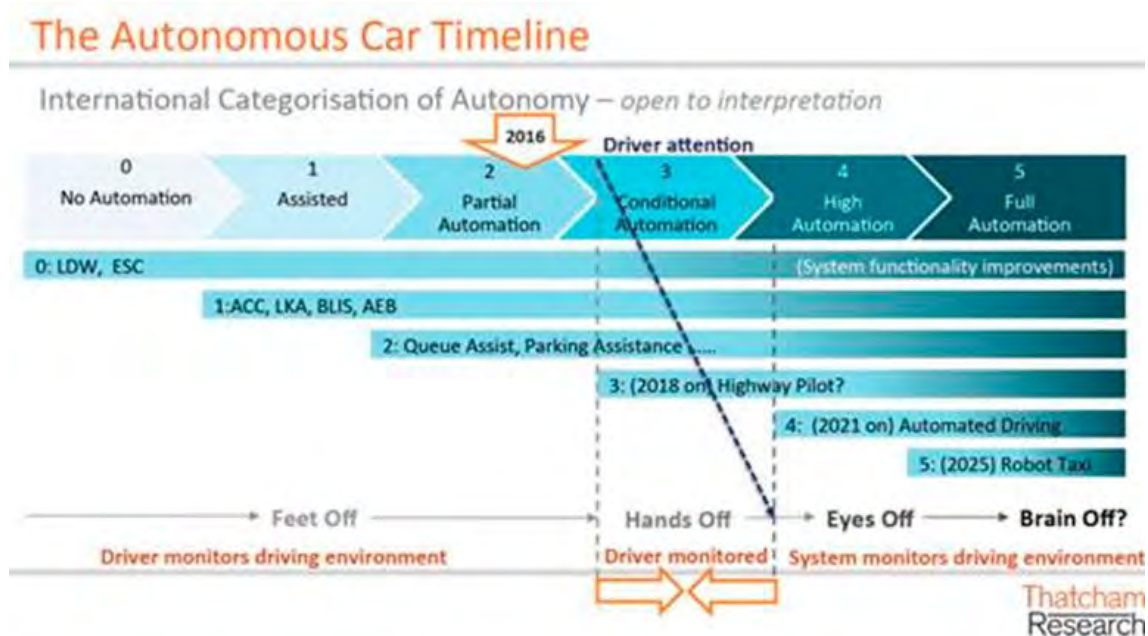


Imagen correspondiente a la: Charla coloquio: "Cómo afectará la conducción autónoma a los conductores"

La conectividad de los vehículos, junto con las funciones GNSS (navegación por satélite) y ADAS (sistemas avanzados de asistencia al conductor) son uno de los pilares tecnológicos clave para la transición hacia la conducción totalmente autónoma (Nivel 5).

Adicionalmente, cubrir las necesidades de comunicación intra-vehicular de alta velocidad y baja latencia de los datos recogidos por sensores perimetrales hacia los procesadores centrales es fundamental para escalar hacia niveles de conducción autónoma mayores.

El nivel 2 es el que más comúnmente nos encontramos en los fabricantes de diferentes marcas, mientras que el nivel 3 se encuentra siendo desarrollado por múltiples fabricantes, con diferentes grados de autonomía.

Cada avance en los diferentes niveles de conducción autónoma ha sido el resultado de muchos años de trabajo y dedicación por parte de las empresas desarrolladoras de tecnología de ayuda a la conducción. Los niveles 4 y 5 llegarán a nuestras carreteras y vidas, aunque para ello tengamos que esperar aún unos años.

La conectividad de un vehículo con el exterior se basa en la capacidad de telecomunicación (mayoritariamente vía radio) de sus componentes y su capacidad para comunicarse de manera inteligente con el resto de los elementos de la vía.



Existe una serie de términos para describir los escenarios de comunicación del vehículo. De forma genérica, las comunicaciones se engloban en la nomenclatura V2X (*vehicle-to-everything*, "vehículo a todo"). Dichas comunicaciones requieren la interoperabilidad y comunicaciones de diferentes elementos, para poder con ello establecer usos concretos, como pueden ser:

- Vehículo a vehículo (V2V, *vehicle-to-vehicle*) para evitar colisiones enviando datos de posición y velocidad entre sí, reaccionando más rápido que el conductor.
- Vehículo a infraestructura (V2I, *vehicle-to-infrastructure*) para gestionar la prioridad y el tiempo de las señales de tráfico, optimizando el tráfico.
- Vehículo a red (V2N, *vehicle-to-network*) para acceder a servicios como enrutamiento, tráfico en tiempo real, avisos "BLOS" (*beyond-line-of-sight*, más allá de la línea de visión, varios km).
- Vehículo a peatones (V2P, *vehicle-to-pedestrian*) para detección, notificación de alertas y prevención de accidentes.

La implementación de este tipo de aplicaciones está en desarrollo y es esperable que se encuentre comercialmente disponible a gran escala a partir de 2020.

Los proveedores de automoción Tier-1 están comprometidos con el desarrollo y las pruebas piloto de nuevas Unidades de Control Electrónico (ECU), capaces de proporcionar las funciones adecuadas a los nuevos vehículos de los fabricantes (OEMs), para lograr sistemas autónomos de nivel 3 y superior.

Al mismo tiempo, los desafíos relacionados con la validación y verificación de dichos componentes y funcionalidades están aumentando, por dos razones principales:

- La estandarización para la conformidad aún está en progreso y sujeta a varias iteraciones hasta que se pueda alcanzar la armonización.
- La tecnología está en continua evolución, causando cambios en los estándares de comunicación e interoperabilidad, también en los elementos software, y en las soluciones hardware, las cuales tardan años en desarrollarse.

En cuanto a la comunicación intra-vehicular, los requisitos de los OEMs sobre el ancho de banda y latencia no han hecho sino crecer de forma exponencial a la vez que los requisitos de conducción autónoma.

El número de sensores perimetrales, entre los cuales se encuentran cámaras de alta resolución, tanto en espectro visible como infrarrojo, radar, lidar, etc., aumenta en los nuevos diseños de vehículos para elaborar, junto con los datos recogidos por la comunicación V2X, un modelo preciso del entorno del vehículo para poder tomar decisiones autónomas.

La comunicación entre estas fuentes de datos (sensores, antenas, ECUs receptoras de comunicación V2X) y el centro de procesamiento y toma de decisiones requieren de una comunicación robusta, segura, de muy alta velocidad y baja latencia.

Afortunadamente, en los últimos años se han culminado esfuerzos en estandarización dentro de IEEE e ISO para definir tecnologías de comunicación para vehículos basados en Ethernet.

De este modo, el estándar ISO / IEC / IEEE 8802-3:2017 y la familia de estándares ISO 21111 definen sistemas de comunicación de hasta 1 Gb/s, conectores, cables y pruebas de conformidad concebidos para ser utilizados en el entorno hostil de un vehículo. Pruebas de resistencia en temperatura, torsión, humedad, ataque químico, inflamabilidad, tensiones, repeticiones de ciclos de conexión/desconexión, etc., han sido definidos para garantizar la robustez de las comunicaciones internas en el vehículo.

El hardware en este caso, ya está disponible e implementado en modelos de automóvil que actualmente ruedan en nuestras carreteras.

Sin embargo, los requisitos en cuanto a conectividad de los OEMs siguen creciendo, y ahora los esfuerzos de estandarización se centran en sistemas de comunicación intra-vehiculares con velocidades que llegan hasta los 50 y 100 Gb/s. De este modo, se encuentran en desarrollo los estándares IEEE 802.3cy e IEEE 802.3cz, para sistemas de comunicaciones Ethernet sobre varios cables de cobre apantallados, o sobre fibra óptica para dentro de vehículos de hasta 100 Gb/s.

A lo largo de 2021 se espera que comiencen los esfuerzos de estandarización, en IEC e ISO, para conectores, cables y conformidad para esta nueva ola de comunicaciones dentro del vehículo por encima del Gbabit por segundo.

## 4.1 Tecnologías de conectividad 5G hacia vehículos autónomos

Los vehículos autónomos requieren nuevas tecnologías de comunicación con capacidades más amplias en parámetros clave de telecomunicaciones:

- Latencia, suficientemente baja para permitir el intercambio de datos entre elementos en tiempos muy bajos, para poder disponer de suficiente tiempo para accionar sistemas físicos en el vehículo, como los frenos.
- Ancho de banda, suficientemente elevado para poder permitir tanto la interacción de un número elevado de elementos en el medio (no saturar las comunicaciones, como pudiera pasar en caso de aglomeraciones), como para permitir los intercambios rápidos de grandes cantidades de datos.

También se necesita una alta capacidad de cómputo en los componentes, para que estos puedan procesar la información recogida por los sensores locales, así como procesar las comunicaciones recibidas de los demás elementos.

En la actualidad existen dos propuestas tecnológicas en el mercado para las comunicaciones V2X, *Cellular V2X* y *Unlicensed V2X*. Ambas tecnologías compiten por ofrecer niveles suficientes de latencia y banda ancha para permitir hasta el nivel 3 y 4 de autonomía.

*Cellular V2X* (C-V2X) es una plataforma de tecnología promovida por 5GAA, 3GPP y operadores de red móvil globales, unificada que combina comunicaciones directas sin red utilizando el protocolo LTE (LTE-V2X) / 5G (NR-V2X) y espectro sin licencia de 5.9GHz (LTE/NR-V2X PC5) para comunicaciones de corto alcance (V2V, V2I, V2P), con comunicaciones de red celular (LTE/NR-V2X Uu) para comunicaciones de largo alcance (V2N).



C-V2X puede usar cualquier opción; la interfaz PC5 es más rápida y permite operación en zonas sin cobertura de estaciones base, mientras que la interfaz Uu proporciona un rendimiento más confiable porque el espectro con licencia se encuentra protegido legalmente contra interferencias.

El principal inconveniente es que las bandas licenciadas se encuentran controladas por operadores de telefonía a nivel nacional o regional y, por lo tanto, los fabricantes de automóviles deben alcanzar acuerdos con muchos operadores y propietarios con licencia para proporcionar un servicio mundial. Este problema causa demoras en el tiempo de comercialización en un entorno tecnológico que experimenta rápidos avances técnicos. El uso de tecnologías como eSIM deberían de simplificar el conexonado de los vehículos a los operadores, sin requerir el cambio de tarjetas SIM.

El uso de 5G para este tipo de comunicaciones podría presentar un papel importante en despliegues masivos de estas tecnologías, en la conectividad V2N, si bien para el uso de las nuevas bandas de milímetro (mmWave), las cuales otorgan a las redes 5G sus principales características distintivas frente a LTE de latencia y ancho de banda, por lo que requieren contacto visual con las antenas, algo problemático para vehículos en movimiento.

*Unlicensed (sin licencia) V2X (U-V2X)* también juega un papel importante porque no se requiere el uso de bandas licenciadas, sino que se hace uso de licencias de propósito específico libres. Las soluciones U-V2X tienen un tiempo de comercialización más corto y muchas de ellas ya están en la fase de prueba. Existen varios estándares de comunicación U-V2X, aunque algunos de ellos se han establecido a nivel regional.

*Direct Short Range Communication (DSRC)*, basado en el estándar IEEE 802.11p se dedica al intercambio de información entre vehículos e infraestructura vial y opera a 5.9 GHz. Es la interfaz de comunicación más desarrollada, con implementaciones globales.

En Europa, IEEE 802.11p es el estándar más utilizado para las comunicaciones U-V2X en la industria automotriz. Desde un punto de vista técnico, su principal inconveniente es la falta de un canal auxiliar de comunicaciones. En EE. UU., la tecnología homónima recibe el nombre de *Wireless Access in Vehicular Environment* (WAVE, Acceso Inalámbrico en Entornos de Vehículos).

## 4.2 Modelo híbrido

Aunque existen diferentes tecnologías disponibles para su uso (celular y sin licencia), los estudios<sup>21</sup> muestran que la coexistencia de ambas tecnologías 802.11p y C-V2X a 5.9 GHz, sujetas a la demanda del mercado ofrecería los mayores beneficios sociales en comparación con escenarios donde solo se exige una tecnología. La coexistencia de 802.11p y C-V2X a 5.9GHz híbrido es posible y será estudiada por el Comité Europeo CEPT/ETSI en respuesta al reciente mandato de EC RSCOM.

---

21 Referencias de estándares técnicos:

- [1] ECC Report 101, Compatibility Studies in the band 5855– 5925 MHz between Intelligent Transport Systems (ITS) and other systems
- [2] ECC Recommendation (08)01, Use of the band 5855-5875 MHz for Intelligent Transport Systems (ITS)

En la Unión Europea, las normas de Seguridad Vial para Sistemas Inteligentes de Transporte (ITS) son, en principio, independientes de la tecnología para evitar favorecer una tecnología de comunicación sobre otra. Además, las regulaciones garantizan que las tecnologías futuras deben ser compatibles con los sistemas actuales para garantizar que los avances técnicos nunca pongan en peligro la seguridad.

Sin embargo, un modelo híbrido implica desafíos de interoperabilidad, ya que los vehículos autónomos deberán estar listos para cambiar entre diferentes operadores de red o perfiles tecnológicos dependiendo de factores ambientales (túneles, condiciones de baja cobertura) y permitir la movilidad entre diferentes regiones y países, particularmente en la Unión Europea. La interoperabilidad es uno de los problemas que ahora se abordan mediante la estandarización y la homogeneización de los requisitos técnicos.

## 4.3 Algunas conclusiones sobre la estandarización de los sistemas de conectividad

Las tecnologías de conectividad actuales, C-V2X y U-V2X, ya están dando los primeros pasos hacia los vehículos de conducción autónoma y autoconducción, pero ambas tecnologías tienen ventajas y desventajas. Los estudios muestran que un modelo híbrido podría ser beneficioso tanto para la industria como para los consumidores, y también se ajusta a la filosofía de agnosticismo tecnológico de los organismos reguladores. Las tecnologías futuras también deben ser compatibles con versiones anteriores.

Los vehículos autónomos transmitirán decisiones críticas de conducción de humanos a máquinas, y el comportamiento de estas máquinas debe ser homogéneo para todos los fabricantes de vehículos y otros dispositivos que puedan interactuar con los vehículos (V2X). Esto significa una estandarización completa para toda la industria y para todos los países. Incluso si la tecnología aún no está en el nivel 5, la estandarización debe estar lista antes de que se desarrolle la tecnología. Los comités mundiales de la industria se encuentran desarrollando dichas normativas. El rendimiento 5G y las capacidades de banda ancha serán clave para desbloquear todo el potencial de la conducción autónoma. Sin embargo, los sistemas de comunicación 5G plantean nuevos desafíos en el desarrollo de productos y específicamente en las pruebas / *testing*. Los métodos de prueba anteriores ya no son válidos para probar componentes y vehículos totalmente automatizados.

En cuanto a redes intra-vehiculares, el estado de la implementación tecnológica y de la estandarización se encuentra más avanzada.

Existen sistemas de comunicación Ethernet de hasta 1 Gb/s implementados en vehículos que permiten conexiones de hasta 15 metros de longitud con 4 conectores intermedios o 40 metros sin conectores intermedios, que cumplen normas de conformidad concebidas para los casos de uso definidos por los OEMs.

Sin embargo, el aumento en la resolución y tiempo de refresco de los sensores perimetrales instalados en futuros vehículos con niveles de conducción autónoma mayores (cámaras, radar, lidar, etc.), requiere de mayor velocidad de transmisión, y por tanto se están llevando a cabo esfuerzos de estandarización para sistemas de hasta 100 Gb/s basados en Ethernet.



## 5 Ciberseguridad y Privacidad en la movilidad inteligente

Hoy en día los vehículos cada vez están más "conectados" V2X, prácticamente en cualquier vehículo existe un intercambio inalámbrico de datos con servidores, infraestructura (V2I), otros vehículos (V2V) y peatones (V2P).



- V2V entre vehículos para prevenir colisiones o interactuar con los mismos.
- V2P entre vehículos y personas para evitar atropellos por ejemplo.
- V2I entre vehículos y las redes viarias o infraestructuras.
- V2C vehículos con la nube para enrutar el tráfico.
- V2H vehículo y hogar para implementar por ejemplo que se abra la puerta de casa.

Pensando en los vehículos del mañana, éstos serán automatizados y autónomos, capaces de detectar su entorno y navegar sin intervención humana. Estos avances aumentarán la comodidad y la experiencia de los usuarios, mejorarán los productos y servicios y contribuirán a mejorar la seguridad vial, reducir el consumo de combustible y facilitar la gestión del tráfico y el estacionamiento.

Para lograr todo esto, el mundo digital es una pieza clave, puesto que ofrece oportunidades sin precedentes. Sin embargo, esta digitalización conlleva riesgos, como por ejemplo la amenaza de ciberataques a vehículos o a flotas de vehículos.



Por este motivo, la ciberseguridad se ha convertido en uno de los aspectos más críticos en el desarrollo de Vehículos Conectados y Automatizados (CAVs), incluidas todas las comunicaciones de vehículo V2X (V2I, V2V, V2P...) y mantener los riesgos de ciberseguridad para los vehículos conectados bajo control es de crucial importancia. Las interfaces de los vehículos conectados presentan una oportunidad para explotar vulnerabilidades si no se implementan mecanismos adecuados de ciberseguridad o si los riesgos de ciberseguridad no se abordan adecuadamente. Los atacantes pueden comprometer los datos personales del usuario, amenazar los sistemas del vehículo, poner en peligro a los pasajeros o a otros ocupantes de la vía.

Por eso es muy importante cultivar una cultura de ciberseguridad y adoptar un ciclo de vida de ciberseguridad para el desarrollo de vehículos con el objetivo de mejorar la protección de los vehículos contra los ciberataques.

A este respecto, actualmente a nivel internacional se están desarrollando distintas iniciativas de normalización sobre la ciberseguridad en vehículos.

Una de las más destacables es la iniciativa del ISO/IEC JTC 1/SC 27 sobre **"Criterios de evaluación de la seguridad de la información de los vehículos conectados basados en la norma ISO/IEC 15408"**. En esta iniciativa, se estudian los criterios y la metodología de evaluación de las tecnologías de los vehículos y los dispositivos conectados a la red. Se analizan sus amenazas y el objetivo de seguridad, así como la relación entre las características del vehículo conectado y la seguridad de la información, y los requisitos de seguridad basados en dichas características.

### Grupo de estudio CTN 320/GT CAV "Ciberseguridad en Ámbito del Vehículo"

A medida que los vehículos se vuelven más inteligentes y aumenta su conectividad e integración con los sistemas externos, también aumenta la necesidad de ciberseguridad relacionada con los vehículos y sus sistemas. Por lo tanto en UNE se ha creado el grupo de estudio CTN 320/GT CAV **"Ciberseguridad en Ámbito del Vehículo"** para realizar el análisis del panorama de las normas, guías y buenas prácticas relativas a la Ciberseguridad en el Ámbito de Vehículos, incluyendo la ciberseguridad y privacidad para Vehículos Conectados y Automatizados (CAVs), Sistemas Inteligentes de Transporte (ITS), y aplicaciones/ dispositivos conectados en la movilidad.

## 5.1 Ciberseguridad en el ámbito de Vehículos Conectados y Automatizados (CAVs)

Se destacan las siguientes normas, guías y buenas prácticas relativas a Ciberseguridad para Vehículos Conectados y Automatizados (CAVs).

### Comité nacional UNE:

CTN 320 Ciberseguridad y proyección de datos personales

CTN 26/SC 1/GT 1 Vehículos de carretera/Equipos Eléctricos y Electrónicos/Ciberseguridad





## Comités internacionales relacionados:

ISO/IEC JTC1/SC 27 *Information security, cybersecurity and privacy protection*

ISO/TC 22/SC 32/WG 1 *Electrical and electronic components and general system aspects – Cybersecurity*

## Normas:

|                            |                                                                                                                                                                     |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UNE 320001: 2021           | Metodología de evaluación LINCE para la seguridad de productos TIC                                                                                                  |
| Serie UNE-EN ISO/IEC 15408 | Tecnología de la información. Técnicas de seguridad. Criterios de evaluación para la seguridad de TI                                                                |
| ISO/IEC 9797-1:2011        | Information technology. Security techniques. Message Authentication Codes (MACs). Part 1: Mechanisms using a block cipher                                           |
| ISO/IEC 27001:2013         | Information technology. Security techniques. Information security management systems ISMS. Requirements                                                             |
| ISO/IEC 27002:2013         | Information technology. Security techniques. Code of practice for information security controls                                                                     |
| ISO/IEC 27017:2015         | Information technology. Security techniques. Code of practice for information security controls based on ISO/IEC 27002 for cloud services                           |
| ISO/IEC 27018:2019         | Information technology. Security techniques. Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors |
| ISO/IEC 27032:2012         | Information technology. Security techniques. Guidelines for cybersecurity                                                                                           |
| Serie ISO/IEC 27034        | Information technology. Security techniques. Application security                                                                                                   |
| Serie ISO/IEC 27035        | Information technology. Information security incident management                                                                                                    |
| ISO/IEC 29101:2018         | Information technology. Security techniques. Privacy architecture framework                                                                                         |
| Serie ISO/IEC 29119        | Software and systems engineering. Software testing                                                                                                                  |

## Proyectos:

|                      |                                                                                                                                                     |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| ISO/IEC (SP)         | Information Security Technology-Evaluation criteria for connected vehicle information security based on ISO/IEC 15408 (ISO/IEC JTC 1/SC 27/WG 3)    |
| ISO/IEC (NP)         | Security Technical Specification for Intelligent and Connected Vehicles On-Board Terminal (ISO/IEC JTC 1/SC 27/WG 3)                                |
| ISO/IEC DIS 15408-1  | Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 1: Vocabulary, introduction and general model |
| ISO/IEC FDIS 15408-2 | Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 2: Security functional components             |
| ISO/IEC DIS 15408-3  | Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 3: Security assurance components              |

|                      |                                                                                                                                                                               |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ISO/IEC FDIS 15408-4 | Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 4: Framework for the specification of evaluation methods and activities |
| ISO/IEC FDIS 15408-5 | Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 5: Pre-defined packages of security requirements                        |
| prEN 17640           | FITCEM -Fixed-Time Cybersecurity Evaluation Methodology for ICT (CEN/CLC JTC 13/WG 3)                                                                                         |
| ISO/SAE DIS 21434    | Road vehicles. Cybersecurity engineering                                                                                                                                      |
| ISO/CD 24089         | Road vehicles. Software Update Engineering                                                                                                                                    |
| ISO/AWI PAS 5112     | Road vehicles. Guidelines for auditing cybersecurity engineering                                                                                                              |

## Guías de referencia de las Organizaciones de Desarrollo de Estándares (SDO)

|                |                                                                                    |
|----------------|------------------------------------------------------------------------------------|
| NIST 800-30    | Guide for conducting risk assessments                                              |
| NIST 800-88    | Guidelines for media sanitization                                                  |
| NIST SP 800-50 | Building an information technology security awareness and training program         |
| NIST SP 800-61 | Computer security incident handling guide                                          |
| SAE J3061      | Cybersecurity guidebook for cyber-physical vehicle systems                         |
| SAE J3101      | Requirements for hardware protected security for ground vehicle applications       |
| SAE J3138      | Guidance for securing the Data Link Connector (DLC)                                |
| 3GPP TR 33.836 | Study on security aspects of 3GPP support for advanced V2X services                |
| 3GPP TS 33.536 | Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services |

## 5.2 Ciberseguridad en el ámbito de Sistemas Inteligentes de Transporte (ITS)

Se presentan las siguientes referencias de normas y proyectos relativos a la ciberseguridad en las comunicaciones y en Sistemas Inteligentes de Transporte (ITS).

### Comité nacional UNE:

CTN 159 Sistemas inteligentes de transporte

### Comités internacionales relacionados:

ISO/TC 204 *Intelligent transport systems*

CEN/TC 278 *Intelligent transport systems*



## Normas y proyectos:

|                           |                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UNE-CEN ISO/TS 19299:2015 | Peaje electrónico. Marco de seguridad (ISO/TS 19299:2015).                                                                                                                                                                                                                                                                                                                        |
| UNE-CEN ISO/TS 21177:2019 | Sistemas inteligentes de transporte. Servicios de seguridad de estaciones ITS para el establecimiento y la autenticación segura de sesiones entre dispositivos confiables (ISO/TS 21177: 2019)                                                                                                                                                                                    |
| UNE-CEN/TR 16968:2016     | Peaje electrónico. Evaluación de las medidas de seguridad para aplicaciones que usan la comunicación dedicada de corto alcance.                                                                                                                                                                                                                                                   |
| UNE-CEN ISO/TS 17574:2017 | Peaje electrónico. Directrices para los perfiles de protección de la seguridad (ISO/TS 17574:2017)                                                                                                                                                                                                                                                                                |
| PNE-FprCEN/TR 17464       | Espacio. Utilización del posicionamiento basado en GNSS para los sistemas de transporte por carretera inteligentes (ITS). Modelado de ataques de seguridad y definición de características de rendimiento y de métricas relacionadas con la seguridad                                                                                                                             |
| PNE-FprCEN/TR 17475       | Espacio. Utilización del posicionamiento basado en GNSS para los sistemas de transporte por carretera inteligentes (ITS). Especificación de las instalaciones de ensayos, definición de escenarios de ensayos, descripción y validación de los procedimientos para ensayos de campo relacionadas con el rendimiento de seguridad de terminales de posicionamiento basados en GNSS |
| PNE-prEN 16803-3          | Espacio. Uso del posicionamiento basado en GNSS para sistemas de transporte inteligente en carretera (ITS). Parte 3: Evaluación de los rendimientos de seguridad de los terminales de posicionamiento basados en GNSS                                                                                                                                                             |
| PNE-prEN ISO 19299        | Peaje electrónico. Marco de seguridad (ISO/DIS 19299:2019).                                                                                                                                                                                                                                                                                                                       |

## 6 Ciberseguridad en las comunicaciones intra-vehiculares

En el panorama actual existen varios protocolos de comunicación entre los dispositivos internos del vehículo que se van implementando poco a poco. Algunos de estos protocolos son:

- CAN-BUS: Diseñado específicamente para la comunicación intra-vehicular a principios de los años 80. El acrónimo CAN viene de *Controller Area Network* y, como es fácil de intuir, en sus inicios incluía una topología en forma de BUS con el fin de reducir cableado en el vehículo. La velocidad máxima es de 1Mb/s, aunque evoluciones posteriores (CAN-FD, CAN-XL), aumenta hasta 5/10 Mb/s respectivamente. Estandarizado en ISO 11898-2 (CAN-FD), ISO 11898-3 (CAN). CAN-XL todavía no ha sido estandarizado.
- FlexRay: Evolución del CAN-BUS desarrollado por un consorcio entre varios OEMs. La principal ventaja frente al CAN-BUS es que permitía un ancho de banda de 10 Mb/s. Estandarizado en la familia de estándares ISO 17458. La definición de casos de uso se estandarizó en ISO 10681-1.

- LIN: El acrónimo LIN significa *Local Interconnect Network* y es básicamente una segmentación de dispositivos conectados al CAN-BUS. De esta forma es posible por ejemplo agrupar dispositivos relacionados con el motor y dispositivos relacionados con el confort del usuario. El ancho de banda está limitado a 40 kb/s. Estandarizado en la familia de estándares ISO 17987.
- MOST: Del inglés *Media Oriented Systems Transport*. Se trata de un bus que utiliza fibra óptica plástica (POF) o pares de cobre trenzado. Hay tres tipos de MOST dependiendo de la velocidad máxima que pueden alcanzar. De este modo, MOST25, MOST50 y MOST 150 pueden alcanzar 25, 50 y 150 Mb/s respectivamente. Los dos primeros tipos estaban muy orientados a la distribución de video y audio dentro del coche para sistemas de entretenimiento, mientras que el segundo soportaba el transporte de tramas Ethernet. Estandarizado en la familia de estándares ISO 21806.
- K-Line: Protocolo de diagnóstico de muy baja velocidad descrito en las normas ISO 9141 e ISO 14230-1 que se utiliza para conectar un dispositivo externo con el vehículo a través del puerto OBD-II.
- Ethernet: Las necesidades cada vez más exigentes de transmitir datos dentro del vehículo dan lugar a la utilización de Ethernet dentro del vehículo, asegurando así una latencia muy baja y alta disponibilidad. Además, su implementación en el vehículo permite la reutilización de protocolos altamente utilizados de forma extensiva en otras redes Ethernet (WiFi, centros de datos, comunicaciones basadas en TCP/IP), incluyendo aquellos de encriptación y autenticación ya desarrollados para redes más extensas. Vehículos que ruedan hoy en carretera utilizan velocidades de hasta 1 Gb/s basadas en fibra óptica plástica (POF) o cable de cobre trenzado y apantallado. Estandarizado en la familia de estándares ISO 21111 e ISO/IEC/IEEE 8802-3. Hay desarrollos en estandarización para comunicaciones intra-vehiculares de hasta 100 Gb/s en IEEE sobre fibra óptica y cable de cobre trenzado y apantallado.
- Etc...

No se conoce si en el futuro se utilizará un mismo estándar para todos los fabricantes o si cada uno seguirá (como hasta ahora) implementando las tecnologías que mejor se adapten a sus vehículos. Sin embargo, la tendencia actual es el uso cada vez más extendido de las soluciones basadas en Ethernet debido a que permite la reutilización de protocolos de gestión, control de latencia, autenticación y cifrado entre otros ya probados extensamente en todo tipo de redes de comunicaciones.

## 6.1 Seguridad en CAN-BUS

Es importante destacar que, en la actualidad, uno de los elementos principales de comunicación intra-vehicular (entre los distintos elementos, sensores, ECUs y TCUs en el vehículo) es el CAN-BUS.

Los riesgos de seguridad asociados al CAN-BUS son evidentes, ya que a fecha de hoy no existen mecanismos de seguridad básicos como pueden ser la segmentación de la red, validación de los componentes de la misma o el filtrado de comportamientos anómalos, por lo que cualquier dispositivo que se conecta a la red es capaz de enviar tráfico a través de ésta.



Además, dado que los servicios de diagnóstico y toma de datos del vehículo funcionan también a través de este protocolo, los vehículos incluyen un conector especial llamado OBD-II que suele encontrarse de forma accesible para que se puedan realizar intervenciones cómodamente.

Históricamente se han reportado ataques que utilizan el conector OBD-II con el fin de inyectar tramas en el CAN-BUS y modificar el comportamiento de los elementos conectados a dicho bus, por ejemplo ataques de denegación de servicio consistentes en inyectar tramas de error haciendo creer al sistema que provienen de uno de los elementos en concreto para que el resto de elementos detecten el error y decidan obviar la información procedente del elemento atacado, con lo que un posible intruso podría llegar incluso a suplantar el elemento atacado.

La evolución de estos ataques consiguió superar la barrera del conector físico, habiéndose reportado ataques remotos que utilizan vulnerabilidades en las redes de comunicaciones y en los sistemas de *infotainment* (información y entretenimiento) del vehículo para acceder a la red CAN.

Es evidente que en una red de vehículos conectados, toda la información que llegara a un vehículo cuyo software ha sido comprometido podría modificarse en tiempo real y, a su vez, transmitir a la red o a otros vehículos (C-V2X y U-V2X tal y como se comentaba en puntos previos de este Informe) información errónea o maliciosa. Por otro lado, el vehículo también debería ser capaz de discernir si la información que está recibiendo del exterior proviene de una fuente fiable y no ha sido alterada durante su transmisión.

No existe una única forma de mejorar la seguridad en el CAN-BUS dado que haría falta la combinación de varios elementos que fueran capaces de detener un ataque en tiempo real. Por otro lado, los elementos actuales no son capaces de procesar toda la información que circula por el bus y analizarla en tiempo real sin introducir un retraso en la transmisión, lo cual podría ser fatal en muchas circunstancias y tener un impacto real en la seguridad (*safety*) del vehículo.

Para proteger el CAN-BUS no sería suficiente con un dispositivo que incorporara reglas para analizar el tráfico del bus como si de un antivirus convencional se tratara, debería incorporar también un motor de Inteligencia Artificial (IA) para el análisis del comportamiento y el conocimiento del entorno, ya que en algunas ocasiones detener un ataque puede suponer un impacto en la seguridad de los ocupantes y del resto de ocupantes de la vía mientras que en otras circunstancias ese mismo ataque podría tener un impacto mínimo. Se necesitaría definir un IDS/IPS adaptado a un automóvil.

## 6.2 Seguridad en Ethernet

Uno de los puntos destacables de las redes intra-vehiculares basadas en Ethernet es que todos los protocolos previamente desarrollados para la protección de datos en entornos de redes locales (LAN) son directamente reutilizables dentro del vehículo.

De este modo, protocolos como MACSec, estandarizado dentro del ISO/IEC/IEEE 8802-1AE, utilizado junto con el protocolo de autenticación de dispositivo e intercambio y gestión de claves estandarizado dentro del ISO/IEC/IEEE 8802-1X, garantizan la autenticación y encriptación del tráfico de datos intercambiado entre ECUs.

Adicionalmente, MACSec incluye un chequeo de la integridad del mensaje recibido, por lo que dificulta los ataques "Man-in-the-middle".

En cuanto a la protección ante la inserción de tramas previamente grabadas, MACSec, utilizado en conjunción con ISO/IEC/IEEE 8802-1X, rechazará todo el tráfico que no esté cifrado con una clave simétrica válida. Adicionalmente, cada trama lleva asociado un número de paquete, que a su vez está protegido por los algoritmos de encriptación y autenticación, con lo que cualquier paquete fuera de secuencia es automáticamente descartado por el receptor.

MACSec actúa en la capa 2 (MAC layer) del sistema OSI, y es generalmente implementado en hardware. Esta hace posible combinarlo con otros protocolos de seguridad en capas superiores, como IPSec o TLS.

## 6.3 Ejemplos de redes vehiculares

A continuación, se incluyen a modo ilustrativo algunos ejemplos de las estructuras de redes de comunicaciones más comunes en los vehículos:

- Red "powertrain" engloba las unidades de control destinadas coordinar la motopropulsión del vehículo (cambios de marchas, caja de transferencia, suspensión neumática, sensores...) utiliza el protocolo CAN-BUS, incluye las ECU'S DDE, DME, EGS (unidad del cambio automático) VTG (control caja de transferencia) ECAS (unidad control suspensión neumática), EKPS (Unidad de bomba de combustible)... Normalmente su arquitectura está basada en ARM con procesadores SH, Tricore...
- Red "chasis control" está formada por los sistemas destinados a ayudarnos en la conducción, incluye entre otros los sistemas de frenado, airbag, dirección asistida.
- Red "body control" es desarrollada para comandar las unidades de carrocería, es decir: las que controlan cierre centralizado, cuadro de mandos, climatización etc. Utiliza los protocolos Can, Flexray, rf... incluye las ECU'S, ABS / DSC / ESP CAS y AIRBAG.
- Red "entertainment" incluye el sistema de navegación, los TCU o sistemas telemáticos, sistemas de comunicaciones bluetooth... Utiliza los protocolos Most, WIFI, *Bluetooth*,... las funciones telemáticas podrán incluir la actualización del software de unidades, enviar datos del vehículo, con *ecall* enviar datos de posición en caso de accidente, enviar datos en caso de robo del vehículo, arranque de remoto del vehículo, gestión de flotas, *big data*.
- Red Ethernet permite la integración de todas las anteriores en un solo sistema de comunicaciones. Cada uno de los distintos tráfico en el vehículo es clasificado según sus necesidades en términos de ancho de banda, latencia y prioridad, garantizando la calidad de servicio en cada uno de ellos a través de redes virtuales (VLAN) o protocolos de red sensibles al tiempo (*Time Sensitive Networks*, TSN), como las estandarizados en ISO/IEC/IEEE 8802-1Q.



## 7 Regulaciones y certificaciones de Ciberseguridad en el ecosistema de la Movilidad Conectada y Automatizada (CAM)

A día de hoy las certificaciones de ciberseguridad en el ámbito del vehículo conectado y/o autónomo se encuentran en una etapa de desarrollo muy inicial.

Y aunque los primeros pasos se están dando, no existen todavía esquemas de certificación que sean aplicados de forma general en la industria o requeridos por reguladores o legisladores y que aborden de forma completa la seguridad de los ecosistemas del vehículo conectado.

A continuación, veremos algunas de las principales dificultades que se plantean al abordar este reto.

### El vehículo conectado, un sistema extremadamente amplio y complejo

El vehículo es un sistema extremadamente amplio compuesto por multitud de subsistemas, redes y componentes diferentes, que engloba un gran número de elementos diferentes desarrollados por diferentes fabricantes y que tienen características y requisitos de seguridad diferentes.

Si abrimos el abanico e incluimos el ecosistema del vehículo conectado y consideramos todos los elementos adicionales que tienen que interactuar con el vehículo y que será necesario proteger, el listado crece de forma exponencial.

Los sistemas de certificación se basan en normas técnicas que definen requisitos de seguridad específicos y metodologías de evaluación concretas para un determinado componente.

Cada uno de los elementos que están integrados en el vehículo conectado tiene características y requerimientos de seguridad diferentes y esto hace que resulte muy complicado definir especificaciones de requisitos de seguridad que cubran de forma general y completa todos los diferentes elementos y componentes de un vehículo y todos los escenarios de interacción entre ellos.

### Un entorno de operación global

Los esquemas de certificación son requeridos habitualmente por reguladores sectoriales (consorcios de industria) o legisladores (estados).

Los vehículos son vendidos y utilizados de forma global en todos los países del mundo y si pensamos en los componentes individuales de cada vehículo el número de países y consorcios industriales involucrados en la cadena de suministros es cada vez más elevado.

Lograr el consenso necesario entre los diferentes países y consorcios industriales que pueden establecer esquemas de certificación (voluntarios u obligatorios) para utilizar un mismo sistema de certificación es en sí mismo una tarea que requiere mucho tiempo para llegar a acuerdos internacionales o globales. Pero además ponerse de acuerdo en los requisitos mínimos de seguridad que pueden ser exigibles en cada país o por cada fabricante hace este trabajo aún más complicado.

## 7.1 Seguridad del vehículo conectado y la operación de servicios y procesos en el ecosistema CAM

En la seguridad del vehículo conectado interviene no solo el vehículo entendido como un producto final o como un conjunto de componentes hardware y software que deben cumplir unos ciertos requisitos de seguridad, sino que son igualmente relevantes los procesos de operación alrededor del producto (vehículo conectado).

Entre estos procesos de operación caben destacar:

### Los procesos de ingeniería asociados al vehículo

Bajo este concepto, se engloban todos los procesos de operación en el diseño, fabricación y mantenimiento del vehículo a lo largo de toda su vida útil.

### Los procesos de operación de los sistemas de movilidad conectada y automatizada (CAM)

De forma simplificada podemos definir los sistemas de Movilidad Conectada y Automatizada (CAM) como el ecosistema de servicios e infraestructuras que operan las redes de los sistemas inteligentes y cooperativos de transporte en los que se ubicará el vehículo conectado.

Los procesos de operación y servicios asociados a los sistemas CAM son extremadamente amplios y variados e involucran una gran variedad de actores y partes interesadas. El reciente informe de ENISA: "*Cybersecurity Stocktaking in the CAM*", analiza el detalle de estos servicios y sus necesidades de seguridad.

La consideración conjunta de los riesgos de seguridad de producto y de los procesos de operación en los futuros esquemas de certificación introduce una dificultad añadida (y no menor) para el diseño y desarrollo de estos esquemas.

La simple observación del alcance y variedad de los ecosistemas ligados a la operación del vehículo conectado, puede darnos una idea del reto al que nos enfrentamos en el desarrollo de los futuros esquemas de certificación.

## 7.2 Primeras iniciativas en certificación del vehículo autónomo conectado

### UNECE W.29/GRVA- Requisitos de ciberseguridad para la homologación de vehículos

El Foro Mundial para la Armonización de la Reglamentación sobre Vehículos es un grupo de trabajo de la Comisión Económica de las Naciones Unidas para Europa (UNECE W.29) que tiene como objetivo crear un sistema uniforme de reglamentos, para el diseño de vehículos con el objeto de armonizar los requisitos de homologación de vehículos a nivel global y facilitar el comercio internacional.





Dentro de este foro, el grupo de trabajo GRVA "*Working Party on Automated/Autonomous and Connected Vehicles*" desarrolla los reglamentos específicos para el vehículo conectado.

En junio de 2020 este organismo incluyó por primera vez en su catálogo de reglamentos, dos reglamentos que contienen requisitos de ciberseguridad para el vehículo conectado: *Cybersecurity requirements for vehicle type approval* y *Requirements for Over the Air Software Updates*.

El primero de ellos "*Cybersecurity requirements*" cubre de forma general los requisitos de ciberseguridad del vehículo (producto) y de los procesos de ingeniería asociados (desarrollo, producción, operación, mantenimiento y retirada del servicio).

Los requisitos de procesos incorporados en este reglamento utilizan como norma técnica base para referenciar los requisitos de seguridad el estándar internacional ISO 21434<sup>22</sup> que se encuentra a la fecha de publicación de este informe en fase final de desarrollo.

La norma ISO 21434 define un sistema de gestión de la ciberseguridad en los procesos de ingeniería del vehículo conectado, cubriendo todas las fases del ciclo de vida del vehículo: desarrollo, producción, operación, mantenimiento y retirada del servicio.

Al respecto de los requisitos de seguridad de producto, ante la falta de un estándar internacional que especifique requisitos de producto para el vehículo conectado de forma genérica, los requisitos de productos definidos aquí, han sido desarrollados de forma interna por el grupo de trabajo específico de UNECE (*Task Force on Cybersecurity and OTA updates*).

El segundo reglamento "*Cybersecurity and OTA updates*" define de forma general los requisitos mínimos de los procesos de actualización de software vía radio, para la homologación de vehículos y entre ellos se consideran requisitos específicos de ciberseguridad.

Este segundo reglamento descansa sobre la base del estándar internacional ISO 24089<sup>23</sup> (que también se encuentran a la fecha de publicación de este informe en fase de desarrollo).

Ambos reglamentos entraran a formar parte de los requisitos de homologación de vehículos, en la Unión Europea a partir de Julio de 2022 para nuevos vehículos y en julio de 2024 para todos.

Esta regulación de UNECE puede considerarse el primer esquema de certificación obligatorio para vehículos conectados que incorpora requisitos de ciberseguridad. Y será aplicable en 54 países que forman parte del WP.29, entre ellos los 26 estados europeos y Japón y Corea del Sur.

---

22 <https://www.iso.org/standard/70918.html>

23 <https://www.iso.org/standard/77796.html>

## 7.3 Primeras iniciativas de certificación de los procesos de fabricación, desarrollo y operación del vehículo

### Esquema de certificación ISO 21434. La nueva norma ISO PAS 5112

En paralelo a este esquema de homologación de vehículos, ISO está desarrollando actualmente la norma ISO/AWI PAS 5112: **"Road vehicles — Guidelines for auditing cybersecurity engineering."**<sup>24</sup>.

Esta norma establece las guías de auditoría para los requisitos del sistema de gestión definido en ISO 21434 y sienta las bases para un futuro esquema de certificación de tercera parte independiente bajo la estructura de las entidades de acreditación internacionales.

Esta certificación de carácter voluntario, es esperable que sea adoptada como referencia de buenas prácticas no solo por los fabricantes de vehículos, que ya se verán afectados por la regulación de UNECE, sino por todo el ecosistema de fabricantes de componentes, cadenas de suministros y operadores de servicios involucrados en los procesos de ingeniería del vehículo conectado.

## 7.4 Primeras iniciativas de certificación de productos (componentes) del vehículo

En materia de certificación de productos con altos requisitos de seguridad, el esquema de certificación más ampliamente utilizado y reconocido a nivel global es la certificación de *Common Criteria* (CC) bajo el paraguas del grupo SOG-IS (grupo de oficiales de seguridad europeos) y el acuerdo de reconocimiento mutuo que extiende el alcance de las certificaciones CC a 31 países.

Este esquema ha sido recientemente adoptado dentro del marco del reglamento Europeo de Ciberseguridad (*Cybersecurity Act* o CSA) y será formalmente implementado como el primer esquema europeo de certificación de ciberseguridad de productos bajo el nombre de EUCC a lo largo del año 2021.

El esquema de *Common Criteria* y el futuro EUCC, están basados en una metodología general de evaluación de la seguridad de los productos (CEM, en sus siglas en inglés) y en especificaciones concretas de requisitos para cada producto (declaraciones de seguridad o ST en sus siglas en inglés) o tipo de productos (Perfiles de protección o PP).

La industria automotriz está dando sus primeros pasos en el desarrollo de perfiles de protección para componentes de vehículos. Entre ellos caben destacar aquí:

- Los perfiles de protección para tacógrafos<sup>25</sup> desarrollados por el *Joint Research Centre of the European Commission*.

---

24 <https://www.iso.org/standard/80840.html>

25 [https://www.commoncriteriaportal.org/files/ppfiles/pp0094b\\_pdf.pdf](https://www.commoncriteriaportal.org/files/ppfiles/pp0094b_pdf.pdf)



- El perfil de protección desarrollado por el BSI Alemán (organismo de certificación del esquema CC en Alemania) para equipos de señalización en la carretera<sup>26</sup>.
- El perfil de protección desarrollado por la Federación Internacional del Automóvil para una unidad genérica de comunicaciones del vehículo<sup>27</sup> (PP pendiente de certificación en CC).
- Los perfiles de protección que se están desarrollando en el Consorcio industrial "Car2Car Communication Consortium" para los elementos más críticos en las comunicaciones del vehículo: el V2X HSM<sup>28</sup> o módulo criptográfico en el que descansa toda la base de la seguridad de los datos transmitidos o recibidos por el vehículo y la unidad de telecomunicaciones (Gateway) que transmite y recibe toda la información del exterior del vehículo (actualmente en desarrollo).

Y a su vez los legisladores europeos están comenzando a incluir requisitos de certificación de los PP existentes en las primeras regulaciones, entre las que cabe mencionar:

- El Reglamento de Ejecución (UE) 2019/1213 de la Comisión de 12 de julio de 2019<sup>29</sup> por el que se establecen disposiciones detalladas para garantizar unas condiciones uniformes a efectos de aplicar la interoperabilidad y la compatibilidad de los equipos de pesaje a bordo con arreglo a la Directiva 96/53/CE del Consejo y que incluye requisitos de certificación CC para los módulos de pesaje (OBW) del vehículo y referencia PP de los módulos V2X HSM y Gateway de Car2Car.
- El Reglamento (UE) 165/2014<sup>30</sup> del Parlamento Europeo y del Consejo, que establece los requisitos para la construcción, ensayo, instalación, funcionamiento y reparación de los tacógrafos y de sus componentes y que referencia a los requisitos de seguridad de los perfiles de protección del *Joint Research Centre* de la Comisión Europea para tacógrafos.

Cabe destacar aquí también, las primeras iniciativas de la regulación europea de sistemas cooperativos e inteligentes de transporte (C-ITS *Delegated Act*) que fueron presentadas en marzo de 2019 y posteriormente retiradas en julio de 2019<sup>31</sup> tras una objeción del Consejo Europeo al respecto de la neutralidad tecnológica, incluían requisitos de certificación CC para los módulos criptográficos y de comunicaciones tanto del vehículo como de las unidades externas.

Es esperable que futuras revisiones de la C-ITS *Delegated Act* puedan seguir la senda abierta e incorporen requisitos de certificación CC, esta vez ya posiblemente bajo el nuevo esquema de certificación europeo EUCC gestionado por ENISA.

---

26 [https://www.commoncriteriaportal.org/files/ppfiles/pp0106b\\_pdf.pdf](https://www.commoncriteriaportal.org/files/ppfiles/pp0106b_pdf.pdf)

27 <https://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29/WP29-181-10e.pdf>

28 [https://www.car-2-car.org/fileadmin/documents/Basic\\_System\\_Profile/Release\\_1.3.0/C2CCC\\_PP\\_2056\\_HSM.pdf](https://www.car-2-car.org/fileadmin/documents/Basic_System_Profile/Release_1.3.0/C2CCC_PP_2056_HSM.pdf)

29 <https://op.europa.eu/en/publication-detail/-/publication/a5b9c070-a92c-11e9-9d01-01aa75ed71a1/language-en>

30 [https://www.commoncriteriaportal.org/files/ppfiles/pp0106b\\_pdf.pdf](https://www.commoncriteriaportal.org/files/ppfiles/pp0106b_pdf.pdf)

31 <https://ec.europa.eu/transparency/regdoc/rep/1/2019/EN/COM-2019-464-F1-EN-MAIN-PART-1.PDF>

## Futuras evoluciones en la aplicación de *Common Criteria* o EUCC en el vehículo conectado

Las principales dificultades para utilizar ampliamente las certificaciones CC (o del nuevo esquema de certificación europeo EUCC que sustituirá a CC a partir de 2021), en el ámbito del vehículo conectado vienen dadas por:

- Por un lado, por la falta de Perfiles de Protección que den una respuesta consensuada desde las normas técnicas y los estándares internacionales a los requisitos de seguridad de los diferentes componentes del vehículo, definiendo de una forma transparente y consensuada por todos los expertos a nivel internacional las garantías de seguridad exigibles de acuerdo al uso previsto para cada componente.
- Y, por otro lado, por la necesidad de contemplar el vehículo en su totalidad, considerando de una forma unificada todos los diferentes componentes que conforman el vehículo conectado y su ecosistema de servicios y procesos asociados (CAM / C-ITS).

Al respecto de la falta de perfiles de protección, podemos decir que este es el proceso natural de cualquier nueva industria que se adentra en la adopción de esquemas de certificación con altos requisitos de garantías de seguridad y que el desarrollo de estos perfiles de protección se irá desarrollando poco a poco en el futuro, pero llevará todavía tiempo. Y que el tiempo invertido en llegar a consensos amplios entre los expertos en las organizaciones de estandarización para definir los perfiles de protección es la más alta garantía que se puede dar sobre la fiabilidad de los requisitos de seguridad que deben ser aplicados.

Puede haber caminos más rápidos para tratar de ofrecer soluciones particulares o privadas definiendo requisitos de seguridad fuera de las SDOs<sup>32</sup>, sin la complejidad de conseguir el consenso entre todos los expertos y todas las partes involucradas y reduciendo la transparencia de los procesos, pero no son caminos que lleven más lejos ni que ofrezcan más garantías.

El esfuerzo conjunto de los fabricantes de componentes y de vehículos, de los expertos en las organizaciones de estandarización y de los reguladores es sin duda la mejor apuesta para hacer avanzar las certificaciones de seguridad en estos niveles de garantías.

Al respecto de la dificultad de certificar el vehículo en su conjunto, podemos señalar que este es un problema común a muchas otras industrias y que no solo afecta al vehículo. Actualmente los grupos de expertos en estandarización están dedicados a buscar soluciones que permitan la certificación incremental de módulos que interoperan entre ellos conformando sistemas mayores.

Una de las más destacables es la iniciativa del ISO/IEC JTC 1/SC 27 WG3 con el estudio sobre "*Criterios de evaluación de la seguridad de la información de los vehículos conectados basados en la norma ISO/IEC 15408*". En este estudio (actualmente en desarrollo todavía), se analizan específicamente las dificultades y posibles soluciones para utilizar esta metodología de forma amplia en el ámbito de vehículo conectado.

---

32 Standardization Development Organizations (Organizaciones de Desarrollo de Estándares).



También es necesario reseñar que la próxima evolución de las normas ISO/IEC 15408 y el nuevo esquema europeo EUCC incluyen nuevas capacidades en este área de la certificación por composición que serán claves en el desarrollo de estas certificaciones en la industria del vehículo conectado.

## 7.5 Normas y Certificaciones en los sistemas de comunicaciones del vehículo conectado

### Certificaciones de los sistemas DSRC

Como se ha descrito antes, las primeras iniciativas para desarrollar requisitos de certificación de los sistemas DSRC, han venido dadas desde la perspectiva de certificación de productos o componentes específicos de los sistemas DSRC de la mano de la regulación Europea y están basadas en las normas ISO/IEC 15408 e ISO/IEC 18045 *Common criteria*.

La norma ISO/IEC 15408 se caracteriza por estructurar evaluaciones de seguridad que cubren todas las áreas posibles de un producto:

- Verificación de la documentación de producto.
- Auditoria de los procesos de desarrollo y fabricación.
- Auditoria de los procesos de operación durante el ciclo de vida del producto.
- Verificación de las funcionalidades de seguridad implementadas.
- Auditoria de vulnerabilidades y test de penetración.

### Esquemas de certificación de Pruebas Funcionales (*Functional Testing*)

En otro nivel, existen esquemas de certificación, habitualmente desarrollados por consorcios industriales, que están focalizados en pruebas funcionales y de interoperabilidad.

El objetivo de estas certificaciones es verificar las funcionalidades operativas de los productos, y garantizar la correcta implementación de los protocolos de comunicaciones y la interoperabilidad de los diferentes equipos entre sí.

En este ámbito podemos destacar el consorcio industrial OMNIAIR<sup>33</sup> y su esquema de certificación de sistemas DSRC que incluye entre sus pruebas funcionales, la verificación de las funciones de seguridad de estos equipos.

A continuación, se referencian los estándares más importantes en estas pruebas funcionales.

---

33 <https://omniair.org/services/connected-vehicle-certification/>

## Estándares:

|                            |                                                                                                                                                                     |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IEEE 802.11:2012           | Physical Layer (PHY) & MAC (Transmit & Receive, Power & Sensitivity)                                                                                                |
| IEEE 1609.2:2017           | Security Services (BSMs and WSAs, Certificate Changes/Authentication)                                                                                               |
| IEEE 1609.3:2016           | Network Services (PSIDs/Data Rates/Power/Channels, WSMs, WSAs & IPv6)                                                                                               |
| IEEE 1609.4:2016           | Multi-Channel Operations (Continuous & Alternating, Transmission Rates, WSMs & IPv6 packets)                                                                        |
| SAE J2735:2016             | Message Dictionary (BSMs for OBUs and BSMs(Rx), SPaT, MAP & TIMs for RSUs)                                                                                          |
| SAE J2945/1:2016           | V2V Minimum Performance (Bench – BSM contents, Field Drive Test Attributes & Location Accuracy) for OBUs                                                            |
| USDOT FHWA-JPO-17-589:2017 | RSU 4.1 (Packaging Environment Attributes, Data Logging, SNMP Commands, Time Source accuracy, SPaT/MAP/WSA Messaging, Immediate Forwarding / Store&Repeat) for RSUs |

## Certificaciones de los sistemas ITS basados en redes de telecomunicaciones 5G

En el ámbito de las comunicaciones celulares existen igualmente consorcios industriales focalizados en las pruebas funcionales y los casos de uso de esta tecnología en el ámbito del vehículo. Entre ellos hay que destacar la asociación internacional *5G Automotive Association* (5GAA)<sup>34</sup> que engloba a la mayoría de fabricantes de vehículos y empresas de telecomunicaciones trabajando de forma coordinada para desarrollar los casos de uso de la tecnología 5G en el ámbito del vehículo conectado.

5GAA y ETSI realizan de forma conjunta *plugfest* o seminarios de pruebas, donde desarrollan baterías de tests operacionales y bajo diferentes casos de uso con el fin de probar y verificar la funcionalidad e interoperabilidad de los diferentes elementos que componen la tecnología 5G aplicada al vehículo conectado.

Y en particular los sistemas de Clave Pública (PKI) que gestionaran de forma centralizada los sistemas de certificados digitales que se utilizaran para identificar los vehículos en los sistemas de transporte inteligentes.

A continuación, se detallan los principales estándares de ISO, CEN y ETSI donde se incorporan y definen las características de seguridad de estos sistemas.

## Normas y proyectos:

|                            |                                                                                |
|----------------------------|--------------------------------------------------------------------------------|
| ETSI EN 302 636-4-1 V1.4.1 | Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking   |
| ETSI TS 103 097 v1.3.      | ITS Security; Security header and certificate formats                          |
| ETSI TS 102 941 v1.3.11    | ITS Security; Trust and Privacy Management                                     |
| ETSI TS 102 940 v1.3.1     | ITS Security; ITS communications security architecture and security management |

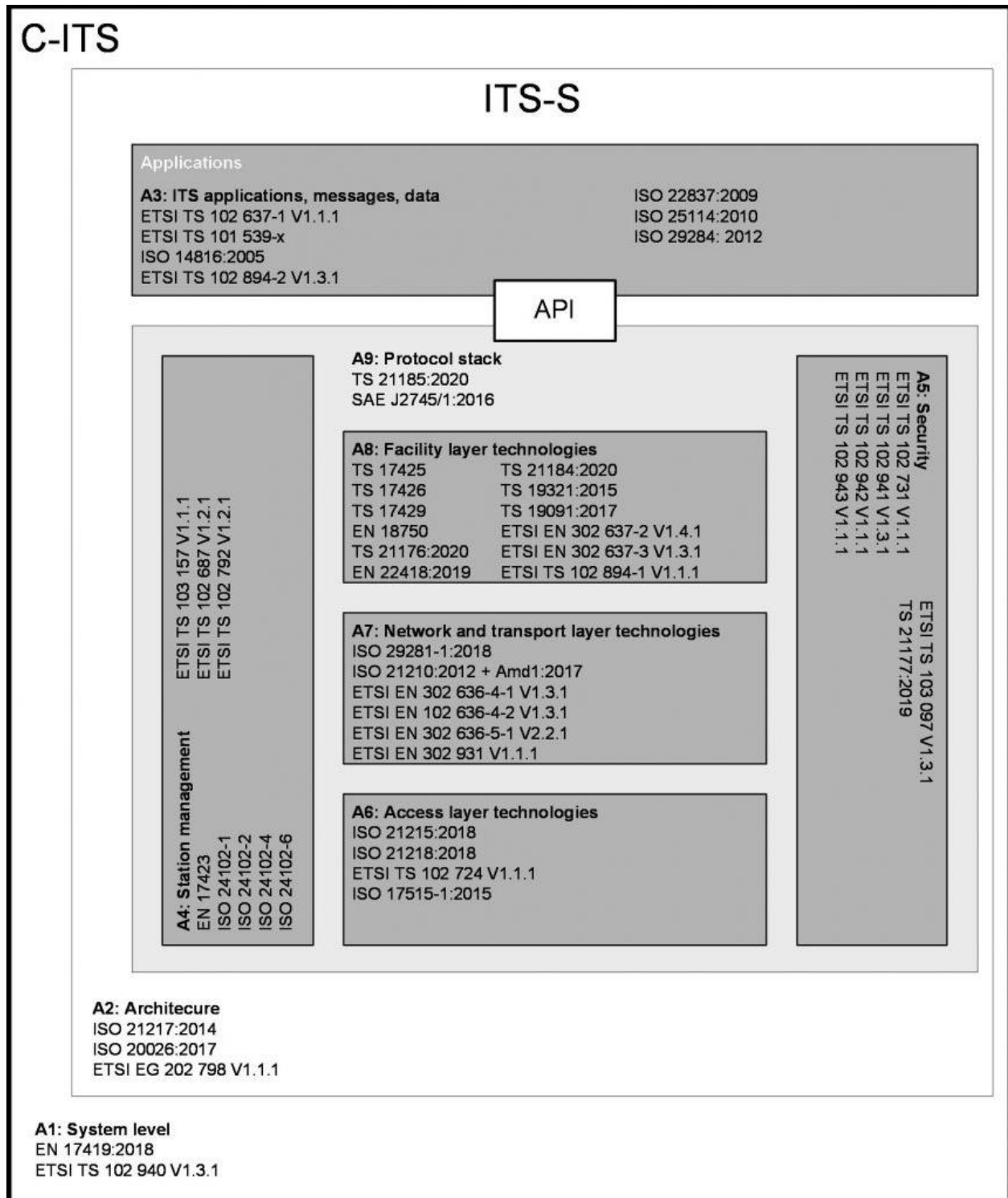
34 <https://5gaa.org/>



|                          |                                                                                                                                                                                                           |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ETSI EN 302 637-2 v1.4.1 | Specification of Cooperative Awareness Basic Service (CAM)                                                                                                                                                |
| ETSI EN 302 637-3 v1.3.1 | Specifications of Decentralized Environmental Notification Basic Service (DENM)                                                                                                                           |
| ETSI TS 103 600 v1.1.1   | Interoperability test specifications for security                                                                                                                                                         |
| ETSI TS 103 096-1 V1.4.1 | Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 1: Protocol Implementation Conformance Statement (PICS)                                              |
| ETSI TS 103 096-2 V1.4.1 | Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 2: Test Suite Structure and Test Purposes (TSS & TP)                                                 |
| ETSI TS 103 096-3 V1.4.1 | Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)       |
| ETSI TS 103 525-1 V1.1.1 | Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS PKI management; Part 1: Protocol Implementation Conformance Statement (PICS)                                        |
| ETSI TS 103 525-2 V1.1.1 | Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS PKI management; Part 2: Test Suite Structure and Test Purposes (TSS & TP)                                           |
| ETSI TS 103 525-3 V1.1.1 | Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS PKI management; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT) |
| ETSI TR 102 893          | Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)                                                                                                             |
| ISO/DIS 17427-1          | Intelligent transport systems. Cooperative ITS. Part 1: Roles and responsibilities in the context of co-operative ITS architecture(s)                                                                     |
| ISO/TS 21177:2019        | Intelligent transport systems. ITS station security services for secure session establishment and authentication between trusted devices                                                                  |
| ISO/PRF TR 21186-3       | Cooperative intelligent transport systems (C-ITS). Guidelines on the usage of standards. Part 3: Security                                                                                                 |
| CEN/TS 21177             | Intelligent transport systems. ITS station security services for secure session establishment and authentication between trusted devices                                                                  |

## Estructura general de las normas técnicas en los sistemas ITS

El siguiente gráfico, muestra la estructura general de normas técnicas y estándares que cubren las arquitecturas de comunicaciones de los sistemas ITS.



Fuente: CEN-CLC / TC 278





## Esquemas de certificaciones de seguridad en las redes de telecomunicaciones 3G, 4G y 5G

En el ámbito de las comunicaciones celulares los esquemas de certificación de ciberseguridad están dando sus primeros pasos, al igual que en la industria del vehículo conectado. A continuación, se detallan las principales iniciativas en esquemas de certificación de seguridad.

### Esquema de certificación 3GPP SECAM and SCAS (*SeCurity Assurance Methodology/ Specifications*)

El esquema de certificación SECAM ha sido desarrollado por el consorcio *The 3rd Generation Partnership Project* (más comúnmente conocido por sus siglas 3GPP).

3GPP congrega los esfuerzos de siete diferentes organizaciones colaboradoras (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC) entre las que destaca ETSI (quien publica de forma conjunta con 3GPP algunas de las normas técnicas más relevantes) y tiene como objetivo unificar y desarrollar normas y especificaciones técnicas en el ámbito de las tecnologías de telecomunicaciones.

Este esquema de certificación tiene su base en el marco de evaluación *Common Criteria* (ISO/IEC 15408 e ISO/IEC 18045) y el acuerdo de reconocimiento mutuo (MRA) que ya ha sido comentado anteriormente y comparte muchos de los conceptos y procedimientos utilizados.

Es un esquema de certificación de producto y se aplica específicamente a los equipos de red de telecomunicaciones y sus diferentes componentes.

La entidad de acreditación encargada de la gestión del esquema de certificación y la emisión de los certificados es la asociación internacional de la industria de telecomunicaciones GSMA.<sup>35</sup>

Al igual que en ISO/IEC 15408 e ISO/IEC 18045 *Common criteria* (CC) este esquema se basa en una metodología general de evaluación de las garantías de seguridad (*Security Assurance Methodology* SECAM) y unas especificaciones de seguridad particulares para cada tipo de componente de los equipos de red denominadas por sus siglas en inglés, *Security Assurance Specifications* (SCASs).

De forma similar a ISO/IEC 15408, la metodología de evaluación SECAM (desarrollada en el documento 3GPP TR 33.916) cubre todas las áreas de evaluación alrededor del producto, incluyendo: desarrollo de producto, gestión de los procesos de ciclo de vida del producto, pruebas funcionales de las funciones de seguridad y análisis de vulnerabilidades. Y la especificación técnica, 3GPP TS 33.117 contiene el catálogo general de garantías de seguridad con las que conformar las especificaciones de requisitos concretos de los productos (SCAS).

---

35 <https://www.gsma.com/>

A continuación se incluye un listado con las principales especificaciones técnicas que conforman este esquema de certificación:

### Especificaciones técnicas:

|                        |                                                                                                                                            |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| 3GPP TR 33.916 V15.1.0 | Security Assurance Methodology (SCAS) for 3GPP network products                                                                            |
| 3GPP TS 33.117         | Catalogue of General Security Assurance Requirements                                                                                       |
| 3GPP TS 33.116         | Security Assurance Specification for the MME network product class                                                                         |
| 3GPP TR 33.818 V0.6.0  | Technical Report Security Assurance Methodology (SECAM) and Security Assurance Specification (SCAS) for 3GPP virtualized network products  |
| 3GPP TR 21.905         | Vocabulary for 3GPP Specifications                                                                                                         |
| 3GPP TS 33.401         | 3GPP System Architecture Evolution (SAE); Security architecture"                                                                           |
| 3GPP TR 33.821         | Rationale and track of security decisions in Long Term Evolution (LTE) RAN / 3GPP System Architecture Evolution (SAE)                      |
| 3GPP TS 33.102         | 3G security; Security architecture                                                                                                         |
| 3GPP TR 33.926         | Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes                                        |
| GSMA FS.13             | Network Equipment Security Assurance Scheme. Overview <sup>36</sup>                                                                        |
| GSMA FS.14             | Network Equipment Security Assurance Scheme. Security Test Laboratory Accreditation Requirements and Process <sup>37</sup>                 |
| GSMA FS.15             | Network Equipment Security Assurance Scheme. Vendor Development and Product Lifecycle Requirements and Accreditation Process <sup>38</sup> |
| GSMA FS.16             | Network Equipment Security Assurance Scheme. Dispute Resolution Process <sup>39</sup>                                                      |

### Esquema de certificación 5G - NESAS *Security Assurance Specifications*

En una versión más evolucionada del esquema SECAM de 3GPP y apuntando específicamente a la certificación de los equipos de red 5G, GSMA ha desarrollado el esquema NESAS (*Network Equipment Security Assurance Scheme*) para la certificación de los equipos de red 5G.

Este esquema, sigue la base de la estructura de los esquemas de *Common Criteria* y SECAM y dispone de una red de laboratorios independientes que evalúan la conformidad de los productos contra unas especificaciones concretas de seguridad (SCAS) para cada tipo de equipo / componente de red 5G.

<sup>36</sup> [http://www.gsma.com/NESAS\\_Overview](http://www.gsma.com/NESAS_Overview)

<sup>37</sup> [http://www.gsma.com/NESAS\\_Test\\_Lab\\_Accreditation](http://www.gsma.com/NESAS_Test_Lab_Accreditation)

<sup>38</sup> [http://www.gsma.com/NESAS\\_Product\\_Lifecycle\\_Accreditation](http://www.gsma.com/NESAS_Product_Lifecycle_Accreditation)

<sup>39</sup> [http://www.gsma.com/NESAS\\_Dispute\\_Resolution](http://www.gsma.com/NESAS_Dispute_Resolution)



Las especificaciones de requisitos SCAS son desarrolladas por 3GPP y publicadas por ETSI como normas técnicas.

Entre las diferencias principales de este esquema con la versión anterior SECAM cabe destacar:

La auditoría de procesos ha sido separada de las tareas de evaluación propia de producto y puede llevarse a cabo por organizaciones independientes de los laboratorios.

Las áreas de evaluación han sido mejoradas con nuevos procedimientos y en esta versión incluyen:

- Seguridad por diseño.
- Sistemas de control de versiones.
- Control de cambios.
- Análisis de código fuente.
- Testing de seguridad.
- Formación del personal.
- Procesos de corrección de vulnerabilidades.
- Independencia en la corrección de vulnerabilidades.
- Gestión de la seguridad de la información.
- Automatización de procesos de fabricación.
- Control de proceso de fabricación.
- Gestión de la información de vulnerabilidades.
- Protección de la integridad del software.
- Identificadores únicos de versión de software.
- Comunicación de las correcciones de seguridad.
- Precisión de la documentación.
- Punto de contacto único de seguridad.
- Gestión del código fuente.
- Procesos continuos de mejora.
- Documentación de seguridad.

## Especificaciones técnicas en seguridad de las comunicaciones celulares:

|                |                                                                                                                |
|----------------|----------------------------------------------------------------------------------------------------------------|
| 3GPP TS 33.116 | Security Assurance Specification (SCAS) for the MME network product class                                      |
| 3GPP TS 33.117 | Catalogue of general security assurance requirements                                                           |
| 3GPP TS 33.216 | Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class                     |
| 3GPP TS 33.250 | Security assurance specification for the PGW network product class                                             |
| 3GPP TS 33.511 | Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class          |
| 3GPP TS 33.512 | 5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)                      |
| 3GPP TS 33.513 | 5G Security Assurance Specification (SCAS); User Plane Function (UPF)                                          |
| 3GPP TS 33.514 | 5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class         |
| 3GPP TS 33.515 | 5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class     |
| 3GPP TS 33.516 | 5G Security Assurance Specification (SCAS) for the Authentication Server Function (AUSF) network product class |
| 3GPP TS 33.517 | 5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class |
| 3GPP TS 33.518 | 5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class     |
| 3GPP TS 33.519 | 5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class       |

## Requisitos específicos de seguridad en las redes de telecomunicaciones aplicados al ámbito del vehículo conectado y las comunicaciones V2X

A continuación, se detallan las especificaciones de seguridad concretas desarrolladas por 3GPP / ETSI en la aplicación de las comunicaciones celulares al ámbito del vehículo conectado.

## Especificaciones e informes técnicos en comunicaciones celulares V2X:

|                                     |                                                                                                                                                           |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| ETSI / 3GPP TS 33.185<br>Release 16 | LTE 5G; Security aspect for LTE support of Vehicle-to-Everything (V2X) services                                                                           |
| 3GPP TR 33.885                      | Technical Specification Group Services and System Aspects; Study on security aspects for LTE support of Vehicle-to-Everything (V2X) services (Release 14) |
| 3GPP TR 33.836                      | Technical Specification Group Services and System Aspects; Study on Security Aspects of 3GPP support for Advanced V2X Services (Release 16)               |
| 3GPP TS 33.536                      | Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services                                                                        |



## 7.6 Esquemas de certificación de la criptografía en el vehículo conectado

La criptografía es la base de la ciberseguridad de cualquier sistema y en este sentido cobra una especial atención en el ámbito del vehículo conectado.

A nivel de esquemas de certificación de módulos criptográficos el más relevante puede considerarse la certificación FIPS-140 desarrollada inicialmente por los gobiernos de Estados Unidos y Canadá, para validar la efectividad de los módulos criptográficos implantados en los equipos.

La relevancia y reputación de FIPS 140 han convertido a este esquema en la referencia de facto en materia de certificación de módulos criptográficos.

En su última versión CMVP<sup>40</sup> FIPS-140-3<sup>41</sup>, en un proceso de armonización global de los requisitos técnicos, pasa de estar basado en normas nacionales NIST a basarse en la norma internacional ISO 19790, dando de esta forma un paso de gigante en la generalización de este estándar como base internacional de requisitos técnicos de seguridad para módulos criptográficos.

Aunque todavía no se han desarrollado requisitos específicos o regulaciones para los sistemas criptográficos del vehículo conectado, la relevancia y reputación de FIPS 140-3 y su reciente adaptación a la norma internacional ISO 19790 en su última versión, hacen pensar que esta norma pueda estar en la base de cualquier futuro esquema de certificación o requisitos regulatorios en materia de la criptografía del vehículo conectado.

A continuación, se incluyen las principales referencias documentales al respecto:

### Normas y proyectos

|                    |                                                                                              |
|--------------------|----------------------------------------------------------------------------------------------|
| ISO/IEC 19790:2012 | Information Technology. Security techniques. Security Requirements for Cryptographic Modules |
| ISO/IEC 24759:2017 | Information Technology. Security techniques. Test Requirements for Cryptographic Modules     |

## 7.7 Regulaciones

Hasta la fecha no existen regulaciones específicas que incluyan requisitos de seguridad en los vehículos autónomos o en sus sistemas de comunicación. Sin embargo, esto está a punto de cambiar y a la fecha de publicación de este informe ya hay varias regulaciones en fase de preparación que planean incorporar nuevos requisitos de ciberseguridad al vehículo conectado y los sistemas inteligentes de transporte.

---

40 CMVP *Cryptographic Module Validation Program*, <http://csrc.nist.gov/groups/STM/cmvp/>

41 FIPS-140-3 *Security Requirements for Cryptographic Modules*. FIPS 140-3 fue creado por el NIST y, de acuerdo con la Ley Federal de Modernización de la Seguridad de la Información (FISMA), es obligatorio para las contrataciones del gobierno estadounidense y canadiense.

A continuación, se presentan los principales proyectos regulatorios en fase de preparación. Hemos de resaltar aquí, que dado el estado preparatorio de estos proyectos la evolución de los mismos es incierta y su versión final puede diferir de los objetivos planteados inicialmente para el desarrollo de estas regulaciones.

### *European C-ITS Platform*

En el marco europeo, la Comisión decidió en 2014 establecer una plataforma común para el desarrollo de los sistemas inteligentes de transporte y vehículos conectados, denominada *C-ITS Deployment Platform*<sup>42</sup>.

En noviembre de 2016, se presentó por primera vez, la estrategia europea para Sistemas Cooperativos e Inteligentes de Transporte (C-ITS) que basaba la estrategia de seguridad en dos pilares: El desarrollo de una política de seguridad común para los sistemas C-ITS en todos los países europeos y una política de gestión de certificados digitales para los vehículos y demás elementos de los sistemas de C-ITS.

Finalmente, en marzo de 2019 se presentó la primera iniciativa de regulación de estos sistemas, conocida como la *C-ITS Delegated Act*, que no llegó a ser ratificada finalmente tras una objeción presentada por el Consejo Europeo con alegaciones sobre la neutralidad tecnológica de los sistemas de comunicaciones previstos para el vehículo autónomo.

Esta primera versión de la *C-ITS Delegated Act*, incluía por primera vez requisitos de ciberseguridad para los sistemas más críticos de las arquitecturas C-ITS basados en certificaciones ISO/IEC 15408 e ISO/IEC 18045 *Common criteria* (CC).

La *C-ITS Delegated Act*, está en fase de revisión y es esperable que futuras versiones, continúen la senda marcada inicialmente adoptando de manera formal los primeros requisitos de seguridad para los sistemas C-ITS.

A continuación, se incluyen las referencias de los principales documentos de estas iniciativas regulatorias y los requisitos de seguridad incluidos.

COM (2016) 766 "A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility"<sup>43</sup>

---

Press release: "Commission presents a Strategy towards cooperative, connected and automated mobility"<sup>44</sup>

---

Memo: "An EU strategy on cooperative, connected and automated mobility"<sup>45</sup>

---

Opinion of the European Economic and Social Committee<sup>46</sup>

---

Opinion of the European Parliament<sup>47</sup>

---

42 [https://ec.europa.eu/transport/themes/its/c-its\\_es](https://ec.europa.eu/transport/themes/its/c-its_es)

43 <http://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=CELEX:52016DC0766>

44 [https://ec.europa.eu/transport/themes/its/news/2016-11-30-c-its-strategy\\_es](https://ec.europa.eu/transport/themes/its/news/2016-11-30-c-its-strategy_es)

45 [http://europa.eu/rapid/press-release MEMO-16-3933\\_en.htm](http://europa.eu/rapid/press-release_MEMO-16-3933_en.htm)

46 <http://www.eesc.europa.eu/?i=portal.en.ten-opinions.41444>

47 <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0063+0+DOC+PDF+V0//EN>



---

Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) (Release 1, December 2017)<sup>48</sup>

---

Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) (Release 1.1, June 2018)<sup>49</sup>

---

Supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems<sup>50</sup>

---

Impact assessment accompanying the document Commission Delegated Regulation supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems<sup>51</sup>

## Directiva europea 2014/53/UE (RED) sobre la comercialización de equipos radioeléctricos

La directiva 2014/53/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014, más conocida por sus siglas en inglés "*Radio Equipment Directive (RED)*" establece un marco regulatorio para la comercialización de equipos de radio.

Esta directiva tiene como objetivo establecer un mercado único de equipos de radio estableciendo requisitos esenciales para la seguridad y la salud, la compatibilidad electromagnética y el uso eficiente del espectro radioeléctrico. Y sienta las bases para regulaciones adicionales con requisitos específicos en ámbitos como la ciberseguridad.

En este sentido, la Comisión Europea ha puesto en marcha varias iniciativas en paralelo con el objetivo de impulsar nuevas iniciativas regulatorias que desarrollen nuevos requisitos de ciberseguridad para los dispositivos conectados.

Los pasos más relevantes dados por la Comisión hasta la fecha, son los siguientes:

- [1] La Comisión Europea solicitó una evaluación de impacto sobre la posible invocación de los artículos 3 (3) (e) (protección de la privacidad de los datos) y 3 (3) (f) (características para evitar el fraude).
- [2] La Comisión Europea, DG GROW, solicitó a los organismos europeos de normalización (ESOs) que realicen una evaluación de los objetivos de seguridad para los actos delegados propuestos (artículo 3, apartado 3, letras d) / e) / f), inciso i) y artículo 4).
- [3] Los trabajos preparatorios están comenzando en este momento en las ESOs preparando nuevos estándares para cubrir los requisitos de seguridad que eventualmente podrían ser aplicados por algunas de las nuevas regulaciones.

---

48 [https://ec.europa.eu/transport/sites/transport/files/c-its\\_security\\_policy\\_release\\_1.pdf](https://ec.europa.eu/transport/sites/transport/files/c-its_security_policy_release_1.pdf)

49 [https://ec.europa.eu/transport/sites/transport/files/c-its\\_certificate\\_policy-v1.1.pdf](https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy-v1.1.pdf)

50 [https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=PI\\_COM:C\(2019\)1789](https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=PI_COM:C(2019)1789)

51 <https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=CELEX:52019SC0096>

Es esperable que los nuevos requisitos de ciberseguridad, afecten de forma directa a los elementos de comunicación radio que puedan incorporar los vehículos conectados.

A continuación, se incluyen las principales referencias documentales al respecto:

The Radio Equipment Directive 2014/53/EU (RED)<sup>52</sup>

---

Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment<sup>53</sup>

## 8 Futuros trabajos

Desde el punto de vista de la normalización y la estandarización, queda mucho trabajo por hacer en materia de seguridad y privacidad dentro del ámbito de la industria de la movilidad conectada y automatizada. Y será un reto diseñar y consensuar los estándares técnicos que permitan a la industria de la CAM crear un entorno confiable tanto en los riesgos de ciberseguridad como en los de privacidad.

En particular las nuevas tecnologías de inteligencia artificial y los sistemas autónomos son un campo nuevo para la ciberseguridad y la privacidad y constituyen un reto apasionante para la estandarización y normalización.

La interoperabilidad de los estándares en un ecosistema especialmente amplio y la necesidad de contar con un alcance global, añadirán nuevas cotas de complejidad al reto.

La criptografía post-cuántica y los sistemas de cifrado homomórficos ofrecerán nuevas capacidades de seguridad y privacidad y nuevos retos para consensuar y estandarizar estas soluciones.

La industria de la movilidad conectada y automatizada es sin duda, uno de los principales ámbitos de nuestra sociedad, donde será necesario contar con las más altas garantías de seguridad y privacidad.

El futuro apunta ser emocionante y traer apasionantes retos para la estandarización y la normalización.

---

52 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0053>

53 <https://ec.europa.eu/docsroom/documents/40763>



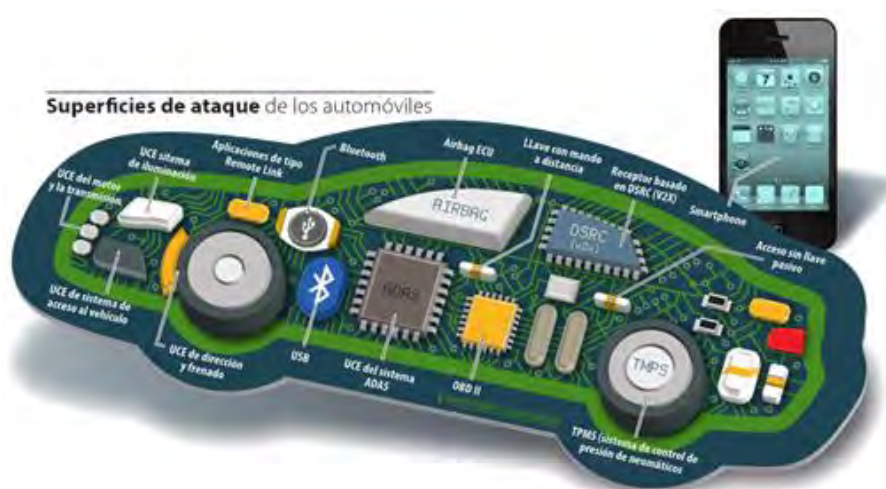


## ANEXO I

# Referencias de algunas amenazas de ciberseguridad del vehículo

En la actualidad los vehículos han pasado de estar formados por elementos mecánicos e hidráulicos a estar formados por elementos eléctricos y electrónicos los cuales pueden ser utilizados como nuevos vectores de ataque en la industria del vehículo y el ecosistema de la movilidad conectada y automatizada.

A continuación, se incluye a modo ilustrativo, algunas de las principales amenazas identificadas en este ámbito:



- Manipulación del software interno del vehículo.
- Modificación de coordenadas GPS.
- Robo de datos del vehículo.
- Sistema de cambio de carril.
- Vulnerabilidad APPs.
- Vulnerabilidad CAN-BUS.
- Vulnerabilidad control de cruce activo.
- Vulnerabilidad de las ECUs.
- Vulnerabilidad *key/less go*.
- Vulnerabilidad medios externos USB, Cd, actualizaciones online, radio RDS.
- Vulnerabilidad receptores del entorno, Yolo.
- Vulnerabilidad sistema confort.
- Vulnerabilidad sistema de intercambio de claves para la apertura.
- Vulnerabilidad sistemas de comunicaciones.
- Vulnerabilidad TPMS.
- Vulnerabilidad unidades telemáticas.
- Redes V2X.
- Sistemas por radiofrecuencia.
- Conectividad a través del USB o la toma OBD2.

## ANEXO II

# Documentos de referencia en las tecnologías de comunicación y conectividad para vehículos conectados

A continuación, se enumeran algunos de los estándares más relevantes y documentos de referencia, en el campo de las tecnologías de comunicación y conectividad para vehículos conectados:

- [1] ECC Report 101, Compatibility Studies in the band 5855– 5925 MHz between Intelligent Transport Systems (ITS) and other systems.
- [2] ECC Recommendation (08)01, Use of the band 5855-5875 MHz for Intelligent Transport Systems (ITS).
- [3] ETSI EN 302 571 v2.1.1 Intelligent Transport Systems (ITS); Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band.
- [4] (DRAFT) DTS/ITS-0010015 v1.1.4 (TS 101 539-2) Intersection Collision Risk Warning Specification.
- [5] DECISION ITSWG1(18)042010 Add Level of automation to data element “VehicleRole”.
- [6] 3GPP TS 22.185 Service requirements for V2X services.
- [7] (DRAFT) 3GPP TR 37.885 Study on evaluation methodology of new Vehicle-to-Everything V2X use cases for LTE and NR.
- [8] 3GPP TS 24.386 User Equipment (UE) to V2X control function; protocol aspects; Stage 3.
- [9] 3GPP TS 38.522 V0.1.0 NR; User Equipment (UE) conformance specification; Applicability of RF and RRM test cases (Release 15).
- [10] 3GPP TR 21.916; Technical Specification Group Services and System Aspects; Release 16 Description; Summary of Rel-16 Work Items (Release 16). “8. Advanced V2X support”.
- [11] 3GPP TS 24.386 User Equipment (UE) to V2X control function; protocol aspects; Stage 3.
- [12] ISO/IEC/IEEE 8802-1X:2013 Telecommunications and exchange between information technology systems. Requirements for local and metropolitan area networks. Part 1X: Port-based network access control.



- 
- [13] ISO/IEC/IEEE 8802-1AE:2020 Telecommunications and exchange between information technology systems. Requirements for local and metropolitan area networks. Part 1AE: Media access control (MAC) security.
  - [14] ISO/IEC/IEEE 8802-3:2017 Information technology. Telecommunications and information exchange between systems. Local and metropolitan area networks. Specific requirements. Part 3: Standard for Ethernet.
  - [15] ISO 21111-1:2020 Road vehicles. In-vehicle Ethernet. Part 1: General information and definitions.

UNE es el organismo  
de normalización español en:



**UNE**  
Normalización Española

Asociación Española  
de Normalización

(+34) 915 294 900 — [une@une.org](mailto:une@une.org)

[www.une.org](http://www.une.org)



# **Control y seguimiento de los costes de la flota de vehículos**



# CONTROL Y SEGUIMIENTO DE LOS COSTES DE LA FLOTA DE VEHÍCULOS





José Miguel Fernández Gómez ha desarrollado este libro para compartir la experiencia y el conocimiento adquirido durante su carrera laboral y académica en el ámbito de la gestión de las flotas de vehículos.

Soy el director de Advanced Fleet Management Consulting, nuestra compañía suministra servicios de consultoría y formación avanzada en gestión de flotas de vehículos, conoce nuestro curso de gestión de flotas.

Hemos desarrollado una metodología innovadora con la que conseguimos reducir el 20% de los costes de una flota de vehículos, así como una optimización de las actividades de la gestión de la flota.

Anteriormente trabajé en Insead (Francia), una de las mejores escuelas de negocio del mundo, realizando actividades de consultoría e investigación en un proyecto para la organización de refugiados de Naciones Unidas (UNHCR), optimizando el tamaño y la gestión de las actividades de la flota de vehículos, que tiene esta organización repartida por todo el mundo (6.500 vehículos), también fui gestor de flota de 1.000 vehículos en una compañía de limpieza viaria.

Soy Doctor Ingeniero Industrial por la Universidad Politécnica de Madrid, mención internacional, ya que realice estancias de investigación en la Universidad de Liverpool (UK) y en el Royal Institute of Technology-KTH (Suecia). Realizo investigación en la optimización de las actividades de la gestión de flotas de vehículos, y he desarrollado algunos modelos que he publicado en congresos internacionales de organización industrial.

Si quieres contactar con nosotros escríbenos al siguiente correo electrónico: [info@advancedfleetmanagementconsulting.com](mailto:info@advancedfleetmanagementconsulting.com)

Este libro está registrado en:



safe**creative**

1709283618115

INFO ABOUT RIGHTS

## ÍNDICE

|                                                                                  |           |
|----------------------------------------------------------------------------------|-----------|
| <b>1. INTRODUCCIÓN .....</b>                                                     | <b>5</b>  |
| <b>2. COSTES DE LA FLOTA DE VEHÍCULOS .....</b>                                  | <b>8</b>  |
| 2.1. COSTES FIJOS .....                                                          | 10        |
| 2.1.1. <i>Costes de capital</i> .....                                            | 10        |
| 2.1.2. <i>Costes de operación</i> .....                                          | 11        |
| 2.1.3. <i>Evolución de los costes fijos</i> .....                                | 12        |
| 2.2. COSTES VARIABLES DE OPERACIÓN .....                                         | 18        |
| 2.2.1. <i>Costes ineludibles</i> .....                                           | 18        |
| 2.2.2. <i>Costes eludibles</i> .....                                             | 19        |
| 2.2.3. <i>Evolución de los costes variables de operación</i> .....               | 20        |
| 2.3. COSTES INDIRECTOS .....                                                     | 21        |
| 2.3.1. <i>Evolución de los costes indirectos</i> .....                           | 22        |
| 2.4. EVOLUCIÓN DE LOS COSTES TOTALES .....                                       | 24        |
| 2.5. CÁLCULO DE LOS COSTES DE LA FLOTA DE VEHÍCULOS .....                        | 33        |
| 2.6. CÁLCULO DEL COSTE DE UN SERVICIO .....                                      | 38        |
| 2.7. CÁLCULO DEL COSTE DE PROPIEDAD TCO ( <i>Total Cost of Ownership</i> ) ..... | 47        |
| 2.8. PRESUPUESTO DE LA FLOTA .....                                               | 50        |
| 2.9. RENOVACIÓN DE LOS VEHÍCULOS DE LA FLOTA .....                               | 53        |
| <b>3. CONTROL Y SEGUIMIENTO DE LOS COSTES VARIABLES DE LA FLOTA .....</b>        | <b>59</b> |
| 3.1. INTRODUCCIÓN .....                                                          | 60        |



|                                         |            |
|-----------------------------------------|------------|
| 3.2. MODELO PROPUESTO .....             | 65         |
| 3.2.1. Caso práctico .....              | 73         |
| 3.2.2. Periodo 1.....                   | 73         |
| 3.2.3. Periodo 2.....                   | 75         |
| 3.2.4. Periodo 3.....                   | 77         |
| 3.2.5. Análisis de los resultados ..... | 79         |
| 3.2.6. Conclusiones.....                | 81         |
| <b>4. CUADRO DE MANDO.....</b>          | <b>82</b>  |
| <b>5. ANEXO.....</b>                    | <b>102</b> |
| 5.1. CASO PRÁCTICO .....                | 103        |
| 5.1.1. Periodo 1.....                   | 103        |
| 5.1.2. Periodo 2.....                   | 106        |
| 5.1.3. Periodo 3.....                   | 109        |
| <b>6. REFERENCIAS .....</b>             | <b>112</b> |

# 1. INTRODUCCIÓN

---

La gestión de una flota es la utilización de un conjunto de vehículos con el objetivo de prestar un servicio a un tercero o realizar una actividad en una organización, de la forma más eficiente y eficaz cumpliendo con un determinado nivel de servicio y coste.

Los costes de una flota de vehículos es un aspecto clave de su gestión, por lo tanto hay que realizar un control y seguimiento de los mismos con los siguientes objetivos:

- Establecer y controlar el presupuesto de la flota
- Establecer las tarifas y precios del servicio que prestamos
- Conocer cuales son las desviaciones respecto a los costes planificados
- Conocer cuanto cuesta el Km. recorrido
- Conocer el coste hundido por Km. y día
- Conocer cuanto cuesta el coste de un servicio/recorrido
- Conocer el coste de propiedad del vehículo TCO (*Total Cost of Ownership*)
- Establecer el periodo de retirada/renovación de los vehículos
- Realizar el control y seguimiento económico de la flota
- Calcular los principales indicadores económicos-financieros de la flota
- Realizar un análisis ABC de los costes de la flota
- Establecer el cuadro de mando de los costes de la flota
- Establecer un histórico de costes para hacer previsiones
- Obtener información valiosa para la toma de decisiones
- Identificar patrones de comportamiento de los costes de la flota

Para conseguir estos objetivos, la organización tiene que establecer el sistema de información apropiado para recopilar y analizar la información de los costes de la flota.

La principal causa por la que una organización no realiza el control y seguimiento de los costes de la flota, es por que no tiene establecido un sistema de información apropiado y no dedica los recursos materiales y humanos necesarios adecuados.

El mayor valor añadido del control y seguimiento de los costes de la flota es el análisis de los datos con el objetivo de obtener información valiosa para la toma de decisiones.

La finalidad del presente documento es explicar como una organización puede desarrollar los objetivos anteriormente comentados. Primeramente se explica cuáles son los costes de una flota de vehículos, su evolución en el tiempo y qué información se puede obtener.

Se realiza un caso práctico de cómo calcular el coste por Km., el coste por la prestación de un servicio, el cálculo del TCO, que partidas componen el presupuesto de una flota, y cómo establecer el periodo de renovación de los vehículos.

A continuación se desarrolla un modelo para realizar el control y seguimiento de los costes variables de operación de una flota para conocer si las desviaciones de los costes son debido a los costes unitarios o a la distancia recorrida.

Por último, para realizar un apropiado control y seguimiento de los costes de una flota de vehículos de una manera sencilla y rápida se desarrolla un cuadro de mando genérico de costes.

## 2. COSTES DE LA FLOTA DE VEHÍCULOS

---

Los costes de una flota de vehículos se clasifican en dos categorías:

- Costes directos: son los costes en los que incurre un vehículo por su posesión y utilización, y se dividen en dos subcategorías como:
  - Costes fijos: son los costes en los que se incurren por la posesión del vehículo, independientemente si el vehículo se utiliza o no, y se computan por unidad de tiempo, normalmente un año natural.
  - Costes variables de operación: son los costes en los que se incurren por la utilización del vehículo, y se computan por los kilómetros recorridos u horas de utilización.
  - Costes indirectos: son los costes en los que se incurren independientemente de la posesión o utilización del vehículo, en la gestión de la flota, y se computan por unidad de tiempo, normalmente un año natural.

El gráfico 1 muestra la estructura de costes de una flota de vehículos.

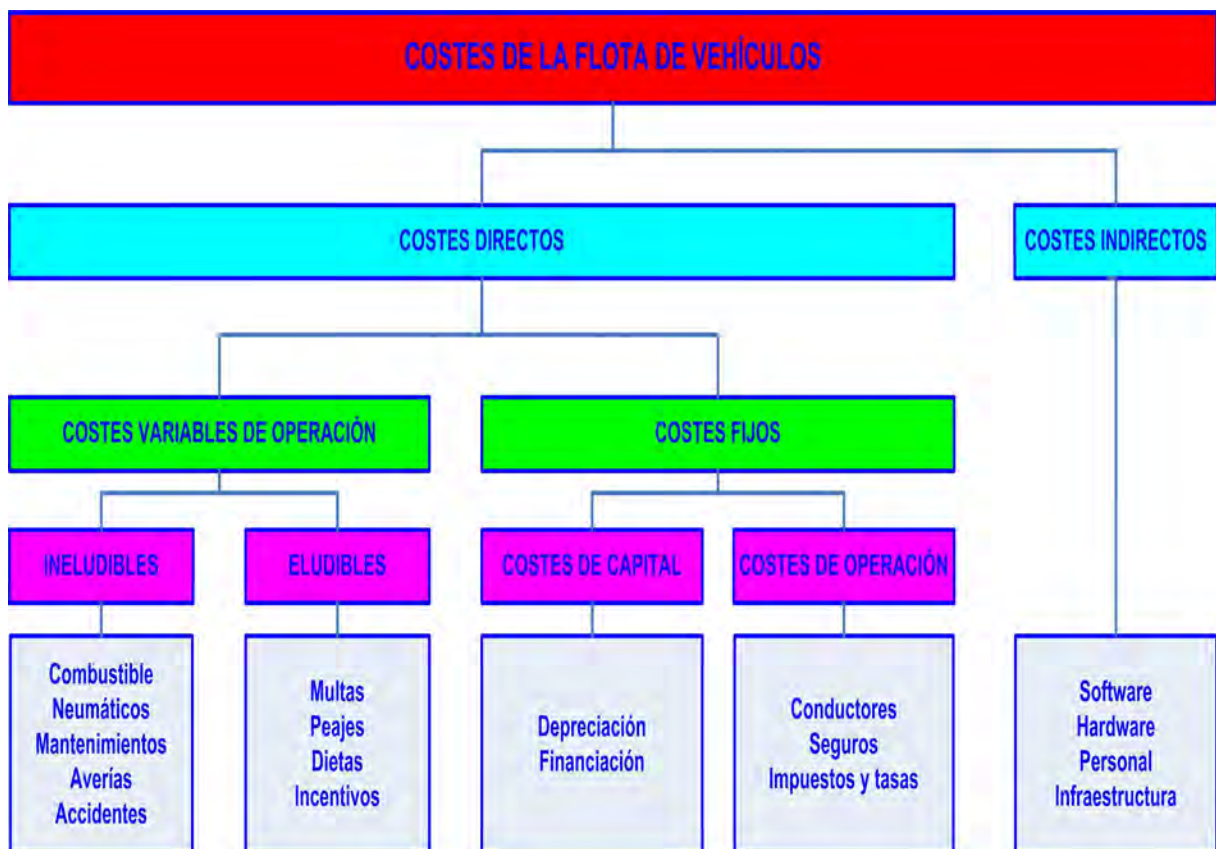


Gráfico 1: estructura de costes de una flota de vehículos

## 2.1. COSTES FIJOS

---

Los costes fijos de la flota de vehículos son aquellos en los que se incurren por la posesión del vehículo y se dividen en costes de capital y costes de operación.

### 2.1.1. Costes de capital

Los costes de capital son los costes de adquisición y forma de financiación del vehículo, y se dividen en la depreciación y financiación.

- Depreciación: es el decremento en el valor de adquisición del vehículo, equipos auxiliares o carrozados a lo largo de su periodo de utilización.

La depreciación del vehículo depende de las siguientes variables:

- El kilometraje del vehículo: cuanto mayor es el kilometraje, mayor es la depreciación.
  - La edad del vehículo: cuanto menor es la edad del vehículo, mayor es la depreciación, los vehículos nuevos se deprecian más rápido que los de más edad.
  - El estado del vehículo: si el vehículo tiene desperfectos en la carrocería, averías no arregladas, etc. la depreciación es mayor.
  - La demanda del vehículo en el mercado de segunda mano: si el vehículo tiene una gran demanda en el mercado de segunda mano, la depreciación es menor.
- Financiación: es la suma de los costes de financiación del vehículo, equipos auxiliares o carrozados en un año. La financiación del vehículo se puede realizar principalmente en las siguientes modalidades: si el vehículo es adquirido mediante un crédito o préstamo será la cuota anual de los intereses del mismo; si la organización ha emitido su propia deuda es la suma de los intereses anuales que se pagan a los compradores de la misma; o si la organización utiliza sus propios fondos propios es el coste de oportunidad de invertir los recursos en otra inversión y/o su propia prima de riesgo.

La depreciación y los costes de financiación son siempre decrecientes, al principio de la vida del vehículo la pérdida de valor es mayor y a lo largo del tiempo que se suele computar por años, va disminuyendo como muestra el gráfico 2.

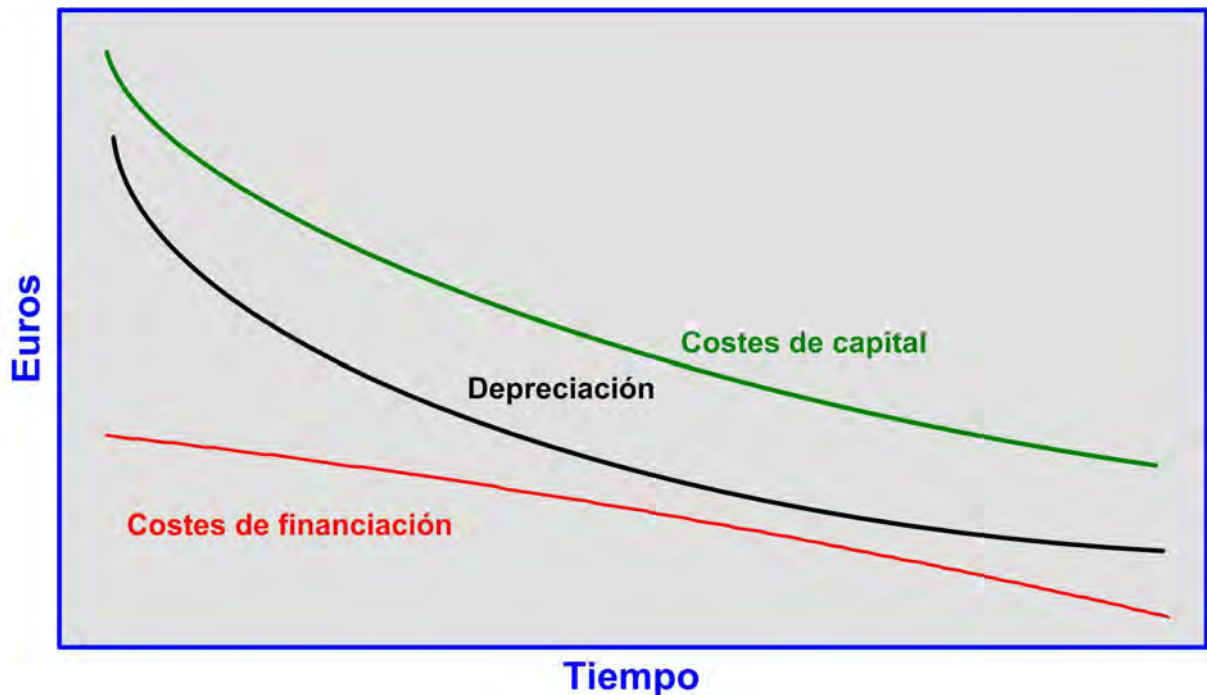


Gráfico 2: evolución de los costes de capital en el tiempo

Si el vehículo, equipos auxiliares o carrozados es adquirido mediante la modalidad de *renting/leasing* el coste de adquisición y financiación esta incluido en la cuota anual.

Hay que tener en cuenta dos siguientes aspectos si el vehículo es adquirido en la modalidad de *renting/leasing*: si el contrato se realiza por los kilómetros recorridos del vehículo, la adquisición del vehículo es un coste variable de operación, pero si el contrato es independiente del número de kilómetros recorridos del vehículo es un coste de capital fijo.

### 2.1.2. Costes de operación

Los costes de operación son los siguientes:

- Conductores de los vehículos: es el coste anual en bruto para la organización de los conductores de los vehículos destinados a la prestación del servicio, en España se incluye el salario en bruto más las aportaciones a la seguridad social.
- Seguros: es el coste anual de los seguros del vehículo, equipos auxiliares, carrozados, conductor o mercancía.
- Impuestos y tasas: es el coste anual de impuestos y tasas como la inspección técnica de vehículos (ITV), tarjeta de transporte, el impuesto de vehículos de



tracción mecánica, revisión del tacógrafo, impuestos especiales sobre determinados medios de transporte o autorizaciones.

Los costes de operación se pueden considerar prácticamente constantes, y que se incrementan con el índice del precio al consumo (IPC) en el tiempo, el gráfico 3 muestra su representación en el tiempo.



Gráfico 3: evolución de los costes de operación

### 2.1.3. Evolución de los costes fijos

Se describe como evolucionan los costes fijos en el tiempo, que es la suma de los costes de capital y los costes de operación descritos en los epígrafes 2.1.1 y 2.1.2.

Primeramente se describen unos conceptos básicos sobre como evolucionan las curvas de costes con un ejemplo práctico. Tenemos dos curvas de costes A y B como las mostradas en el gráfico 4 totalmente simétricas, la suma de ambas nos da como resultado la curva de costes totales C.

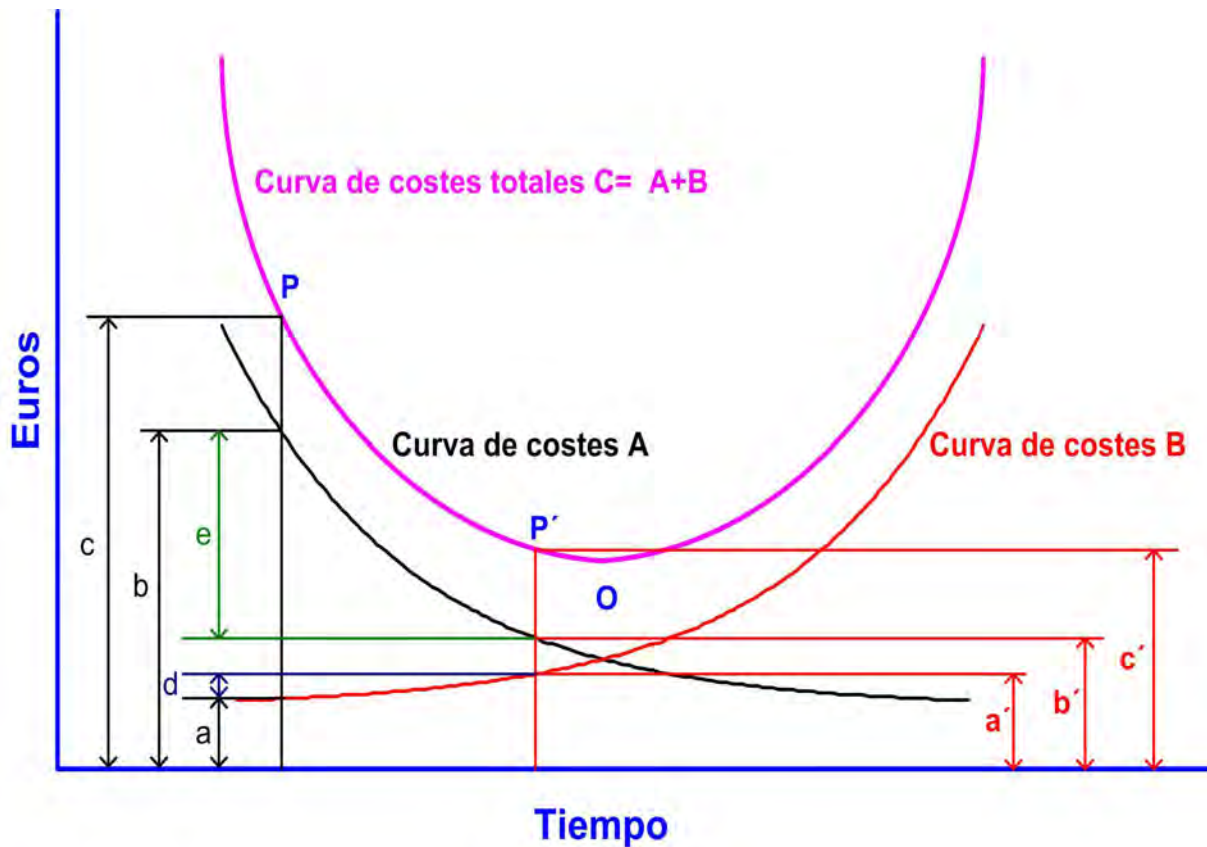


Gráfico 4: evolución de dos curvas de costes

Si tomamos dos puntos de la curva de costes totales  $P$  y  $P'$ , para que  $P > P'$  se tiene que cumplir la condición siguiente:

$$c > c'; a+b > a'+b'; b-b' > a'-a; e > d$$

Por lo tanto tenemos las tres siguientes situaciones posibles:

- El decremento de la curva de costes A es mayor que el incremento de la curva de costes B, por lo que la curva de costes totales C es decreciente.
- El decremento de la curva de costes A es igual al incremento de la curva B, se produce el punto de inflexión O y la curva de costes totales obtiene su mínimo.
- El decremento de la curva de costes A es menor al incremento de costes de la curva de costes B, la curva de costes totales C es creciente.

Al ser las curvas de costes A y B simétricas, el punto de inflexión O se obtiene donde se cortan, pero en la realidad las curvas de costes no son simétricas y el punto de inflexión no se obtiene donde se cortan las curvas de costes A y B.

Para que se produzca el punto de inflexión O tiene que haber un decremento en una curva de costes y un incremento en la otra curva de costes, aplicando estos conceptos a la gestión de flotas obtenemos los siguientes gráficos.

El gráfico 5 representa la evolución de los costes fijos en los siguientes tres casos en que los costes de operación; son mayores que los costes de capital (C), cortan a la curva de costes de capital (A) o es menor que la curva de costes de capital (B), considerando que los precios permanecen constantes a lo largo del tiempo.

La curva de costes fijos estará más arriba o abajo dependiendo de la suma de los costes de capital y de operación.

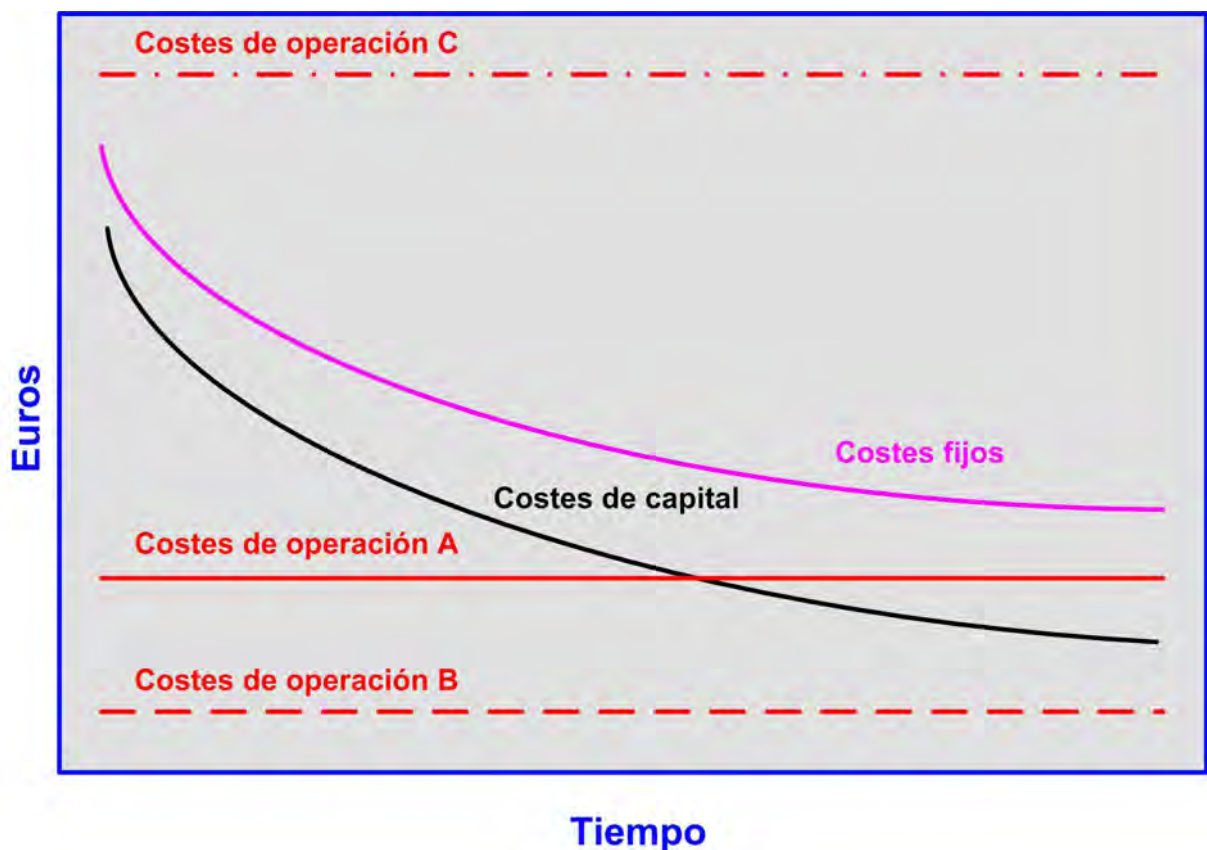


Gráfico 5: evolución de los costes fijos sin variación de precios

En todos los casos se obtiene una curva decreciente con mayor o menor pendiente dependiendo de como es la curva de costes operativos, pero nunca se puede obtener un punto de inflexión O por que no hay incrementos en los costes de operación.

En la realidad los precios varían a lo largo del tiempo, y la evolución de los costes fijos puede ser principalmente de las tres siguientes formas diferentes:

1. Los costes fijos son siempre decrecientes, debido a que los incrementos en los costes de operación nunca son mayores que los decrementos en los costes de capital. Este tipo de curva es la que se obtiene en flotas en los que la depreciación de los vehículos es alta y el vehículo esta asignado a un solo conductor, como es el transporte de mercancías. El gráfico 6 muestra este tipo de curva.

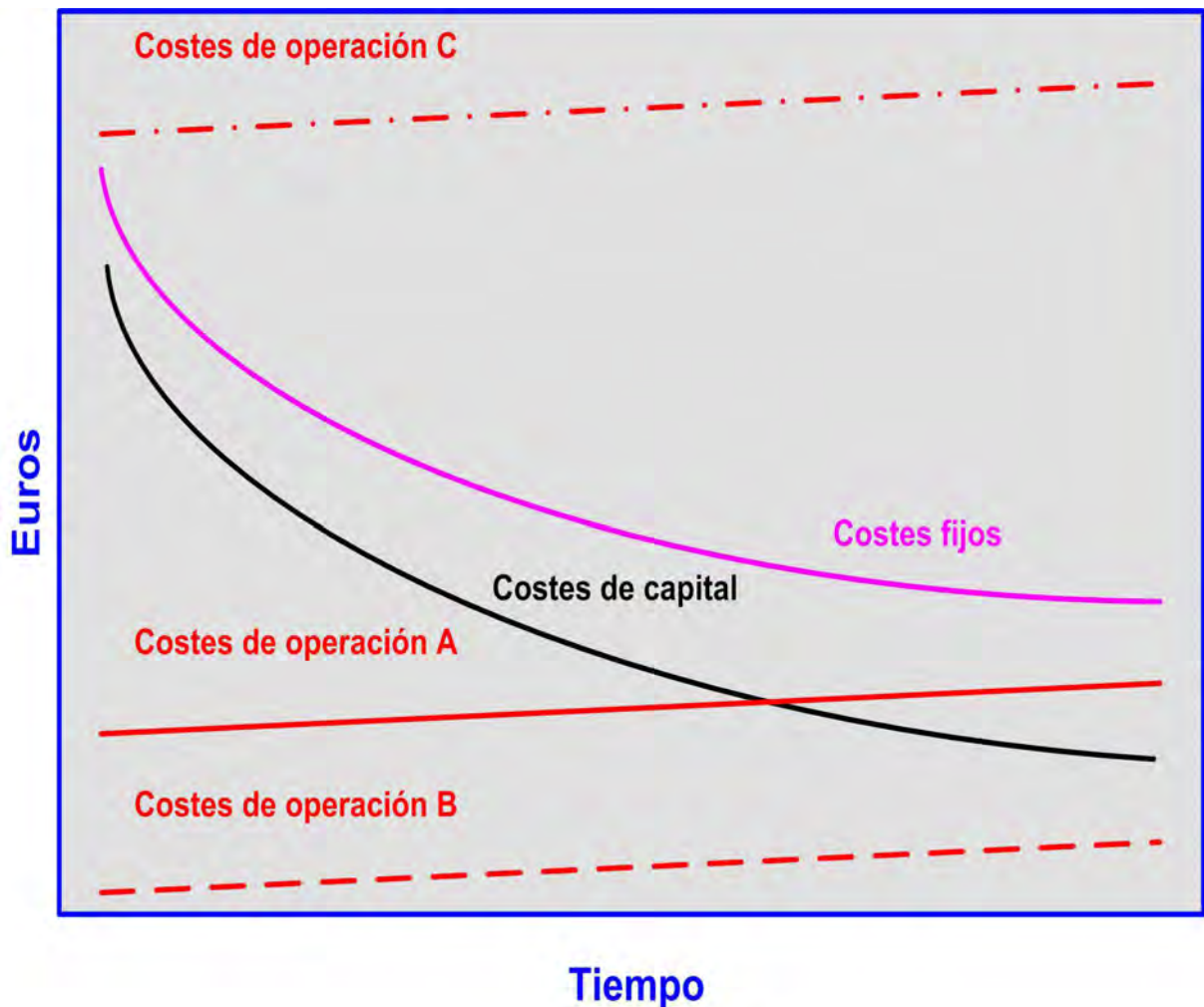


Gráfico 6: evolución de los costes fijos decreciente

2. Los costes fijos son siempre crecientes, debido a que los incrementos en los costes de operación son siempre mayores que los decrementos en los costes de capital. Este tipo de curva es la que se obtiene en flotas en los que la depreciación de los vehículos es baja, y el vehículo está asignado a varios conductores. Este tipo de curva es característica de flotas que trabajan los siete días de la semana, 3 turnos al día, y dos tipos de servicios como puede ser de lunes a viernes y fines de semana-festivos, con lo que el vehículo tendría asignado a 6 conductores. Este tipo de flota son las de limpieza viaria y recogida de basuras en ciertos vehículos (turismos, furgonetas, compactadores) o servicio de taxi.

Este tipo de curva también se puede obtener si la inflación a lo largo del tiempo es alta, aunque la depreciación de los vehículos sea baja. El gráfico 7 muestra este tipo de curva.

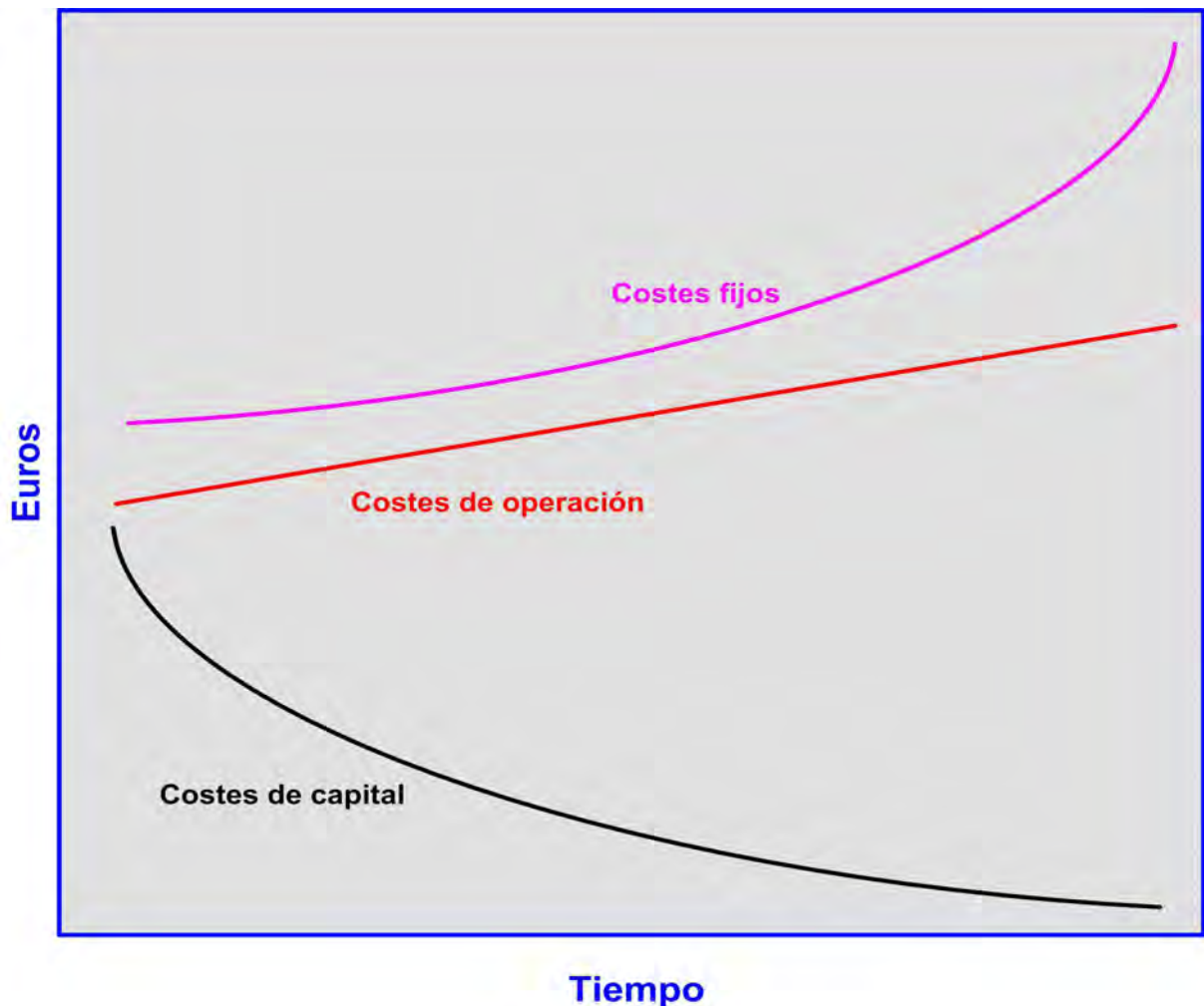


Gráfico 7: evolución de los costes fijos creciente

3. Los costes fijos son decrecientes al principio, pero tienen un punto de inflexión en el tiempo que la convierte en creciente, esto es debido a que al principio los incrementos en los costes de operación son menores que los decrementos en los costes de capital, pero a partir del punto de inflexión los incrementos en los costes de operación son mayores que los decrementos en los costes de capital.

Esta es una situación intermedia de los dos casos explicados anteriormente, y dependerá de la depreciación del vehículo, cuántos conductores tiene asignado el vehículo, la inflación a lo largo del tiempo o los tipos de interés. El gráfico 8 muestra este tipo de curva.

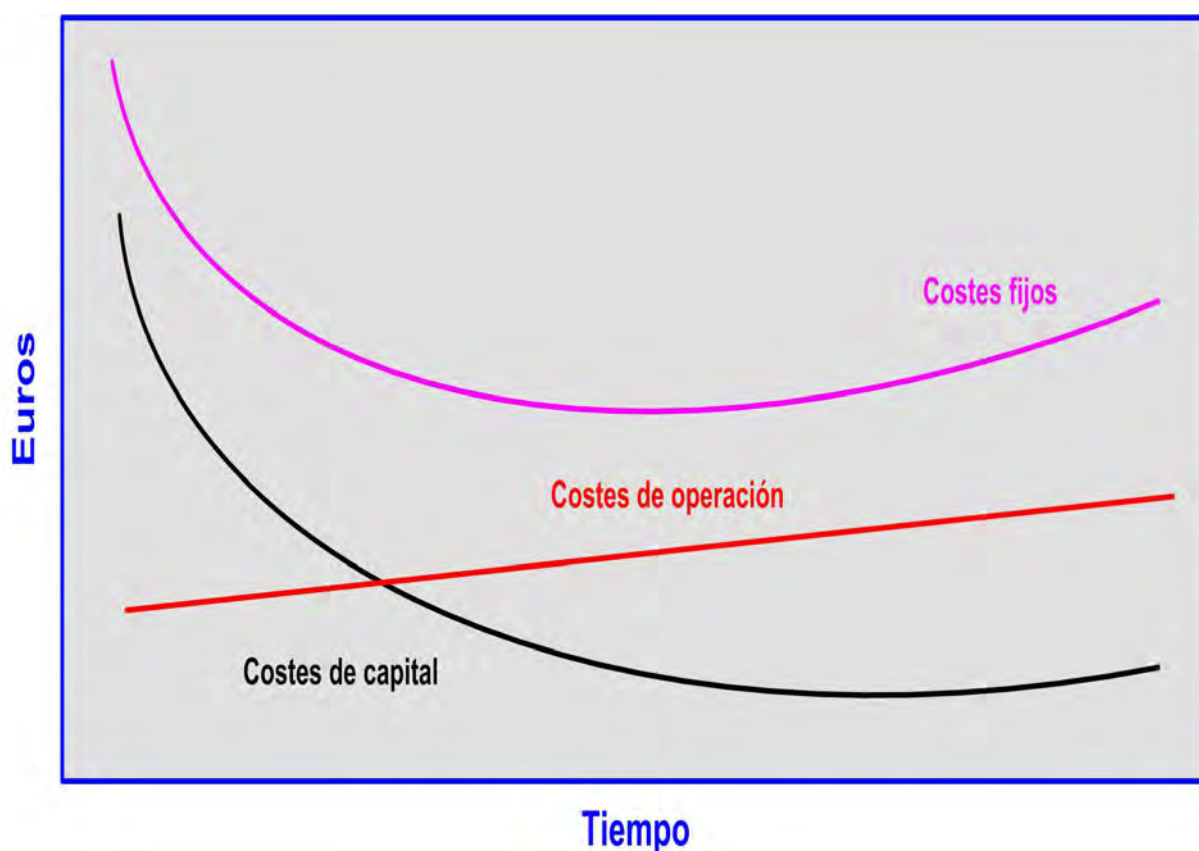


Gráfico 8: evolución de los costes fijos con punto de inflexión

De los tres casos descritos anteriormente, el más habitual en las flotas de vehículos es el primero (gráfico 6) en el que los costes fijos son decrecientes, aunque también se puede obtener los dos restantes (gráficos 7 y 8) dependiendo de las características de la flota explicados anteriormente.

## 2.2. COSTES VARIABLES DE OPERACIÓN

---

Los costes variables de operación de la flota son aquellos en los que se incurren por la utilización de los vehículos. Hay que diferenciar entre dos categorías de costes directos variables, aquellos en los que se incurren obligatoriamente por la utilización de los vehículos, y aquellos en los que se puede incurrir o no por la utilización de los vehículos, y que dependen de la operativa del servicio y de cómo la flota es gestionada.

### 2.2.1. Costes ineludibles

Los costes ineludibles de la flota de vehículos son aquellos en los que se incurre por la utilización de los vehículos, y son los siguientes:

- Combustible: es el coste anual del combustible de los vehículos y equipos auxiliares.
- Neumáticos: es el coste anual de la adquisición y reparación de los neumáticos.
- Mantenimiento: es el coste anual de los mantenimientos planificados según el fabricante del vehículo y de los mantenimientos preventivos, y han de incluir la mano de hora, los repuestos y lubricantes.
- Averías: es el coste anual de las averías, y han de incluir la mano de hora, los repuestos y lubricantes.
- Accidentes: es el coste anual de los accidentes de tráfico, y han de incluir los costes de reparación del vehículo, así como el pago de las indemnizaciones a terceros que la organización incurra.

Los costes ineludibles son siempre crecientes a lo largo del tiempo, y además existe una edad del vehículo o kilometraje en el cual se incrementan considerablemente. El gráfico 9 muestra la evolución de los costes variables de operación ineludibles en el tiempo.





Gráfico 9: evolución de los costes variables de operación ineludibles.

### 2.2.2. Costes eludibles

Los costes eludibles de la flota de vehículos son aquellos en los que se puede incurrir o no en la utilización de los vehículos, y dependen de la operativa del servicio y de cómo la flota es gestionada, y son los siguientes:

- Multas y sanciones: son el coste de las infracciones como las multas de tráfico que cometen los conductores, la carencia de la tarjeta de transporte, la manipulación del tacógrafo, no cumplir los tiempos de conducción y descanso o el exceso de peso.
- Peajes: es el coste anual correspondiente al pago de peajes, se deberá utilizar las autovías del peaje si es necesario para cumplir el nivel de servicio y/o por ser más seguras y reducir los accidentes de tráfico.
- Dietas del conductor: es el coste anual de los conductores de los vehículos por el desplazamiento fuera de su lugar de residencia por un periodo determinado de tiempo.
- Incentivos: son los incentivos que se pagan a los conductores de los vehículos por diversos motivos, como la reducción del consumo de combustible o el reporte de los accidentes de tráfico.

Los costes variables de operación eludibles pueden adoptar cualquier evolución, creciente, decrecientes, con varios puntos de inflexión etc. debido a que dependen de cómo la flota es gestionada, si se utilizan peajes o no etc.



### 2.2.3. Evolución de los costes variables de operación

Debido a que los costes variables de operación ineludibles son de mucha mayor cuantía que los costes variables de operación eludibles, la evolución de los costes variables de operación es siempre creciente, como muestra el gráfico 10:



Gráfico 10: evolución de los costes variables de operación.

En cada clasificación de estos costes hay que incluir en cada categoría el concepto “Otros”, ya que por ejemplo hay compañías que realizan un mantenimiento obligatorio al vehículo al año, lo utilicen o no, por lo que es un coste fijo.

## 2.3. COSTES INDIRECTOS

---

Los costes indirectos son los siguientes:

- *Software* de gestión de la flota: hay diversos tipos de *software* que son utilizados para gestionar la flota o el servicio que prestamos, los principales son:
  - Servicios telemáticos: ofrecen multitud de funcionalidades, como posicionamiento GPS (*global positioning system*), consumo de combustible, forma de conducir de los conductores, eco conducción, robo de combustible, descarga remota del tacógrafo, usos indebidos de los vehículos etc.
  - Optimización de rutas: en este tipo de *software*, tenemos unos puntos de recogida o entrega principalmente de mercancías o pasajeros, y unos vehículos con unas capacidades, el resultado son las rutas a realizar, que vehículos utilizar, el tiempo del servicio etc.
  - *Advanced driver-assistance systems* (ADAS): en los últimos años han aparecido diferentes sistemas para la ayuda a la conducción, algunos de estos sistemas son gestionados con su *software* correspondiente.
  - *Transportation management system* (TMS): es un sistema de información que gestiona las operaciones de transporte de mercancía, y es muy utilizado por los gestores de tráfico.
- *Hardware*: actualmente la mayoría de los *software* que se utilizan en la gestión de la flotas anteriormente comentados son soluciones SaaS (*Software as a Service*) en los que se utilizan directamente desde un navegador entrando en una plataforma en *Internet*, aunque puede haber algunos *software* que necesitemos tener nuestro propio servidor en nuestras instalaciones. Además el *hardware* son los dispositivos que necesitamos para prestar el servicio como *tablets*, ordenadores, *smartphones* o dispositivos *aftermarket* que incorporemos a los vehículos como por ejemplo los dispositivos de ayuda a la conducción (ADAS).
- Personal: son los trabajadores que necesitamos para gestionar la flota como: el gestor de flota, el personal de taller, las personas encargadas de gestionar las multas o los accidentes de tráfico, adquirir los vehículos, vender los vehículos etc.

- Infraestructura: son las instalaciones necesarias para operar la flota como: el taller si lo tenemos propio, el inmueble para aparcar los vehículos cuando no se utilicen, los depósitos de combustible si lo tenemos propio, las oficinas que utilizan los trabajadores que gestionan la flota etc.

### 2.3.1. Evolución de los costes indirectos

Los costes indirectos se pueden considerar prácticamente constantes y que se incrementan con el IPC a lo largo del tiempo, y se representan en el gráfico 11

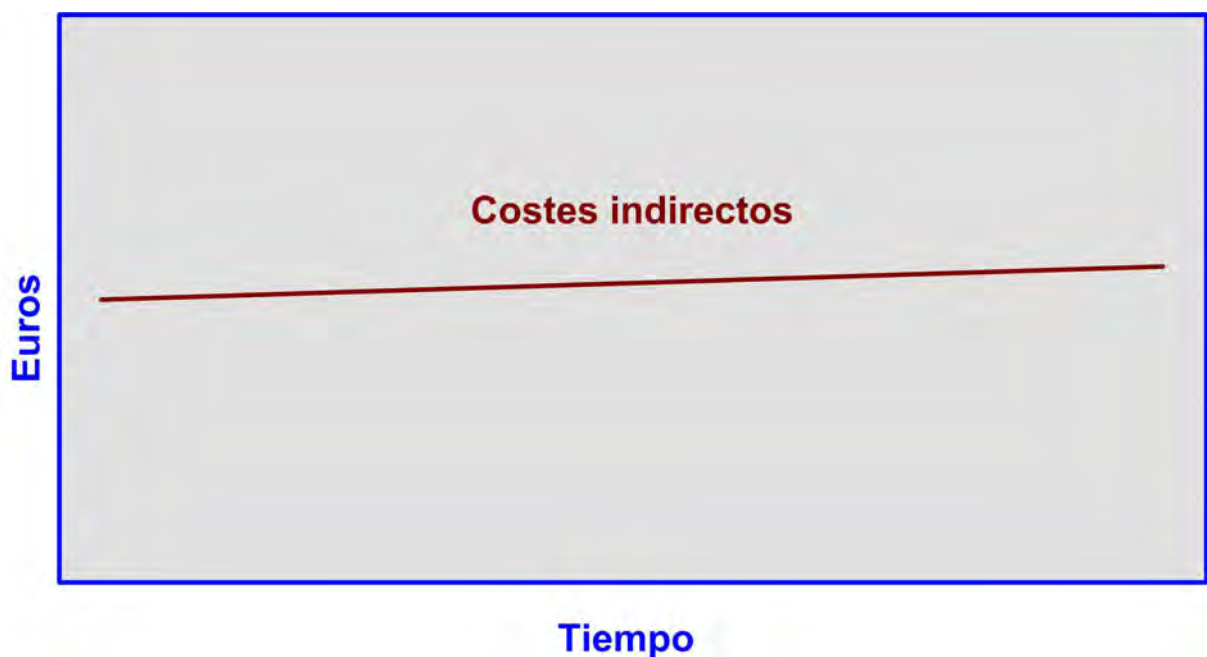


Gráfico 11: evolución de los costes indirectos.

A mayor tamaño de flota, se necesita más personal, controles, procesos, espacio para almacenar los vehículos, infraestructura etc. para gestionar la flota. Dependiendo de las características de la flota, la evolución de los costes indirectos con el número de vehículos de la flota puede ser:

- Exponencial: cuanto mayor tamaño de flota, la evolución de los costes indirectos es una curva exponencial como muestra el gráfico 12.

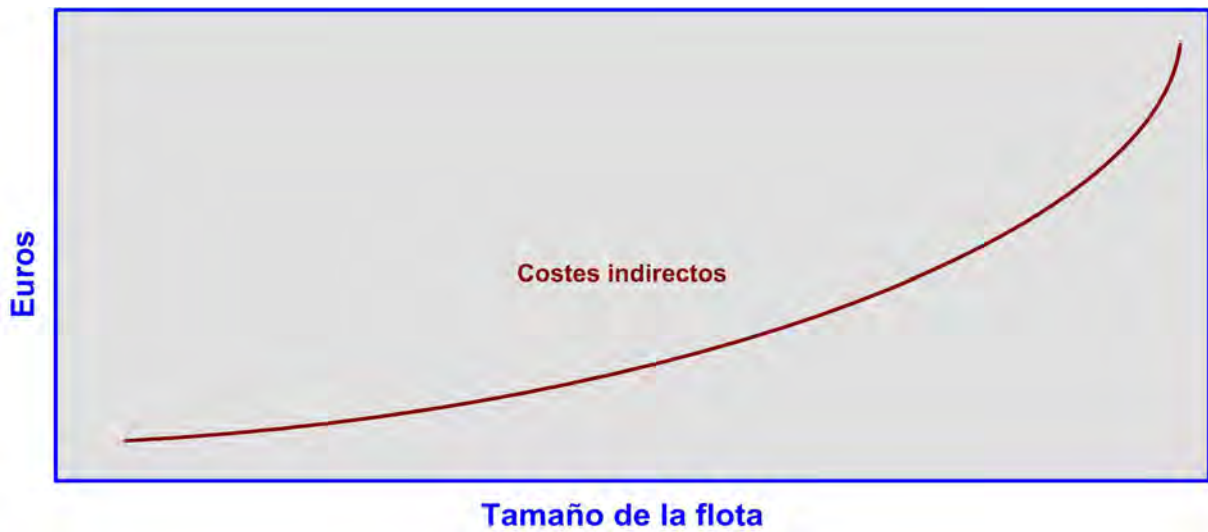


Gráfico 12: evolución exponencial de los costes indirectos con el tamaño de la flota.

- Escalonada: cuanto mayor tamaño de flota, la evolución de los costes indirectos es de forma escalonada como muestra el gráfico 13.



Gráfico 13: evolución escalonada de los costes indirectos con el tamaño de la flota.

El gráfico 13 muestra que existen dos tipos de evolución en cada tramo que puede ser que los costes indirectos permanezcan constantes (línea continua) o que se incrementen (línea discontinua).

## 2.4. EVOLUCIÓN DE LOS COSTES TOTALES

Se describe como evoluciona los costes totales de una flota de vehículos en el tiempo, que nos suministra la información sobre la estructura de los mismos, para ello utilizaremos la curva de costes indirectos del gráfico 10, por que es la más habitual en las flotas de vehículos.

Existen principalmente tres patrones de comportamiento de la evolución de los costes totales a lo largo del tiempo y son las siguientes: decreciente, forma de bañera y creciente, y se obtienen dependiendo si los costes fijos son decrecientes, con un punto de inflexión, o crecientes, tal como se han explicado en el epígrafe 2.1.3, a continuación se desarrollan.

- Considerando los costes fijos decrecientes tal como muestra el gráfico 6, la evolución de los costes totales de una flota de vehículos tiene dos patrones de comportamiento como son:

1. La curva de costes totales es decreciente, por que la suma de los incrementos en los costes variables de operación e indirectos son siempre menores que los decrementos de los costes fijos, como muestra el gráfico 14.

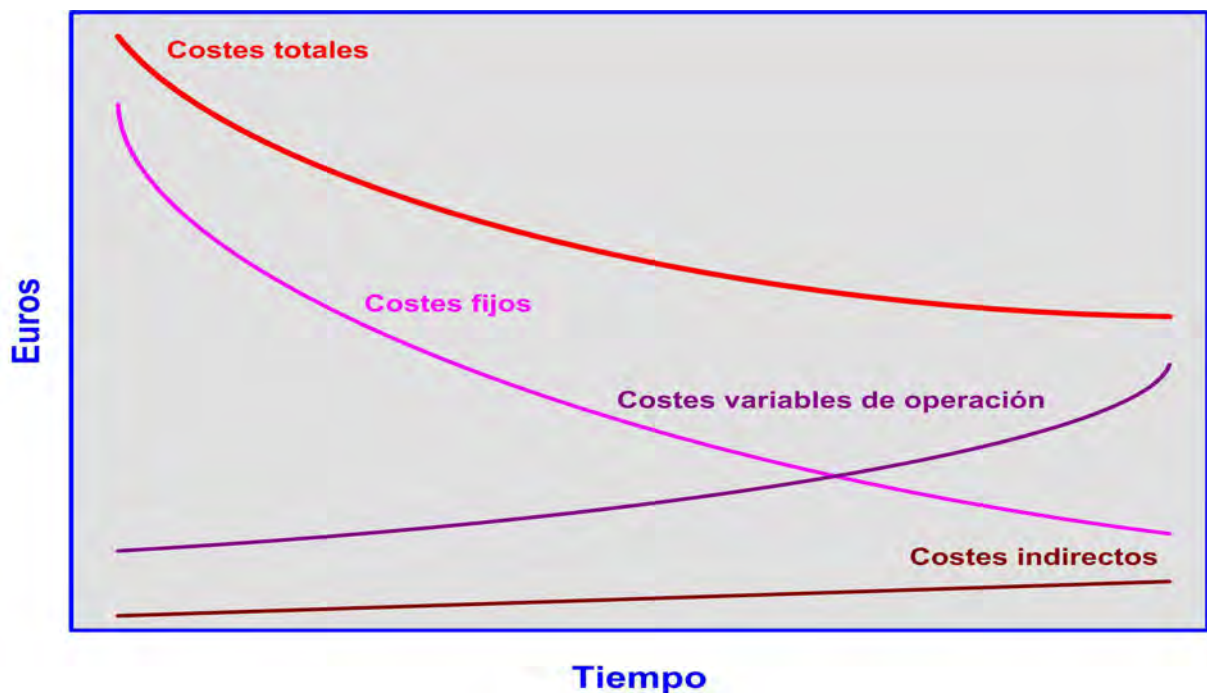


Gráfico 14: costes totales decrecientes

Este es el caso ideal para cualquier tipo de flota, por que los costes totales son siempre decrecientes, y podría ser el caso de una flota de vehículos eléctricos, en el que los costes de adquisición de los vehículos son altos y los costes variables de operación bajos.

2. La curva de costes totales tiene forma de bañera, al principio es decreciente y tiene un punto de inflexión, en la que es creciente debido a que la suma de los incrementos de los costes variables de operación y costes indirectos son mayores que los decrementos en los costes totales, como muestra el gráfico 15.

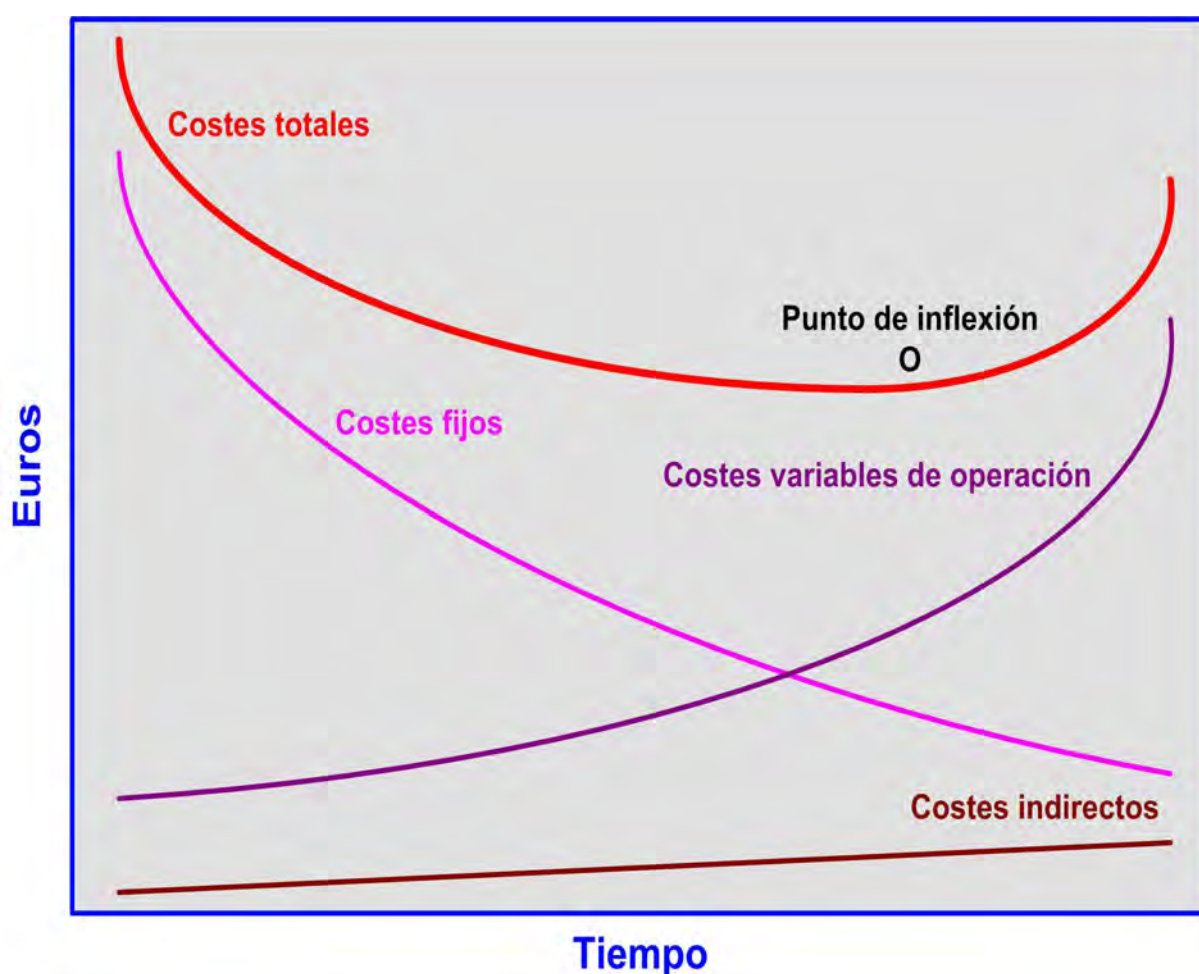


Gráfico 15: costes totales con un punto de inflexión O.

Esta evolución de los costes fijos es la más habitual en las flotas de vehículos., lo más importante es conocer cuando se produce el punto de inflexión O, ya que se pasa de costes totales decrecientes a crecientes.

- Considerando que los costes fijos tienen un punto de inflexión como muestra el gráfico 8, la curva de costes totales tiene forma de bañera, como muestra el gráfico 16.

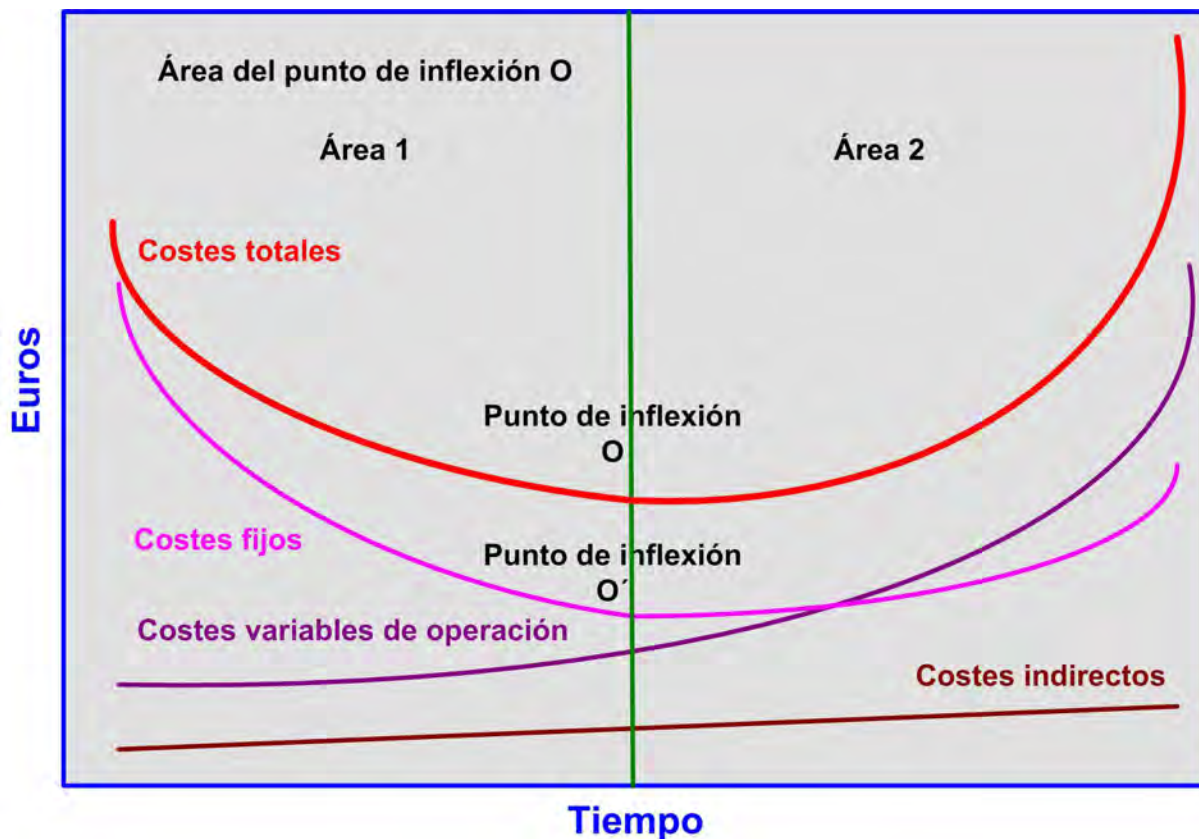


Gráfico 16: evolución de los costes totales teniendo los costes fijos un punto de inflexión

Los costes fijos tienen un punto de inflexión O', esto provoca que los costes totales sean decrecientes al principio y a partir del punto de inflexión O' sean crecientes ya que todas las curvas de costes son crecientes,

El punto de inflexión de los costes totales O siempre está localizado en el área 1, a la izquierda o en la vertical del punto de inflexión O', obteniéndose dos casos:

1. El punto de inflexión O está en la vertical del punto de inflexión O' cuando el decremento de los costes fijos es mayor que la suma de los incrementos de los costes variables de operación y los costes fijos en todo el área 1, hasta el punto de inflexión O' tal como muestra el gráfico 16.



2. El punto de inflexión O está a la izquierda de la vertical del punto de inflexión O', cuando el decremento de los costes fijos es igual que la suma de los incrementos en los costes variables de operación y los costes fijos en algún lugar del área 1, tal como muestra el gráfico 17.

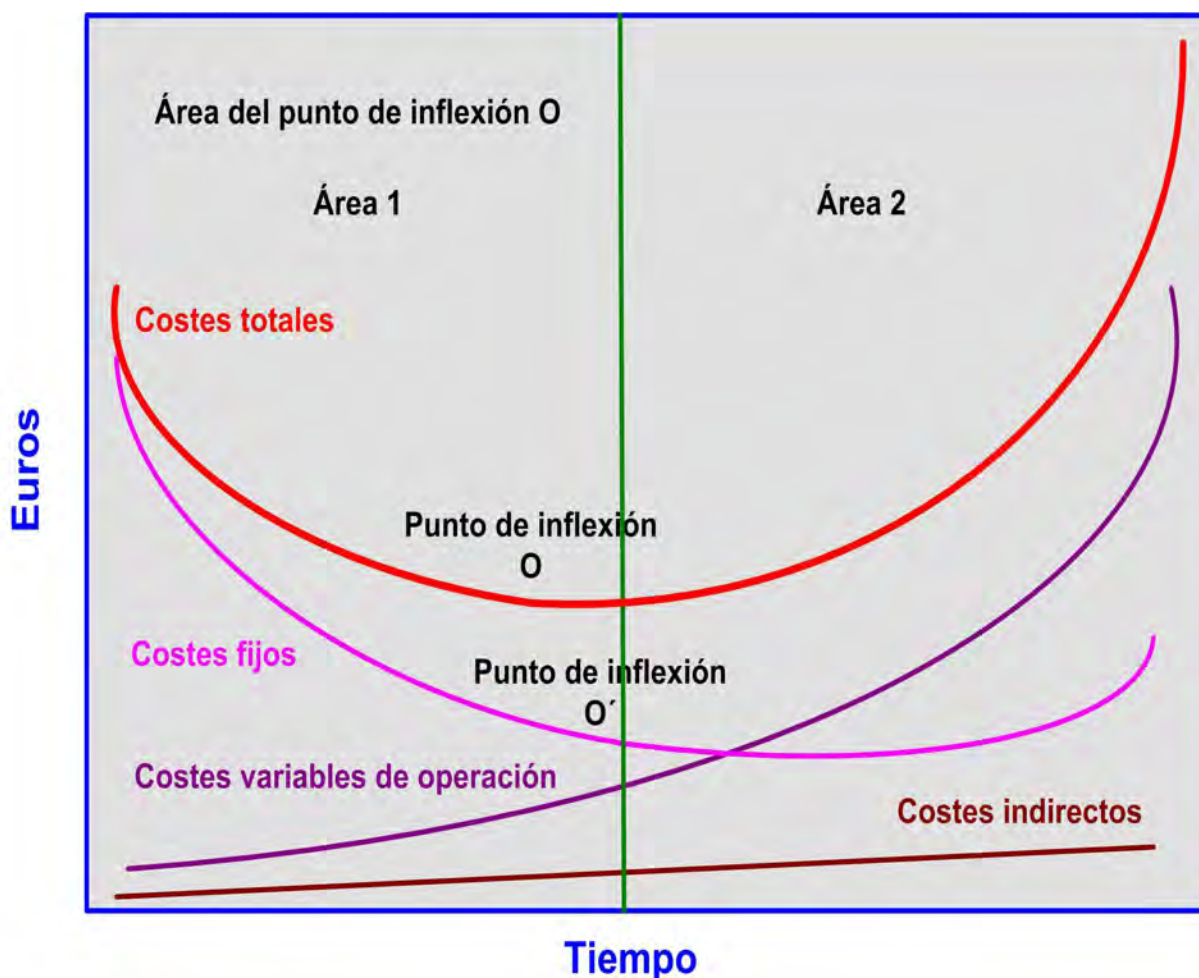


Gráfico 17: evolución de los costes totales, teniendo los costes fijos un punto de inflexión.

Debido a que a partir del punto de inflexión O, los costes fijos, los variables de operación y los indirectos son crecientes, en el área 2 los incrementos en los costes totales son mucho mayores que los decrementos que se producen en el área 1, por lo que se pasa de costes totales decrecientes a costes totales crecientes que tienen grandes incrementos en el tiempo.

- Considerando la curva de costes fijos creciente como muestra el gráfico 7, la evolución de los costes totales es creciente como muestra el gráfico 18:



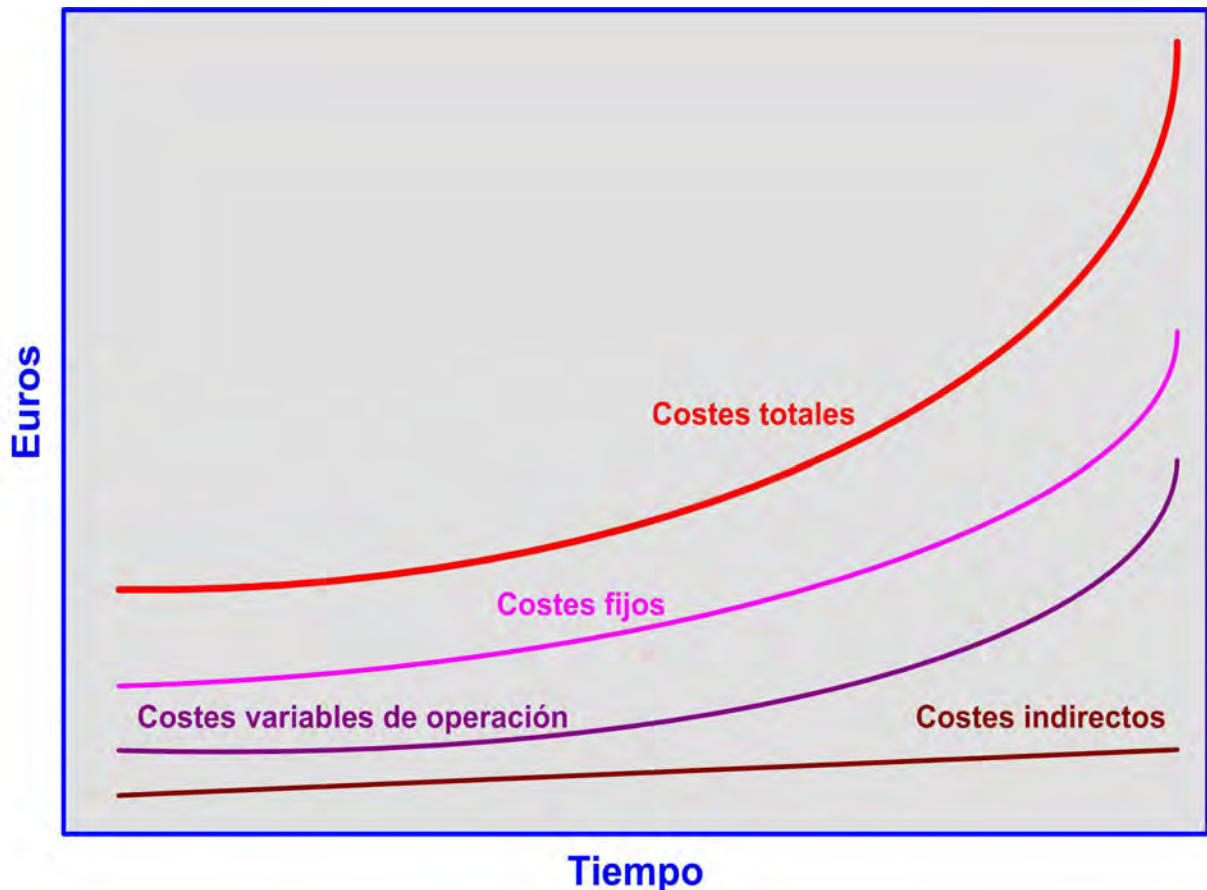


Gráfico 18: evolución de los costes totales teniendo los costes fijos crecientes.

Como los costes variables de operación, fijos e indirectos son crecientes, la curva de costes totales es creciente, y los incrementos que se producen a lo largo del tiempo son cada vez mayores.

Como los costes variables de operación e indirectos son siempre crecientes, la evolución de los costes totales de la flota depende de los costes fijos, cuyas mayores cuantías son la depreciación y los salarios de los conductores.

Si adquirimos el vehículo en propiedad, la depreciación es un coste fijo, si adquirimos el vehículo en *renting* en función de los kilómetros que realice el vehículo es un coste variable de operación, por lo tanto una de las decisiones más importantes en la gestión de la flota de vehículos, es como se adquieren los vehículos. Existen varias opciones como: adquirirlos en propiedad; en la modalidad de *renting/leasing*; a través de un crédito automoción destinado a la adquisición de vehículos de flotas; o utilizando el *car sharing*, cual elegir depende de los siguientes factores:

- La estrategia de la organización

Si la gestión de la flota de vehículos es la actividad principal de nuestra organización (transporte por carretera de personas y mercancías, actividades postales y de correo, etc.), la mejor solución es la adquisición en propiedad, ya que tendremos el control absoluto de los vehículos para desarrollar la estrategia de nuestra organización.

Podemos realizar todas las modificaciones que requieran los vehículos, repararlos en nuestros propios talleres y no tener que esperar a que lo realice un tercero, utilizarlos y retirarlos del servicio cuando deseemos, además de que representan nuestra imagen de marca y pueden ser rotulados con la publicidad de nuestra organización.

Si la gestión de la flota de vehículos es una actividad secundaria de nuestra organización (utilización particular por los directivos o comerciales de nuestra organización), la mejor solución es adquirir los vehículos en la modalidad de *renting/leasing* o utilizar el *car sharing*.

Hay que tener en consideración que los contratos de *renting/leasing* suelen tener una duración mínima de 2 años, si no se cumple con la duración del contrato nuestra organización tiene que pagar una penalización a la compañía de *renting/leasing*, además pueden incluir otros servicios como mantenimiento, neumáticos etc. provocando que nuestra organización tenga mucha menos libertad para gestionar la flota y desarrollar la estrategia de nuestra organización.

- Las características del vehículo y el servicio a realizar

Los vehículos especializados o que necesitan un equipamiento o carrozados a medida para prestar un determinado servicio (transporte por carretera de mercancías, actividades postales y de correo, limpieza viaria, etc.), la mejor solución es la adquisición en propiedad, ya que podemos hacer todas las modificaciones que requieran, además tienen una gran dificultad para su venta por que tienen un mercado de segunda mano muy restringido, y los equipamientos especializados tienen un valor residual prácticamente nulo, provocando que la adquisición en *renting* sea incluso más costosa o no exista esta posibilidad.

Los vehículos que son especializados como los turismos y furgonetas, y que no requieran ninguna modificación (los directivos y/o comerciales de una compañía) la mejor solución es adquirirlos en la modalidad de *renting*.

- Consideraciones financieras y fiscales

La adquisición en propiedad requiere de una inversión inicial, por el contrario la modalidad *renting/leasing* requiere de menor capacidad financiera de nuestra organización y se considera como gasto en la cuenta de resultados.

Hay que establecer la posibilidad de adquirir vehículos de segunda mano, ya que los vehículos con edades bajas tienen prácticamente las mismas prestaciones y costes que un vehículo nuevo, pero son más económicos de adquirir, así mismo hay que establecer la edad máxima que deben tener estos vehículos para poder ser adquiridos.

- El mercado donde opera nuestra organización

Si nuestra organización opera en un mercado con una gran variabilidad en la demanda a corto-medio plazo, el número óptimo de vehículos que necesita nuestra organización variará en el tiempo considerablemente, y por lo tanto la mejor solución es adquirir los vehículos en propiedad ya que los podemos retirarlos del servicio y venderlos cuando queramos.

Si nuestra organización opera en un mercado estable sin variabilidad en la demanda a corto-medio plazo, el número óptimo de vehículos que necesita nuestra organización prácticamente no variará en el tiempo, la mejor solución es adquirir los vehículos en la modalidad de *renting* utilizar el *car sharing*.

En algunos concursos públicos de servicios municipales como contratos de limpieza viaria o recogida de basuras por los requerimientos y especificaciones del mismo, la flota de vehículos ha de ser adquirida en propiedad.

- Disponibilidad de los vehículos en el mercado del *renting*

Cuanto más especializado sea el vehículo menos oferta en el mercado de *renting* hay disponible, además puede ser más económico adquirirlo en propiedad que en *renting*.

Las empresas de *renting* son competitivas en vehículos *standard* como son los turismos y furgonetas, pero actualmente están ofreciendo sus servicios en más clases de vehículos y hay que realizar el cálculo del TCO para conocer si es mejor adquirir en propiedad o en *renting*.

- Subcontratación de parte de la flota.

Una solución intermedia es adquirir una parte de la flota de la organización en propiedad por debajo del número óptimo, y el resto de vehículos hasta el número óptimo se renta/subcontrata a un tercero, con lo que tendremos una gran flexibilidad para adaptarnos a la demanda, esta práctica es frecuentemente realizada por las empresas de reparto de mercancía y paquetería, por que existe una gran oferta de transporte de trabajadores autónomos con su propio vehículo.

La cuantía total de los salarios de los conductores viene establecido por cuantos conductores tiene asignado el servicio a prestar y de su salario, y depende:

- Tipo de servicio a prestar: en flotas de vehículos que prestan el servicio los 7 días de la semana, las 24 horas del día, el vehículo tiene asignado varios conductores, por el contrario si el servicio es prestado de lunes a viernes o los fines de semana en un solo turno el vehículo tendrá asignado un solo conductor.
- La demanda del servicio: dependiendo de la demanda del servicio, podemos tener un turno o más, prestar el servicio los 7 días de la semana y por lo tanto tener uno o más conductores asignados al vehículo.

Es muy importante conocer cuál es la estructura de costes y su evolución en el tiempo, por que nos suministra la siguiente información para la toma de decisiones:

- La cuantía de los costes totales de la flota, los variables de operación, los fijos e los indirectos.
- Realizar un control y seguimiento de los costes totales de la flota, los variables de operación, los fijos e los indirectos.
- Conocer si costes totales son crecientes o decrecientes.

- Conocer el punto de inflexión donde se pasa de tener costes decrecientes a crecientes.
- Conocer cuáles son los incrementos en los costes totales a lo largo del tiempo.
- Hacer previsiones de los costes totales de la flota, los variables de operación, los fijos e los indirectos.
- Conocer la cuantía de las reducciones en los costes que estamos obteniendo

La estructura de costes de una compañía y su evolución en el tiempo dependerá de los variables anteriormente descritas y puede ocurrir que compañías similares que operen en el mismo mercado, tengan diferente estructura de costes.

Podemos definir dos tipos de flotas que representan los dos extremos en cuanto a los costes de estructura y que son:

- Costes hundidos (fijos más indirectos) alto: es un tipo de flota con vehículos especializados, adquiridos en propiedad, trabaja 7 días de la semana, 24 horas del día, el vehículo tiene asignado varios conductores y tiene un taller propio donde reparar los vehículos. Este tipo de flota corresponde a flotas de limpieza viaria y recogida de basuras o minería.
- Costes hundidos (fijos más indirectos) bajos: es un tipo de flota con turismos o furgonetas que no necesitan ninguna modificación, la adquisición es en *renting*, tiene asignado solamente un conductor, y no tiene un taller propio donde reparar los vehículos. Este tipo de flota corresponde a comerciales o ejecutivos de compañías a los que se les suministra un vehículo como gratificación para su uso privado.

Estos dos casos son los más extremos y entre medias hay una gran diversidad de tipos de flotas y por lo tanto de sus costes de estructura.

## 2.5. CÁLCULO DE LOS COSTES DE LA FLOTA DE VEHÍCULOS

---

La organización tiene que establecer la frecuencia para realizar el control y seguimiento de los costes que dependerá de las características, presupuesto y objetivos de cada organización. El control y seguimiento de los costes se recomienda realizarlo por las siguientes categorías:

- Un genérico para toda la flota
- Por tipo de vehículo
- Por tipo de servicio

Además de realizar el control y seguimiento para el total de la flota, hay que realizarlo por tipo de vehículo y servicio para conocer donde se esta gestionando la flota de forma inapropiada y priorizar las medidas a tomar.

Dependiendo del tipo de flota se puede realizar el control y seguimiento de los costes en más categorías, por ejemplo en una empresa de autobuses, por rutas u horarios.

A continuación se muestra un ejemplo práctico de como realizar este control y seguimiento para un vehículo considerando los siguientes datos de operación de la tabla 1.

| Características de operación | Cantidad |
|------------------------------|----------|
| Km. recorridos al año        | 75.000   |
| Días trabajados al año       | 225      |
| Horas trabajadas al año      | 1.900    |

Tabla 1: datos de operación

La tabla 2 muestra todos los costes totales de un vehículo en un año según el gráfico 1.

| Denominación                                        | Costes    | % costes | Coste por Km. |
|-----------------------------------------------------|-----------|----------|---------------|
| <b>Costes directos</b>                              | 82.182,86 | 92,36%   | 1,096         |
| <b>Costes fijos (Tiempo)</b>                        | 38.929,30 | 43,75%   | 0,519         |
| <b>Costes de operación</b>                          | 32.585,71 | 36,62%   | 0,434         |
| Conductor                                           | 29.562,14 | 33,22%   | 0,394         |
| Seguros                                             | 2.400,12  | 2,70%    | 0,032         |
| Impuestos y tasas                                   | 623,45    | 0,70%    | 0,008         |
| <b>Costes de capital</b>                            | 6.343,59  | 7,13%    | 0,085         |
| Depreciación                                        | 5.321,14  | 5,98%    | 0,071         |
| Financiación                                        | 1.022,45  | 1,15%    | 0,014         |
| <b>Costes variables (Km.)</b>                       | 43.253,56 | 48,61%   | 0,577         |
| <b>Ineludibles</b>                                  | 35.897,51 | 40,34%   | 0,479         |
| Combustible                                         | 26.548,49 | 29,84%   | 0,354         |
| Neumáticos                                          | 2.645,14  | 2,97%    | 0,035         |
| Mantenimientos                                      | 1.902,78  | 2,14%    | 0,025         |
| Averías                                             | 1.500,65  | 1,69%    | 0,020         |
| Accidentes                                          | 3.300,45  | 3,71%    | 0,044         |
| <b>Eludibles</b>                                    | 7.356,05  | 8,27%    | 0,098         |
| Multas                                              | 425,26    | 0,48%    | 0,006         |
| Peajes                                              | 987,41    | 1,11%    | 0,013         |
| Dietas                                              | 4.253,6   | 4,78%    | 0,057         |
| Incentivos                                          | 1.689,78  | 1,90%    | 0,023         |
| <b>Costes Indirectos</b>                            | 6.800,25  | 7,64%    | 0,091         |
| <b>Total costes</b>                                 | 88.983,11 | 100%     | 1,186         |
| <b>Coste por Km.= Coste/ Km. recorridos al año.</b> |           |          |               |

Tabla 2: coste total de un vehículo de la flota

Hay que realizar un análisis ABC de los costes para conocer que partidas del gráfico 1 nos producen el 80% de los costes, y se representan según la tabla 3 y/o el gráfico 19:

| Denominación      | Costes           | % costes    | % acumulado |
|-------------------|------------------|-------------|-------------|
| Conductor         | 29.562,14        | 33,22%      | 33,22%      |
| Combustible       | 26.548,49        | 29,84%      | 63,06%      |
| Costes Indirectos | 6.800,25         | 7,64%       | 70,70%      |
| Depreciación      | 5.321,14         | 5,98%       | 76,68%      |
| Dietas            | 4.253,60         | 4,78%       | 81,46%      |
| Accidentes        | 3.300,45         | 3,71%       | 85,17%      |
| Neumáticos        | 2.645,14         | 2,97%       | 88,14%      |
| Seguros           | 2.400,12         | 2,70%       | 90,84%      |
| Mantenimientos    | 1.902,78         | 2,14%       | 92,98%      |
| Incentivos        | 1.689,78         | 1,90%       | 94,88%      |
| Averías           | 1.500,65         | 1,69%       | 96,56%      |
| Financiación      | 1.022,45         | 1,15%       | 97,71%      |
| Peajes            | 987,41           | 1,11%       | 98,82%      |
| Impuestos y tasas | 623,45           | 0,70%       | 99,52%      |
| Multas            | 425,26           | 0,48%       | 100%        |
| <b>Total</b>      | <b>88.983,11</b> | <b>100%</b> |             |

Tabla 3: análisis ABC de los costes

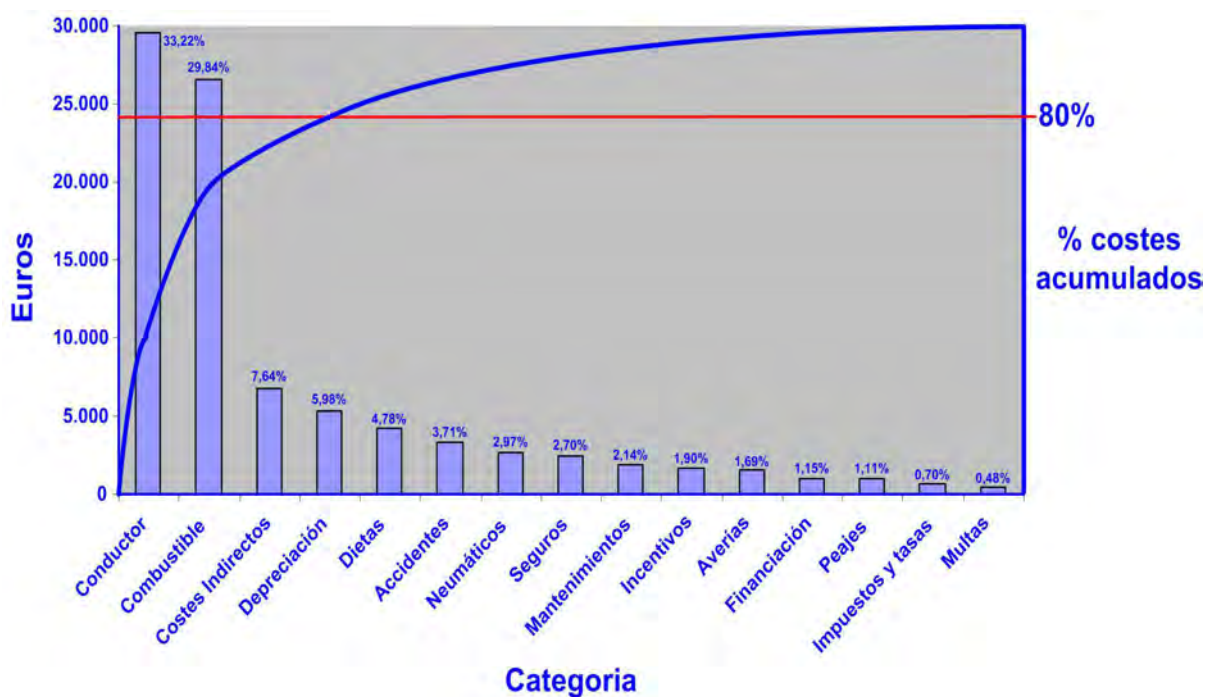


Gráfico 19: análisis ABC de los costes



Los costes del conductor, el combustible, indirectos, la depreciación y las dietas son alrededor del 80% de los costes totales.

Como los costes del conductor, indirectos y la depreciación son prácticamente costes fijos, nos tenemos que centrar en reducir los costes del combustible y las dietas.

Con los datos de la tabla 1 obtenemos los costes hundidos por tiempo= Costes fijos+indirectos/ (días u horas) de la tabla 4.

| Costes hundidos                                                         |                   |
|-------------------------------------------------------------------------|-------------------|
| Costes por tiempo                                                       | Cantidad          |
| Día                                                                     | 203,42 Euros/día  |
| Hora                                                                    | 24,068 Euros/hora |
| $203,42=(38.929,30+6.800,25)/225$ ; $24,068=(38.929,30+6.800,25)/1.900$ |                   |

Tabla 4: costes hundidos por tiempo.

Considerando los costes directos e indirectos, obtenemos el coste por kilómetro del vehículo según la tabla 5.

| Costes totales (directos e indirectos) |           |
|----------------------------------------|-----------|
| Euros                                  | Euros/Km. |
| 88.983,11                              | 1,186     |
| $1,186=88.983,11/75.000$               |           |

Tabla 5: coste total por Km. de un vehículo de la flota

Así mismo, dividiendo cada partida de la tabla 2 por el número de kilómetros. obtenemos el coste por Km. de cada partida.

El siguiente ratio nos suministra información de cómo la flota esta optimizada y utilizamos los recursos disponibles. Considerando los costes totales de la tabla 2 y cada una de las siguientes compañías de la tabla 6: transporte de mercancía, transporte de viajeros y taxis, que realizan las siguientes cantidades durante un año.

| Concepto  | Cantidad | Unidades           |
|-----------|----------|--------------------|
| Toneladas | 1.000    | Euros/km.-Tonelada |
| Viajeros  | 3.000    | Euros/Km.-Viajero  |
| Viajes    | 500      | Euros/Km.-viaje    |

Tabla 6: cantidades para viajeros y viajes

Aplicando la formula Coste/Km.\* (Toneladas o viajeros o viajes) obtenemos las siguientes datos de la tabla 7.

| Toneladas                                                                                        | Viajeros | Viajes  |
|--------------------------------------------------------------------------------------------------|----------|---------|
| 0,0012                                                                                           | 0,0004   | 0,00237 |
| 0,0012=88.983,11/(75.000*1.000); 0,0004=88.983,11/(75.000*3.000); 0,00237=88.983,11/(75.000*500) |          |         |

Tabla 7: costes Euros/Km.-Tonelada; Euros/Km.-Viajero; Euros/Km.-Viaje

El escenario ideal es obtener un coste por Km. bajo con un coste Euros/Km.-Tonelada; Euros/Km.-Viajero; Euros/Km.-Viaje bajo debido a que se utiliza la totalidad de la capacidad del vehículo, por que se puede tener un vehículo con un coste por kilómetro bajo con un coste Euros/Km.-Tonelada; Euros/Km.-Viajero; Euros/Km.-Viaje alto, por lo que no estamos optimizando la utilización de los vehículos.

## 2.6. CÁLCULO DEL COSTE DE UN SERVICIO

---

En flotas como las de transporte de mercancías o viajeros discrecional, los clientes nos solicitan realizar un servicio/trayecto y su correspondiente coste o presupuesto, o en flotas como el transporte de viajeros regular que realizan una ruta fija, tenemos que conocer el coste de realizar este servicio/trayecto para establecer las tarifas o presentar nuestra oferta en el concurso público de este servicio/trayecto, por lo tanto es recomendable conocer el coste de realizar este servicio/trayecto, para establecer una tarifa o precio con el objetivo de obtener un beneficio y rentabilidad.

Es una práctica muy habitual suministrar un presupuesto para este tipo de servicio al cliente sin calcular el coste de realizarlo, no sabiendo si se obtendrá una pérdida o un beneficio. Solamente al final de año con la información suministrada por la cuenta de resultados se obtiene una visión general, de si se ha obtenido beneficios o pérdidas para el conjunto de la compañía.

Para calcular el coste de realizar un trayecto se necesita conocer:

- El recorrido, para conocer los kilómetros y calcular los costes variables.
- El tiempo de duración para calcular los costes fijos e indirectos.
- La edad o el kilometraje del vehículo.
- El coste de oportunidad o el tipo de interés.

Con estos datos calculamos cada uno de los costes del gráfico 1.

A continuación se desarrolla un ejemplo práctico para el cálculo del coste de un trayecto en el transporte de mercancías, que tiene las siguientes características:

- Recorrido del trayecto: 1.925 Km. (ida y vuelta)
- Nº de conductores: 1
- Duración del trayecto: 3 días (2 noches), 23,45 horas de conductor considerando la legislación vigente de tiempo de descanso, el tiempo máximo de conducción, el tiempo de descarga y una velocidad media de 75,6 Km./hora.
- Edad del vehículo antes de realizar el trayecto: 1.123 días

- Depreciación: la depreciación es uno de los mayores costes de un vehículo, por lo tanto una desviación en el cálculo de cuanto se deprecia el vehículo para el trayecto que vamos a realizar, hará que el cálculo del coste del trayecto sea erróneo.

El cálculo de la depreciación del vehículo es lo más complejo de conocer de todas los costes del gráfico 1, las fuentes de información para calcular la depreciación son: históricos del vehículo, estimaciones, datos suministrados por compañías especializadas en este tipo de información o realizar benchmarking con otras flotas. Un error muy grave y habitual es utilizar la amortización contable en vez de la depreciación para calcular el coste del trayecto y que no se tiene que utilizar por que no se ajusta a la realidad.

Para calcular la depreciación del vehículo, lo más recomendable es aplicar un modelo que tenga en consideración las variables explicadas en el epígrafe 2.1.1.

El vehículo tiene un valor de adquisición de 100.000 euros y la depreciación tiene los siguientes valores para los siguientes 10 años considerando solamente el tiempo.

| Año          | Valor     | Depreciación     | % valor año 0 |
|--------------|-----------|------------------|---------------|
| 0            | 100.000   |                  |               |
| 1            | 70.000    | 30.000,00        | 30,00%        |
| 2            | 48.510    | 21.490,00        | 21,49%        |
| 3            | 33.449,34 | 15.060,66        | 15,06%        |
| 4            | 22.372,56 | 11.076,79        | 11,07%        |
| 5            | 14.814,22 | 7.558,33         | 7,55%         |
| 6            | 9.711,30  | 5.102,92         | 5,10%         |
| 7            | 6.347,04  | 3.364,26         | 3,36%         |
| 8            | 4.135,80  | 2.211,23         | 2,21%         |
| 9            | 2.689,55  | 1.446,26         | 1,44%         |
| 10           | 1.747,29  | 942,26           | 0,94%         |
| <b>TOTAL</b> |           | <b>98.252,71</b> |               |

Tabla: valores de depreciación para 10 años.

El gráfico 20 representa el valor del vehículo para los 10 años.

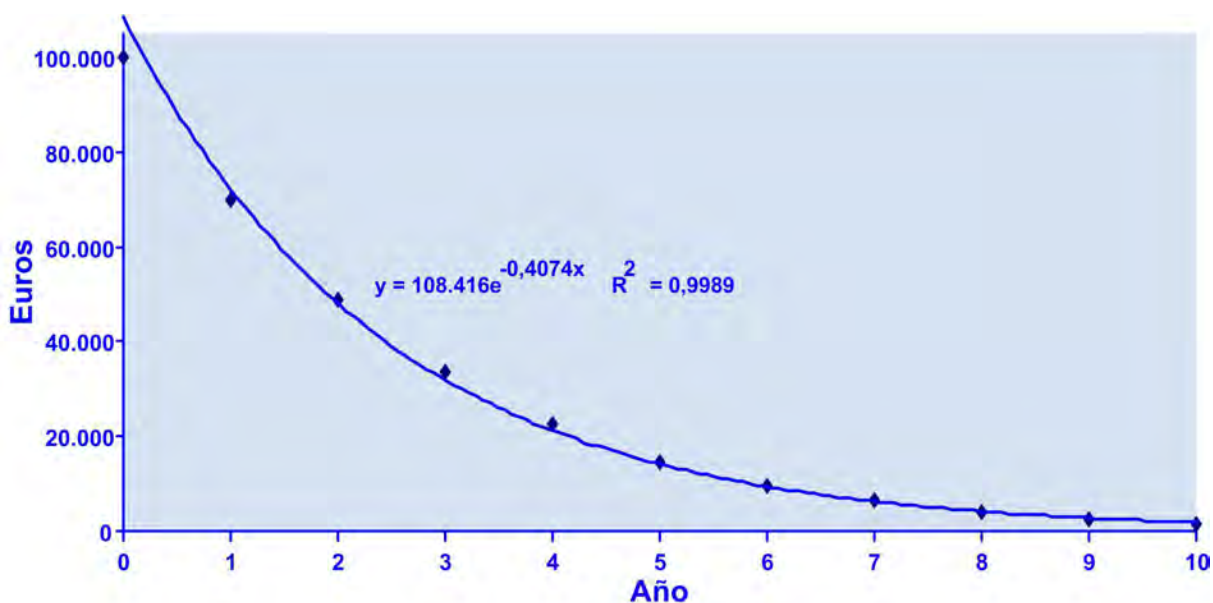


Gráfico 20: evolución del valor de la depreciación del vehículo

La evolución del valor del vehículo en el tiempo se ajusta a un modelo de regresión exponencial con un coeficiente de determinación  $R^2$  aproximadamente de 1, el gráfico 20 muestra su ecuación.

Para calcular la depreciación del vehículo se tiene que conocer el valor del vehículo antes y después del servicio/trayecto a realizar.

El valor del vehículo para 1.123 días ( $1.123/365=3,076712$  años) aplicando la ecuación de regresión exponencial del gráfico 20 es de 30.954,64 euros.

Como el viaje va a tener una duración de 3 días, el vehículo tendrá 1.126 días ( $1.126/365=3,08493$  años) a la finalización del mismo, el valor del vehículo aplicando la ecuación de regresión exponencial del gráfico 20 será de 30.851,16 euros.

La depreciación del vehículo para el servicio/trayecto es de:  $30.954,64 - 30.851,16 = 103,47$  euros.

- Financiación

Adquirimos el vehículo pagando 20.000 euros y el resto lo financiamos a 10 años con un tipo de interés del 8%, el cuadro de amortización es el mostrado en la tabla 8:

| Año          | Interés          | Amortización  | Pendiente |
|--------------|------------------|---------------|-----------|
| 1            | 6.203,25         | 5.444,21      | 74.555,80 |
| 2            | 5.751,37         | 5.896,07      | 68.659,74 |
| 3            | 5.262,01         | 6.385,44      | 62.274,31 |
| 4            | 4.732,03         | 6.915,41      | 55.358,89 |
| 5            | 4.158,06         | 7.489,38      | 47.869,49 |
| 6            | 3.536,42         | 8.111,02      | 39.758,48 |
| 7            | 2.863,23         | 8.784,22      | 30.974,26 |
| 8            | 2.134,14         | 9.513,32      | 21.460,95 |
| 9            | 1.344,53         | 10.302,92     | 11.158,04 |
| 10           | 489,41           | 11.158,03     | 0,00      |
| <b>Total</b> | <b>36.474,45</b> | <b>80.000</b> |           |

Tabla 8: cuadro de amortización de adquisición del vehículo.

El gráfico 21 representa los valores de los intereses a lo largo de los 10 años:

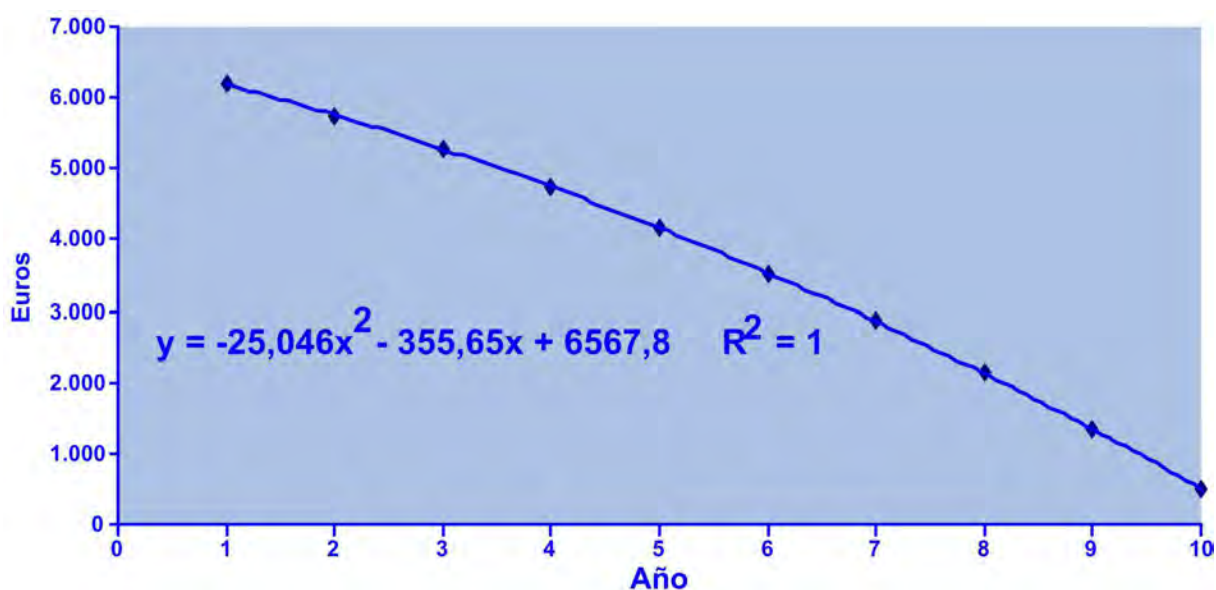


Gráfico 21: evolución de los intereses del préstamo.

Para calcular los costes de financiación del vehículo se tiene que conocer el valor de los intereses del préstamo antes y después del servicio/trayecto a realizar. La evolución del valor de los intereses del préstamo se ajusta a un modelo de regresión polinomial con un coeficiente de determinación  $R^2$  de 1, el gráfico 21 muestra su ecuación.

El valor de los intereses del vehículo para 1.123 días ( $1.123/365=3,076712$  años) aplicando la ecuación de regresión exponencial del gráfico 21 es de 5.236,48 euros.

Como el viaje va a tener una duración de 3 días, el vehículo tendrá 1.126 días ( $1.126/365=3,08493$  años) a la finalización del mismo, el valor de los intereses de vehículo aplicando la ecuación de regresión exponencial del gráfico 21 será de 5.232,28 euros.

El valor de los intereses para este servicio/trayecto es de:  $5.236,48-5.232,28=4,19$  euros.

- Conductor

Teniendo en consideración que las horas al año del conductor son 1.900 al año, y que su coste para la organización es de 32.000 euros brutos incluyendo el salario en bruto más las aportaciones a la seguridad social, el coste por hora es de  $32.000/1.900= 16,84$  euros/hora.

Las horas de conductor para este trayecto es de 23,45 horas, el coste para este trayecto del conductor es de  $23,45 \times 16,84= 394,95$  euros.

- Seguro

El coste del seguro del vehículo para el año asciende a 4.345,45 euros, como el vehículo tiene asignado un solo conductor que puede realizar al año 1.900 horas, el coste por hora del seguro es de  $4.345,45/1.900= 2,28$  euros/hora.

El coste del seguro para este trayecto es de  $23,45 \times 2,28=53,63$  euros.

- Impuestos y tasas:

Los impuestos y tasas para el año son de 600,45 euros, como el vehículo tiene asignado un solo conductor que puede realizar al año 1.900 horas, el coste por hora de los impuestos y tasas es de  $600,45/1.900=0,316$  euros/hora.

El coste del seguro para este trayecto es de  $23,45 \times 0,316=7,41$  euros.

- Costes indirectos

Los costes indirectos para el vehículo son de 5.245,78 euros, como el vehículo tiene asignado un solo conductor que puede realizar al año 1.900 horas, el coste por hora de los costes indirectos es de  $5.245,78/1.900=2,761$  euros/hora.

El coste de los costes indirectos para este trayecto es de  $23,45 \times 2,761=64,73$  euros.

- Combustible

La estimación de consumo para este trayecto de 1.925 Km. es la siguiente: en el viaje de ida que el vehículo esta cargado con la mercancía a transportar, la estimación del consumo es de 23,45 litros/100Km. y para el viaje de vuelta que el vehículo esta vacío es de 20,78 litros/100 Km.

El litro de combustible tiene un coste de 1,15 euros.

Coste del viaje de ida=  $(1.925/2 \times 100) \times 23,45 \times 1,15=259,56$  euros.

Coste del viaje de vuelta=  $(1.925/2 \times 100) \times 20,78 \times 1,15= 230,01$  euros

El coste total de combustible para este trayecto es de  $259,56+230,01=489,57$  euros.

- Neumáticos

El kilometraje medio de utilización de todos los neumáticos es de 50.000 Km. con un coste medio de 421,56 euros, por lo que el coste por Km. es  $421,56/50.000=0,008$  euros/Km.

El coste de los neumáticos para este trayecto es  $1.925 \times 0,008=16,21$  euros.

- Mantenimientos

El periodo del mantenimiento planificado es cada 30.000 Km. y tienen un coste medio de 521,45 euros, por lo que el coste por Km. es  $521,45/30.000=0,017$  euros/Km.

El coste del mantenimiento para este trayecto es  $1.925 \times 0,017=33,45$  euros.



- Averías

El vehículo tiene una avería cada 18.967 Km. con un coste medio de 785,45 euros, por lo que el coste por Km. es de  $785,45/18.967 = 0,041$  euros/Km.

El coste de las averías para este trayecto es  $1.925 \times 0,041 = 79,71$  euros.

- Accidentes

El vehículo tiene un accidente cada 28.365 Km. con un coste medio de 1.123,24 euros, por lo que el coste por Km. es  $1.123,24/28.365 = 0,039$  euros/Km.

El coste de los accidentes para este trayecto es  $1.925 \times 0,039 = 76,22$  euros.

- Multas

El vehículo es sancionado con una multa de tráfico cada 16.258 Km. con un coste medio de 125,54 euros, por lo que el coste por Km. es  $125,54/16.258 = 0,0077$  euros/Km.

El coste de las multas para este trayecto es  $1.925 \times 0,0077 = 14,86$  euros.

- Peajes

La ruta a realizar para este trayecto tiene 2 peajes con un coste de 20,45 euros y 41,23 euros para el viaje de ida y los mismos peajes para el viaje de vuelta.

El coste de los peajes asciende a  $2 \times (20,45 + 41,23) = 123,36$  euros.

- Dietas

El trayecto tiene una duración de 3 días, 2 noches, el conductor tiene unas dietas de manutención de 30 euros y por pernoctar por noche de 75 euros.

El coste de las dietas es  $3 \times 30 + 2 \times 75 = 90 + 150 = 240$  euros.

- Incentivos

La organización tiene un programa de incentivos para la reducción del consumo de combustible y los accidentes de tráfico, cada 23.454 kilómetros concede una gratificación

con un coste medio de 234,56 euros, por lo que es coste por Km. es  $234,56/23.454=0,01$  euros/Km.

El coste de los incentivos es  $1.925*0,01=19,25$  euros.

Agrupando todos los costes como en la tabla 2, obtenemos el coste para este trayecto y el coste por Km. mostrados en la tabla 9.

| Denominación                                        | Coste           | % coste     | Coste por Km. |
|-----------------------------------------------------|-----------------|-------------|---------------|
| <b>Costes directos</b>                              | 1.656,28        | 96,24%      | 0,860         |
| <b>Costes fijos (Tiempo)</b>                        | 563,65          | 32,75%      | 0,293         |
| <b>Costes de capital</b>                            | 107,66          | 6,26%       | 0,056         |
| Depreciación                                        | 103,47          | 6,01%       | 0,054         |
| Financiación                                        | 4,19            | 0,24%       | 0,002         |
| <b>Costes de operación</b>                          | 455,99          | 26,50%      | 0,237         |
| Conductor                                           | 394,95          | 22,95%      | 0,205         |
| Seguros                                             | 53,63           | 3,12%       | 0,028         |
| Impuestos y tasas                                   | 7,41            | 0,43%       | 0,004         |
| <b>Costes variables (Km.)</b>                       | 1.092,63        | 63,49%      | 0,568         |
| <b>Ineludibles</b>                                  | 695,16          | 40,39%      | 0,361         |
| Combustible                                         | 489,57          | 28,45%      | 0,254         |
| Averías                                             | 79,71           | 4,63%       | 0,041         |
| Accidentes                                          | 76,22           | 4,43%       | 0,039         |
| Mantenimientos                                      | 33,45           | 1,94%       | 0,017         |
| Neumáticos                                          | 16,21           | 0,94%       | 0,008         |
| <b>Eludibles</b>                                    | 397,47          | 23,10%      | 0,206         |
| Dietas                                              | 240,00          | 13,95%      | 0,125         |
| Peajes                                              | 123,36          | 7,17%       | 0,064         |
| Incentivos                                          | 19,25           | 1,12%       | 0,01          |
| Multas                                              | 14,86           | 0,86%       | 0,077         |
| <b>Costes indirectos</b>                            | 64,73           | 3,76%       | 0,034         |
| <b>Total costes</b>                                 | <b>1.721,01</b> | <b>100%</b> | <b>0,894</b>  |
| <b>Coste por Km.= Coste/ Km. recorridos (1.925)</b> |                 |             |               |

Tabla 9: estructura de costes para la realización del servicio/trayecto.

La tabla 10 muestra el análisis ABC para este servicio/trayecto.

| Denominación      | Costes          | % costes    | % acumulado |
|-------------------|-----------------|-------------|-------------|
| Combustible       | 489,57          | 28,45%      | 28,45%      |
| Conductor         | 394,95          | 22,95%      | 51,40%      |
| Dietas            | 240             | 13,95%      | 65,34%      |
| Peajes            | 123,36          | 7,17%       | 72,51%      |
| Depreciación      | 103,47          | 6,01%       | 78,52%      |
| Averías           | 79,71           | 4,63%       | 83,15%      |
| Accidentes        | 76,22           | 4,43%       | 87,58%      |
| Costes indirectos | 64,73           | 3,76        | 91,34%      |
| Seguros           | 53,63           | 3,12%       | 94,46%      |
| Mantenimientos    | 33,45           | 1,94%       | 96,40       |
| Incentivos        | 19,25           | 1,12%       | 97,52       |
| Neumáticos        | 16,21           | 0,94%       | 98,46%      |
| Multas            | 14,86           | 0,86%       | 99,33%      |
| Impuestos y tasas | 7,41            | 0,43%       | 99,76%      |
| Financiación      | 4,19            | 0,24%       | 100%        |
| <b>Total</b>      | <b>1.721,01</b> | <b>100%</b> |             |

Tabla 10: análisis ABC de costes del servicio.

Alrededor del 80% de los costes de este servicio/trayecto son el combustible, el conductor, las dietas, los peajes y la depreciación del vehículo.

Los mayores costes de este servicio corresponden al combustible, seguido del coste del conductor, pero si al conductor le sumamos las dietas, el conductor sería el primer coste de este servicio.

El coste total de este trayecto para esta organización es de 1.721,01 euros. La organización tiene que ofertar el precio para este servicio a partir de este coste base, teniendo en consideración sus costes de estructura (contabilidad, marketing, dirección etc.) y política de precios para obtener un beneficio y rentabilidad por la prestación de este servicio.

## 2.7. CÁLCULO DEL COSTE DE PROPIEDAD TCO (*Total Cost of Ownership*)

---

El coste de propiedad es el coste del vehículo durante el periodo de tiempo que presta el servicio (vida útil). En la industria de la gestión de flotas y *renting* se ha convertido en un *standard* y se utiliza principalmente para conocer:

- El coste total del vehículo durante su vida útil.
- Si es mejor adquirir el vehículo en propiedad o en *renting* desde el punto de vista económico.

El coste de propiedad descontado se calcula según la formula 1, también se puede calcular sin una tasa de descuento. La tabla 11 muestra las partidas a tener en consideración para calcular el TCO.

$$TDCO = \sum_{t=1}^{t=n} \frac{CT_t}{(1+r)^t}$$

Formula 1: coste de propiedad descontado

- TDCO: coste total descontado de propiedad.
- CTt: costes totales de propiedad.
- t: periodo de tiempo.
- r: tasa de descuento o coste del capital.
- n: periodo de renovación/retirada.

La tabla 11 muestra un ejemplo de coste de propiedad descontado para un vehículo adquirido en propiedad para un periodo de 6 años.

| Denominación                     | Año 1            | Año 2            | Año 3            | Año 4            | Año 5            | Año 6            | Total     |
|----------------------------------|------------------|------------------|------------------|------------------|------------------|------------------|-----------|
| <b>Costes de capital</b>         | <b>9.086,34</b>  | <b>8.177,71</b>  | <b>7.523,49</b>  | <b>6.996,85</b>  | <b>6.577,03</b>  | <b>6.248,18</b>  | 44.609,60 |
| <b>Depreciación</b>              | 8.796,56         | 7.916,90         | 7.283,55         | 6.773,70         | 6.367,28         | 6.048,92         | 43.186,92 |
| <b>Financiación</b>              | 289,78           | 260,80           | 239,94           | 223,14           | 209,75           | 199,27           | 1.422,68  |
| <b>Costes de operación fijos</b> | <b>3.023,57</b>  | <b>3.084,04</b>  | <b>3.145,72</b>  | <b>3.208,64</b>  | <b>3.272,81</b>  | <b>3.338,27</b>  | 19.073,05 |
| <b>Seguros</b>                   | 2.400,12         | 2.448,12         | 2.497,08         | 2.547,03         | 2.597,97         | 2.649,93         | 15.140,25 |
| <b>Impuestos y tasas</b>         | 623,45           | 635,92           | 648,64           | 661,61           | 674,84           | 688,34           | 3.932,80  |
| <b>Costes variables</b>          | <b>4.935,50</b>  | <b>5.083,57</b>  | <b>5.236,07</b>  | <b>5.393,15</b>  | <b>5.662,81</b>  | <b>5.945,95</b>  | 32.257,06 |
| <b>Combustible</b>               | 2.345,58         | 2.415,95         | 2.488,43         | 2.563,08         | 2.691,23         | 2.825,79         | 15.330,06 |
| <b>Mantenimientos</b>            | 712,36           | 733,73           | 755,74           | 778,42           | 817,34           | 858,20           | 4.655,79  |
| <b>Accidentes</b>                | 712,23           | 733,60           | 755,60           | 778,27           | 817,19           | 858,05           | 4.654,94  |
| <b>Averías</b>                   | 623,23           | 641,93           | 661,18           | 681,02           | 715,07           | 750,82           | 4.073,26  |
| <b>Neumáticos</b>                | 542,10           | 558,36           | 575,11           | 592,37           | 621,99           | 653,08           | 3.543,01  |
| <b>Costes de propiedad</b>       | <b>17.045,41</b> | <b>16.345,31</b> | <b>15.905,28</b> | <b>15.598,64</b> | <b>15.512,66</b> | <b>15.532,40</b> | 95.939,70 |
| <b>Costes de propiedad (3%)</b>  | <b>16.548,94</b> | <b>15.407,02</b> | <b>14.555,59</b> | <b>13.859,19</b> | <b>13.381,35</b> | <b>13.008,14</b> | 86.760,23 |

Tabla 11: costes de propiedad descontado

Hay que recalcar que para el cálculo del TCO no hay que tener en consideración el salario del conductor.

La tabla 12 muestra un ejemplo de coste de propiedad descontado para el mismo vehículo que la tabla 11 adquirido en *renting*, e incluye todas las partidas de la tabla 11 menos el combustible.

| Denominación               | Año 1            | Año 2            | Año 3            | Año 4            | Año 5            | Año 6            | Total            |
|----------------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|
| <b>Couta de renting</b>    | 15.780,05        | 14.040,94        | 13.638,02        | 14.226,37        | 13.545,25        | 13.414,33        | 84.644,96        |
| <b>Combustible</b>         | 2.345,58         | 2.415,95         | 2.488,43         | 2.563,08         | 2.691,23         | 2.825,79         | 15.330,06        |
| <b>Total</b>               | 18.125,63        | 16.456,89        | 16.126,45        | 16.789,45        | 16.236,48        | 16.240,12        | 99.975,02        |
| <b>Total descontado 3%</b> | <b>17.597,70</b> | <b>15.512,20</b> | <b>14.757,99</b> | <b>14.917,21</b> | <b>14.005,73</b> | <b>13.600,84</b> | <b>90.391,67</b> |

Tabla 12: TCO para un vehículo adquirido en *renting*.

Comparando las tablas 11 y 12, el vehículo desde el punto de vista económico, es mejor adquirirlo en propiedad debido a que es más económico que adquirirlo en *renting*.

Es importante conocer la desviación del TCO teórico y el real en un periodo de tiempo, las fuentes de los datos teóricos pueden ser un histórico de la flota; realizar estimaciones; otras flotas de vehículos; terceras compañías; instituciones u organismos oficiales; o los fabricantes de los vehículos. En la siguiente tabla 13 es un ejemplo de estas desviaciones para el primer año.

| Denominación                                                                                                                                                                               | Teórico          | Real             | Diferencia    | % diferencia   | % teórico     | % diferencia   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|------------------|---------------|----------------|---------------|----------------|
| <b>Costes de capital</b>                                                                                                                                                                   | <b>9.086,34</b>  | <b>9.222,90</b>  | <b>136,56</b> | <b>1,503%</b>  | <b>0,801%</b> | <b>16,660%</b> |
| <b>Depreciación</b>                                                                                                                                                                        | 8.796,56         | 8.926,36         | 129,80        | 1,476%         | 0,761%        | 15,835%        |
| <b>Financiación</b>                                                                                                                                                                        | 289,78           | 296,54           | 6,76          | 2,333%         | 0,040%        | 0,825%         |
| <b>Costes de operación-fijos</b>                                                                                                                                                           | <b>3.023,57</b>  | <b>3.379,57</b>  | <b>356,00</b> | <b>11,774%</b> | <b>2,089%</b> | <b>43,432%</b> |
| <b>Seguros</b>                                                                                                                                                                             | 2.400,12         | 2.654,12         | 254,00        | 10,583%        | 1,490%        | 30,988%        |
| <b>Impuestos y tasas</b>                                                                                                                                                                   | 623,45           | 725,45           | 102,00        | 16,361%        | 0,598%        | 12,444%        |
| <b>Costes variables</b>                                                                                                                                                                    | <b>4.935,50</b>  | <b>5.262,62</b>  | <b>327,12</b> | <b>6,628%</b>  | <b>1,919%</b> | <b>39,908%</b> |
| <b>Combustible</b>                                                                                                                                                                         | 2.345,58         | 2.478,54         | 132,96        | 5,669%         | 0,780%        | 16,221%        |
| <b>Mantenimientos</b>                                                                                                                                                                      | 712,36           | 741,25           | 28,89         | 4,056%         | 0,169%        | 3,525%         |
| <b>Accidentes</b>                                                                                                                                                                          | 712,23           | 756,48           | 44,25         | 6,213%         | 0,260%        | 5,398%         |
| <b>Averías</b>                                                                                                                                                                             | 623,23           | 654,21           | 30,98         | 4,971%         | 0,182%        | 3,780%         |
| <b>Neumáticos</b>                                                                                                                                                                          | 542,10           | 632,14           | 90,04         | 16,609%        | 0,528%        | 10,985%        |
| <b>Costes de propiedad</b>                                                                                                                                                                 | <b>17.045,41</b> | <b>17.865,09</b> | <b>819,68</b> | <b>4,809%</b>  | <b>4,809%</b> | <b>100%</b>    |
| Diferencia= Real-Teórico; % diferencia= Diferencia/Teórico;<br>% teórico= Diferencia/ total costes de propiedad Teórico;<br>% diferencia= Diferencia/total costes de propiedad Diferencia. |                  |                  |               |                |               |                |

Tabla 13: desviaciones del TCO real y teórico.

Como se observa en la tabla 13, la mayor desviación se ha producido en los seguros de los vehículos, seguido de la depreciación y el consumo de combustible.

## 2.8. PRESUPUESTO DE LA FLOTA

El presupuesto de la flota es una estimación de los ingresos y gastos por un periodo de tiempo, que se recomienda realizarlo por año natural con el objetivo de realizar un control y seguimiento desde el punto de vista económico.

El presupuesto de la flota ha de realizarse en un documento único, en que cada responsable o departamento realice su parte correspondiente, pero que tengan acceso a la totalidad del presupuesto. Un error muy común es que cada departamento o responsable de un área de la gestión de la flota elabora su presupuesto realizando el control y seguimiento de manera individual. El presupuesto de la gestión de la flota tiene las siguientes partidas mostradas en el gráfico 22:

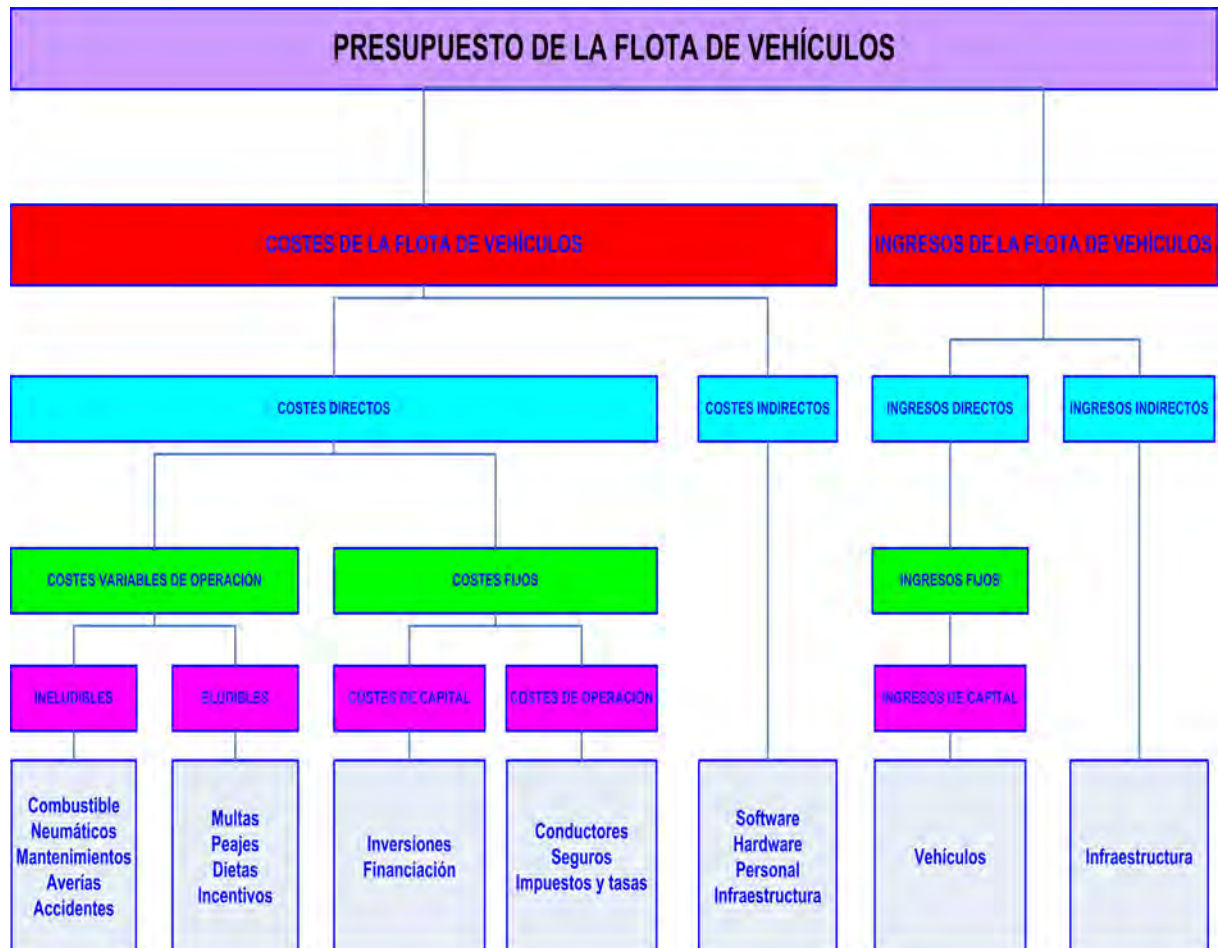


Gráfico 22: presupuesto de una flota de vehículos.

El presupuesto esta conformado prácticamente por las mismas partidas que las explicadas en el capítulo 2, pero hay unos cambios que se describen a continuación:

- Costes de las inversiones: es el presupuesto destinado a adquirir los vehículos, ya sean en propiedad o en *renting*, además del presupuesto para adquirir la infraestructura necesaria (inmuebles, taller etc.) para operar la flota.
- Ingresos por la venta de los vehículos: un vehículo se adquiere, opera, retira del servicio y vende a un tercero obteniendo un ingreso, que lo más conveniente es que sea utilizado de nuevo para adquirir nuevos vehículos o en otras partidas de la gestión de la flota.
- La organización tiene que establecer el tiempo máximo para vender el vehículo, y que depende principalmente de razones financieras, ya que es recomendable que el ingreso que se obtiene por la venta de los vehículos sea utilizado para la adquisición de nuevos vehículos, inversiones o gastos de la flota, además de que la organización dispone de un espacio limitado para almacenar un determinado número de vehículos.
- Ingresos por la venta de infraestructura: son los ingresos obtenidos por la venta de infraestructura como el terreno para almacenar los vehículos, material del taller, inmuebles etc. que no se necesitan para la gestión de la flota.

Para establecer el presupuesto del año se necesita conocer:

- El número óptimo de vehículos que se necesitan para un determinado nivel de servicio, para calcular los costes e ingresos fijos según el gráfico 22, los escenarios resultantes son los siguientes:

1. El número óptimo de vehículos que se necesitan es mayor que los que se tienen actualmente, por lo tanto hay que realizar las adquisiciones de estos vehículos.

2. El número óptimo de vehículos que se necesitan es menor que los que se tienen actualmente, por lo tanto hay que retirar estos vehículos del servicio y venderlos obteniendo un ingreso.



3. El número óptimo de vehículos que se necesitan es igual que los que se tienen, por lo tanto no hay que ni adquirir o retirar ningún vehículo de la flota.

- Cuantos conductores se necesitan para calcular los costes fijos de operación.
- Los kilómetros u horas que realizaremos para calcular los costes variables de operación.
- Los costes e ingresos indirectos necesarios para operar la flota.
- El periodo de renovación para calcular las inversiones en vehículos y sus ingresos por la venta de los vehículos retirados del servicio, y que a continuación en el siguiente epígrafe 2.8 se desarrolla como establecerla.

Una vez establecido el presupuesto para un periodo de tiempo, que suele ser normalmente un año natural, hay que realizar el control y seguimiento para conocer las desviaciones que se producen, que es recomendable realizarlo cada mes, aplicando el mismo análisis realizado en la tabla 13 que para el TCO.

## 2.9. RENOVACIÓN DE LOS VEHÍCULOS DE LA FLOTA

---

La organización tiene que establecer la política de renovación del vehículo del servicio, que puede ser cuando se alcance un kilometraje, una edad del vehículo o la que antes se cumpla, los aspectos fundamentales a considerar son los siguientes:

- Imagen de marca

Modelos de vehículos novedosos en el mercado del automóvil representan mejor la marca de una organización que vehículos más antiguos.

- Tecnología de los vehículos

Modelos de vehículos novedosos en el mercado del automóvil incorporan la última tecnología referente en seguridad activa y pasiva, consumo de combustible y las emisiones contaminantes, por lo tanto son un aspecto clave para la reducción de los accidentes de tráfico, el consumo de combustible, las emisiones contaminantes y las averías, además es una buena oportunidad para incorporar a la flota, vehículos que utilizan nuevas tecnologías en combustibles alternativos a los combustibles fósiles o vehículos eléctricos.

- Accidentes de tráfico

Existe una cierta edad del vehículo que los accidentes de tráfico se incrementan, y por lo tanto la disponibilidad del vehículo para prestar el servicio disminuye y los costes variables de operación aumentan.

- Legislación vigente

En ciertos tipos de servicios y/o mercados por ley no se pueden utilizar vehículos por encima de una antigüedad o edad, por lo que a partir de esa edad el vehículo tiene un valor residual prácticamente nulo en ese país y lo más recomendable es exportarlo a otro país donde pueda seguir operando. Este es el caso del transporte escolar en el que el vehículo no puede tener más de 16 años, contados desde su primera matriculación al inicio del curso escolar.

- Consumo de combustible

Existe una cierta edad del vehículo que el consumo de combustible se incrementa, y por lo tanto las emisiones contaminantes y los costes variables de operación.

- Averías

Existe una cierta edad del vehículo que el número de averías se incrementan, y por lo tanto la disponibilidad del vehículo para prestar el servicio disminuye y los costes variables de operación aumentan.

- Mercado en el que opera la organización

En determinados casos, la renovación de los vehículos está dictaminada por la competencia en el mercado en el que opera la organización, y es una ventaja competitiva. Las empresas de *renting* o alquiler de vehículos tienen que ofrecer a sus clientes los vehículos más novedosos del mercado del automóvil para prestar su servicio y ser competitivos.

- Restricciones financieras

El presupuesto destinado a la renovación de los vehículos limita el número de vehículos a renovar por cada periodo y por lo tanto la edad media de la flota.

- Sistema de información de la organización

Cuanta más información tengamos de los costes de los vehículos de la flota más preciso y confiable será el resultado del periodo de renovación.

Existe una amplia literatura científica en renovación de flotas de vehículos, los modelos más utilizados son el modelo básico de los costes del ciclo de vida (LCCA, *lyfe cycle cost analysis*), el modelo con descenso de la tasa de utilización con la edad o el modelo de renovación en paralelo (*parallel fleet replacement problem*) (Simms, Lamarre y Jardine, 1984) (Buddhakulsomsiri, Parthanadee y Charnsethikul, 2012).

Otros métodos basados en el LCCA son el coste anual equivalente, el de comparación con coste anual, el de reposición de activos o los desarrollados por Eilon, King y Hutchinson (1966), y Redmer (2009). La mayoría de los métodos utilizan los costes del ciclo de vida para determinar el periodo de renovación.

El modelo a utilizar en nuestra organización es el que mejor se adapte a las especificaciones, características, operativa y objetivos de nuestra flota, y a la disponibilidad de los datos.

Se desarrolla el modelo básico, que es el más sencillo y extendido, que considera que el vehículo tiene una tasa de utilización constante durante su vida útil.

Para calcular algunos de los costes de propiedad del vehículo se utilizan las siguientes fuentes de datos; un histórico de nuestra organización; el fabricante del vehículo; otras flotas de vehículos; terceras compañías que suministran esta información; o estimarlos directamente.

El periodo de renovación del vehículo es cuando el coste total de propiedad es mínimo (TCO), utilizando el modelo básico mostrado en el gráfico 23.

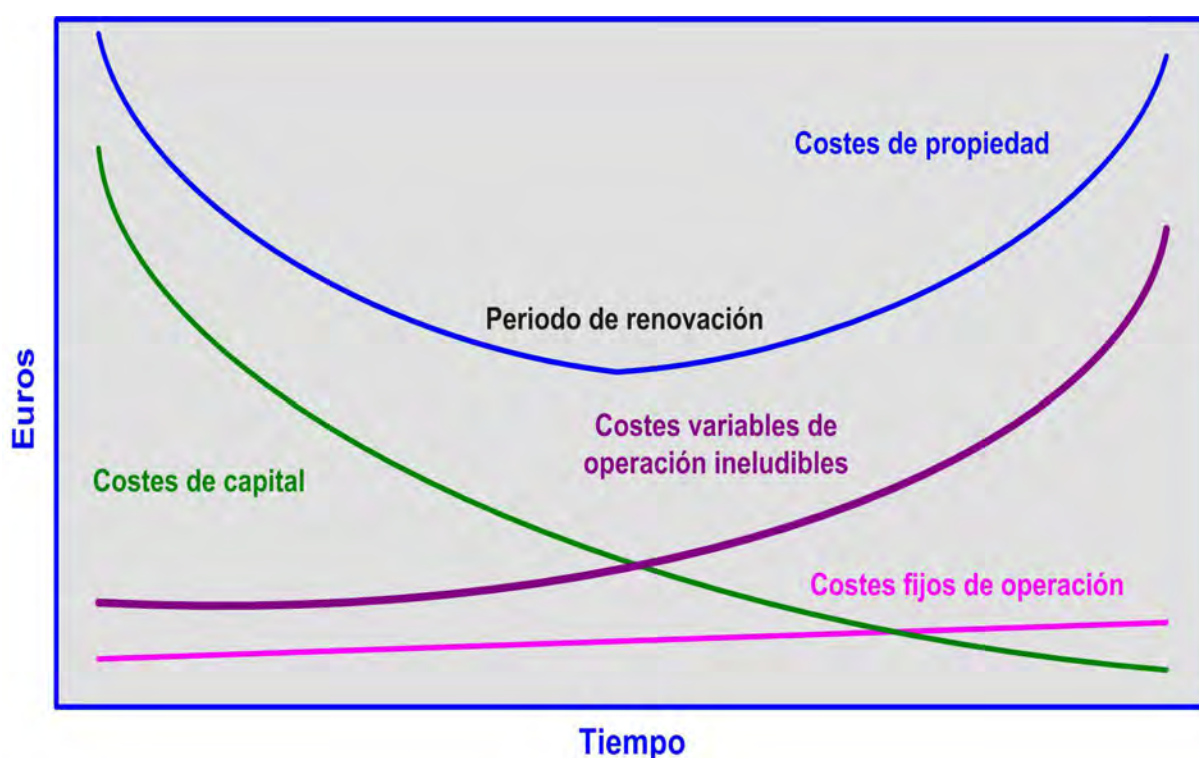


Gráfico 23: cálculo del periodo de renovación de la flota de vehículos.

Los costes que se utilizan para calcular el periodo de renovación son los mismos que los utilizados para calcular el TCO del vehículo tal como muestra la tabla 13.

Si los costes variables de operación ineludibles disminuyen, su curva se desplazará hacia la derecha como muestra el gráfico 24 y el periodo de renovación de los vehículos será mayor y por lo tanto utilizaremos los vehículos un mayor periodo de tiempo y necesitaremos menos presupuesto para operar la flota, como muestra el gráfico 24.

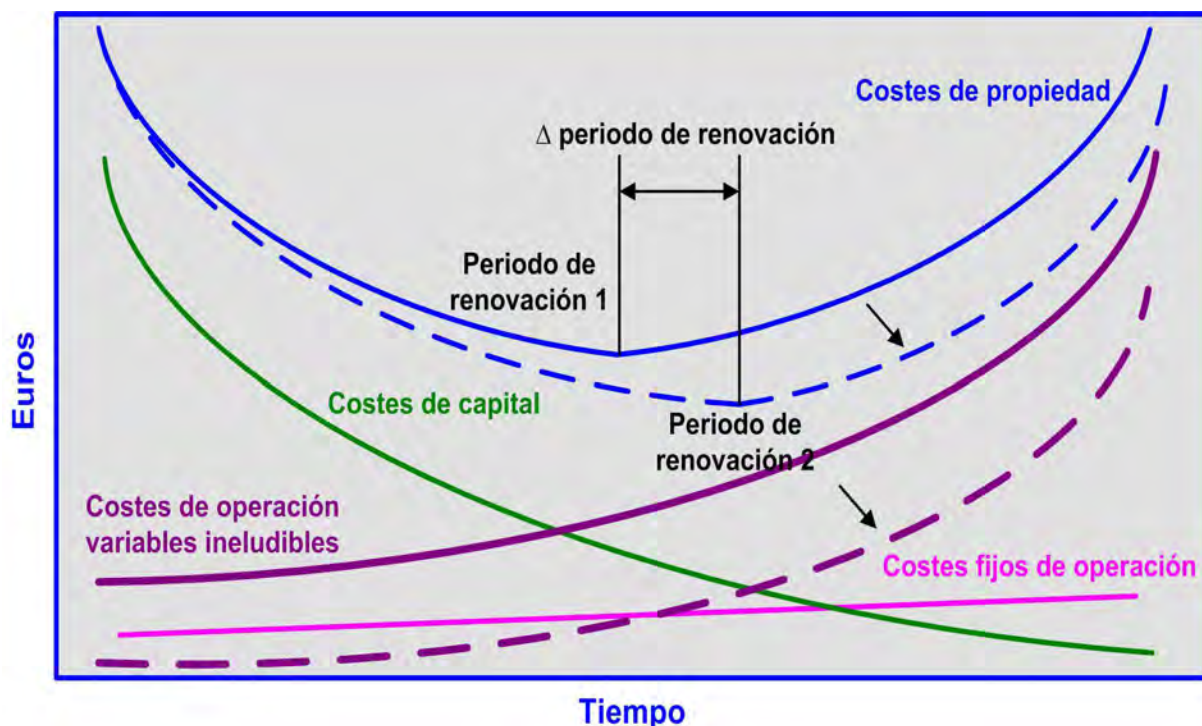


Gráfico 24: incremento del periodo de renovación

El periodo de renovación debe ser establecido por clases de vehículos de similares características, que tengan la misma estructura de costes a lo largo de su vida útil, y que presten el mismo tipo de servicio. La gestión de la renovación es más compleja cuanto más vehículos de diferentes edades y tipos.

Cuando el número de vehículos es superior al número óptimo, los conductores y/o usuarios prefieren utilizar los vehículos con menos kilometraje o edad, provocando un exceso de utilización en estos y una infrautilización en los vehículos más antiguos, y por lo tanto los costes variables de operación ineludibles de los vehículos con menos kilometraje o edad son mayores que los antiguos y la hipótesis de que estos costes son crecientes según el modelo básico no se cumple, lo que unido a que los costes de capital siempre disminuyen provocan que la curva de los costes totales de propiedad no tenga forma de bañera y por lo tanto el cálculo de un periodo de renovación es más complejo.

Si el presupuesto para la renovación de los vehículos es limitado, hay que determinar el orden de los vehículos que se tienen que renovar, para ello se tiene que establecer un criterio como los vehículos con más edad o kilometraje, con mayor valor residual, que más contaminen, prioritarios en nuestra flota o con mayores costes totales acumulados.

A continuación se desarrolla un ejemplo práctico de renovación utilizando los datos utilizados para el ejemplo del cálculo del TCO del epígrafe 2.6 como muestra la tabla 14.

| Denominación                     | Año 1            | Año 2            | Año 3            | Año 4            | Año 5            | Año 6            | Año 7            | Año 8            | Año 9            | Año 10           | Total             |
|----------------------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|-------------------|
| <b>Costes de capital</b>         | <b>9.086,34</b>  | <b>8.177,71</b>  | <b>7.523,49</b>  | <b>6.996,85</b>  | <b>6.577,03</b>  | <b>6.248,18</b>  | <b>5.998,26</b>  | <b>5.818,31</b>  | <b>5.701,94</b>  | <b>5.644,92</b>  | <b>67.773,03</b>  |
| <b>Depreciación</b>              | 8.796,56         | 7.916,90         | 7.283,55         | 6.773,70         | 6.367,28         | 6.048,92         | 5.806,96         | 5.632,75         | 5.520,10         | 5.464,90         | 65.611,62         |
| <b>Financiación</b>              | 289,78           | 260,80           | 239,94           | 223,14           | 209,75           | 199,27           | 191,30           | 185,56           | 181,85           | 180,03           | 2.161,41          |
| <b>Costes de operación fijos</b> | <b>3.023,57</b>  | <b>3.084,04</b>  | <b>3.145,72</b>  | <b>3.208,64</b>  | <b>3.272,81</b>  | <b>3.338,27</b>  | <b>3.405,03</b>  | <b>3.473,13</b>  | <b>3.542,59</b>  | <b>3.613,45</b>  | <b>33.107,25</b>  |
| <b>Seguros</b>                   | 2.400,12         | 2.448,12         | 2.497,08         | 2.547,03         | 2.597,97         | 2.649,93         | 2.702,92         | 2.756,98         | 2.812,12         | 2.868,37         | 26.280,64         |
| <b>Impuestos y tasas</b>         | 623,45           | 635,92           | 648,64           | 661,61           | 674,84           | 688,34           | 702,11           | 716,15           | 730,47           | 745,08           | 6.826,60          |
| <b>Costes variables</b>          | <b>4.935,50</b>  | <b>5.083,57</b>  | <b>5.236,07</b>  | <b>5.393,15</b>  | <b>5.662,81</b>  | <b>5.945,95</b>  | <b>6.362,17</b>  | <b>6.807,52</b>  | <b>7.420,20</b>  | <b>8.088,02</b>  | <b>60.934,96</b>  |
| <b>Combustible</b>               | 2.345,58         | 2.415,95         | 2.488,43         | 2.563,08         | 2.691,23         | 2.825,79         | 3.023,60         | 3.235,25         | 3.526,42         | 3.843,80         | 28.959,14         |
| <b>Mantenimientos</b>            | 712,36           | 733,73           | 755,74           | 778,42           | 817,34           | 858,20           | 918,28           | 982,56           | 1.070,99         | 1.167,37         | 8.794,98          |
| <b>Accidentes</b>                | 712,23           | 733,60           | 755,60           | 778,27           | 817,19           | 858,05           | 918,11           | 982,38           | 1.070,79         | 1.167,16         | 8.793,38          |
| <b>Averías</b>                   | 623,23           | 641,93           | 661,18           | 681,02           | 715,07           | 750,82           | 803,38           | 859,62           | 936,99           | 1.021,31         | 7.694,56          |
| <b>Neumáticos</b>                | 542,10           | 558,36           | 575,11           | 592,37           | 621,99           | 653,08           | 698,80           | 747,72           | 815,01           | 888,36           | 6.692,91          |
| <b>Costes de propiedad</b>       | <b>17.045,41</b> | <b>16.345,31</b> | <b>15.905,28</b> | <b>15.598,64</b> | <b>15.512,66</b> | <b>15.532,40</b> | <b>15.765,46</b> | <b>16.098,96</b> | <b>16.664,73</b> | <b>17.346,38</b> | <b>161.815,23</b> |

Tabla 14: costes de propiedad para calcular el periodo de renovación

El periodo de renovación viene establecido cuando el coste de propiedad es mínimo, el gráfico 25 muestra la evolución de los costes de propiedad, capital variables ineludibles de operación y fijos de operación.

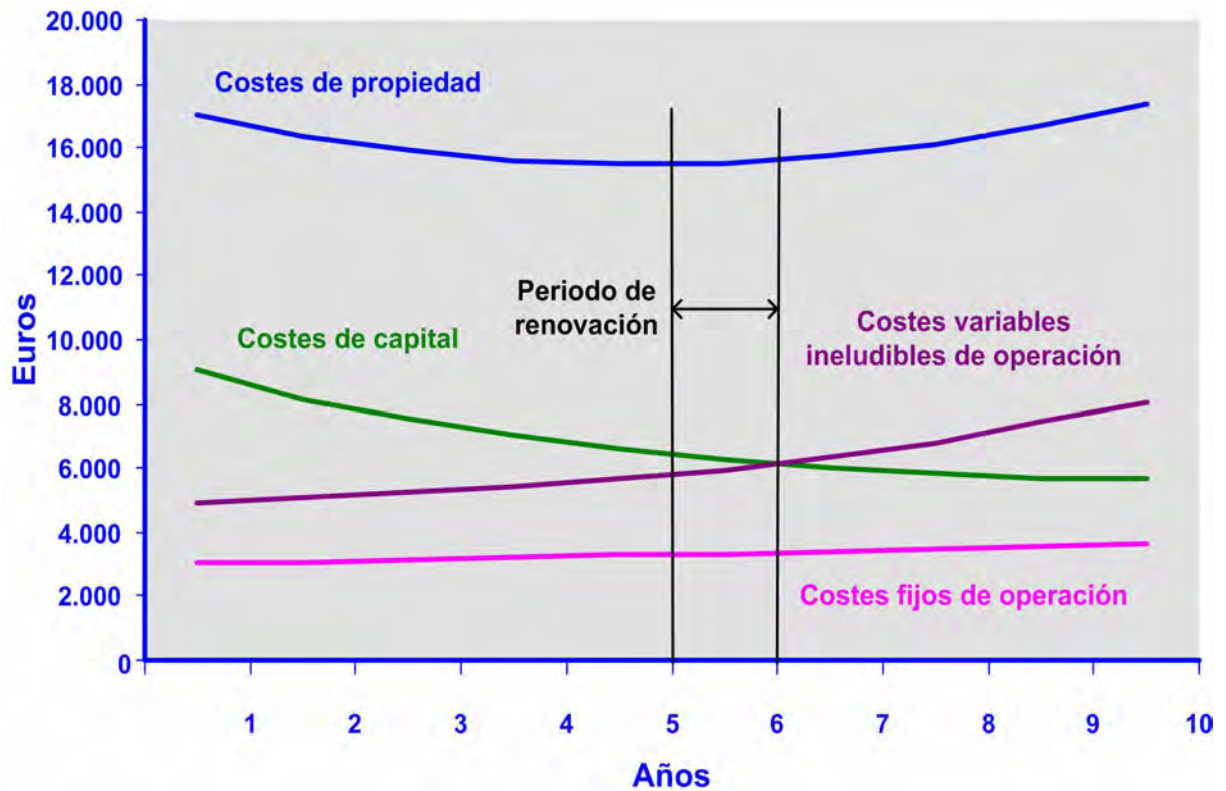


Gráfico 25: caso práctico de un periodo de renovación

Según los datos de la tabla 14 y el gráfico 25, el coste de propiedad mínimo se produce entre los años 5 y 6, por lo que el periodo de renovación tiene que estar comprendido en este periodo, para ser práctico se recomienda establecer el periodo de renovación en 6 años.

### 3. CONTROL Y SEGUIMIENTO DE LOS COSTES VARIABLES DE LA FLOTA

---



### 3.1. INTRODUCCIÓN

---

El valor monetario de un coste es igual a su cantidad multiplicado por su precio, la tabla 15 muestra como varia el valor de un coste dependiendo de las variaciones de los precios y las cantidades.

| Concepto   | Precio + | Precio = | Precio - |
|------------|----------|----------|----------|
| Cantidad + | +        | +        | +,=,-    |
| Cantidad = | +        | =        | -        |
| Cantidad - | +,=,-    | -        | -        |

Tabla 15: diferentes posibilidades de la variación del valor de un coste.

Los costes directos están divididos según el gráfico 1 en costes fijos y en costes variables de operación.

- Los costes fijos permanecen prácticamente constantes a lo largo de la vida útil del vehículo, a continuación se desarrolla como cada coste directo fijo puede variar en el tiempo
  - La depreciación puede variar por las siguientes causas: el vehículo esta muy deteriorado por haber tenido accidentes y averías que no se han reparado, las variaciones de precio en el mercado de segunda mano, añadir equipamiento o realizar mejoras en el vehículo durante su vida útil que incrementen su valor.
  - El coste de financiación puede variar dependiendo de las características de nuestra organización o de los tipos de interés.
  - Los salarios de los conductores pueden variar dependiendo del convenio del sector y/o del IPC.
  - Los seguros pueden variar dependiendo de la modalidad contratada como a todo riesgo, a terceros o con franquicia, y los precios se pueden considerar que varían según el IPC.
  - Los impuestos y tasas son establecidos por las administraciones públicas y se pueden considerar que varían según el IPC.
- Los costes indirectos permanecen prácticamente constantes a lo largo de la vida del vehículo y se puede considerar que varían según el IPC.
- Los costes variables de operación son los costes en los que se incurren por la cantidad de kilómetros recorridos u horas realizadas, y pueden variar

considerablemente en el tiempo, por lo que hay que realizar un control y seguimiento de los mismos en profundidad.

A continuación se desarrolla que impacto tienen las variables involucradas y partidas del gráfico 1 en los costes variables de operación.

- La distancia recorrida tiene un impacto alto en los costes variables de operación: a mayor distancia recorrida que la planificada, aumentan los costes variables de operación en todas sus partidas, la depreciación y el tiempo de disponibilidad del vehículo disminuye, por lo que en cualquier tipo de flota uno de los objetivos es cumplir con la distancia planificada y minimizar la distancia recorrida.
- La velocidad media tiene un impacto alto en los costes variables de operación: a mayor velocidad media, aumentan el consumo de combustible, las probabilidades de sufrir un accidente de tráfico, el desgaste de los neumáticos y el vehículo y por lo tanto la depreciación.
- El combustible tiene un impacto alto en los costes variables de operación: es principalmente el mayor de todos los costes variables de operación y puede variar considerablemente en el tiempo.

El precio del combustible esta determinado por razones externas como el libre mercado y los impuestos o por razones internas de nuestra organización como realizar coberturas sobre el precio del combustible comprando opciones o futuros del mismo, tener nuestros propios depósitos de combustible o un acuerdo marco con un proveedor, por lo que el precio del combustible es más económico.

La cantidad de combustible varia dependiendo del consumo de combustible y la distancia recorrida.

- Los accidentes de tráfico tienen un impacto alto en los costes variables de operación: a mayor número de accidentes, aumentan el tiempo en el que no se puede utilizar el vehículo, la depreciación, el tiempo en el que los conductores están de baja y no pueden trabajar, además de las posibles lesiones que causan a los conductores, usuarios y terceras personas como peatones o ciclistas.

El precio puede variar por razones externas como el libre mercado, o por razones internas como la elección de la marca de los recambios, tener un seguro a todo riesgo, a terceros o con franquicia, la utilización de talleres propios o externos, o por tener un acuerdo marco con un distribuidor de recambios, por lo que estos son más económicos.

- Los neumáticos tienen un impacto moderado en los costes variables de operación: utilizar neumáticos que no tienen las mínimas condiciones de seguridad, excesivamente desgastados, no tener la presión de inflado apropiada aumentan los accidentes de tráfico, las averías y el consumo de combustible.

El precio puede variar por razones externas como el libre mercado o los impuestos, o por razones internas como la elección de la marca del neumático o por tener un acuerdo marco con una marca de neumáticos y/o proveedor, por lo que estos son más económicos.

- El mantenimiento tiene un impacto moderado en los costes variables de operación: no realizar el mantenimiento según las instrucciones del fabricante del vehículo aumentan las averías, los accidentes de tráfico, la depreciación y el consumo de combustible.

El precio puede variar por razones externas como el libre mercado, o por razones internas como la elección de la marca de los recambios, la utilización de talleres propios o externos, o por tener un acuerdo marco con un distribuidor de recambios, por lo que estos son más económicos.

- Las averías tienen un impacto moderado en los costes variables de operación: a mayor número de averías, aumentan el tiempo en el que no se puede utilizar el vehículo, los accidentes de tráfico, la depreciación y el consumo de combustible.

El precio puede variar por razones externas como el libre mercado, o por razones internas como la elección de la marca de los recambios, la utilización de talleres propios o externos, o por tener un acuerdo marco con un distribuidor de recambios, por lo que estos son más económicos.

- Las multas tienen un impacto bajo en los costes variables de operación, y dependerán de la formación recibida por los conductores y si se cumple con la legislación vigente, el precio es establecido por las administraciones públicas.
- Los peajes tienen un impacto bajo en los costes variables de operación: disminuyen los accidentes de tráfico y el consumo de combustible debido a que son autovías y autopistas que evitan las carreteras secundarias que es donde más accidentes de tráfico se producen.

El precio está determinado por las compañías gestoras de los peajes o las administraciones públicas.

- Las dietas tienen un impacto bajo en los en los costes variables de operación: dependen de si los servicios que se prestan son de corto o largo recorrido donde es necesario pernoctar. El precio esta determinado por los acuerdos que pueden llegar entre la organización y los conductores y/o por un convenio colectivo.
- Los incentivos tienen un impacto moderado en los costes del variables de operación: si el programa de incentivos se cumple, puede reducir considerablemente el consumo de combustible o los accidentes de tráfico. El precio esta determinado por los acuerdos que pueden llegar entre la organización y los conductores.

La tabla 16 muestra que impacto tiene cada variable involucrada en los costes variables de operación.

| Concepto              | Impacto  |
|-----------------------|----------|
| Distancia             | Alto     |
| Velocidad media       | Alto     |
| Combustible           | Alto     |
| Accidentes de tráfico | Alto     |
| Neumáticos            | Moderado |
| Mantenimientos        | Moderado |
| Averías               | Moderado |
| Incentivos            | Moderado |
| Multas                | Bajo     |
| Peajes                | Bajo     |
| Dietas                | Bajo     |

Tabla 16: impacto de las variables y partidas en los costes variables de operación

El gráfico 26 muestra la relación entre los diferentes costes variables de operación, la distancia, la velocidad media, el tiempo productivo del vehículo y la depreciación.

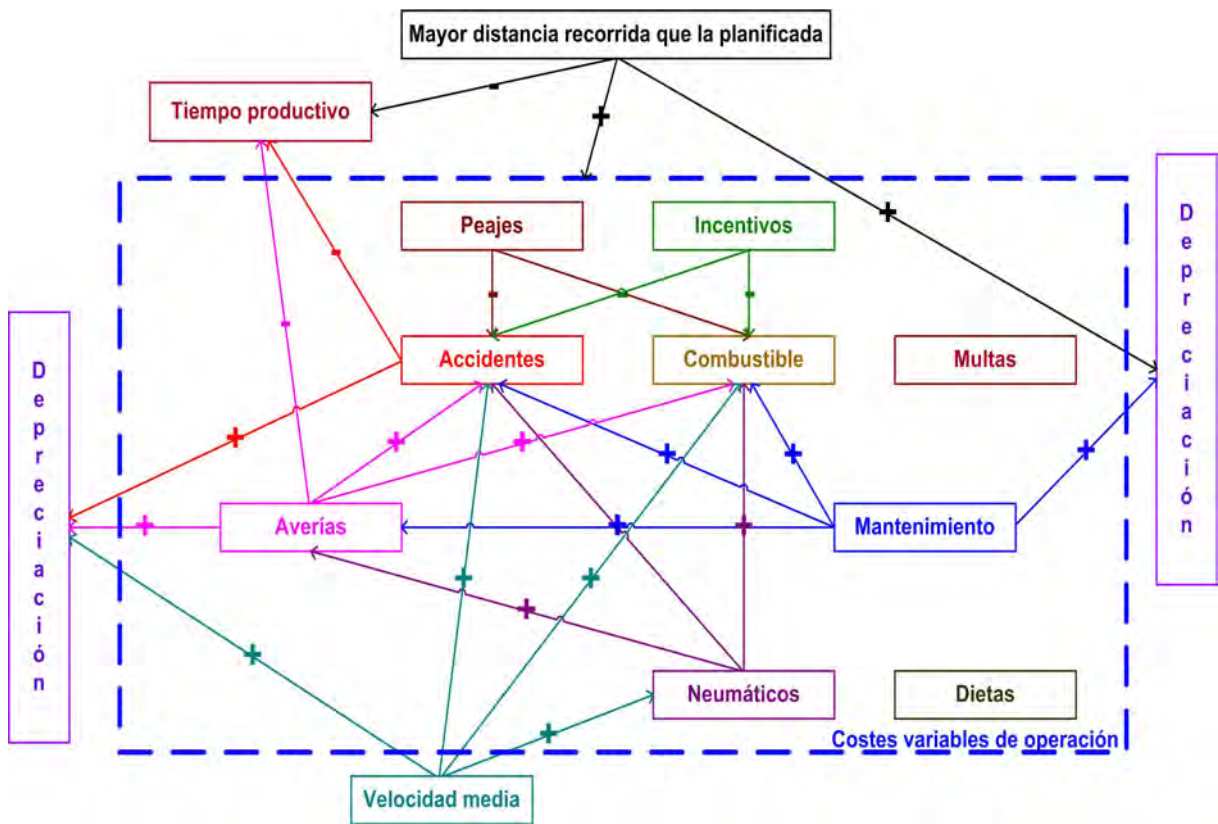


Gráfico 26: relación entre los diferentes costes variables de operación.

### 3.2. MODELO PROPUESTO

---

A continuación se desarrolla un modelo para el control y seguimiento de los costes variables de operación de una flota de vehículos.

En cada instante de tiempo  $T_x$ , se establece los costes variables de operación planificados para un periodo  $P_x$ , una vez transcurrido el periodo  $P_x$  en el instante  $T_{x+1}$  se cuantifican los costes de operación variables reales y se miden las desviaciones producidas respecto a los planificados, tal como muestra el gráfico 27:

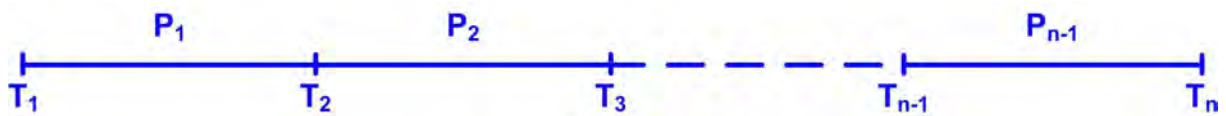


Gráfico 27: periodos de tiempo de la metodología propuesta

El coste real (Crt) en el instante  $T_{x+1}$  pueden tener desviaciones respecto al coste planificado en el instante  $T_x$  (Cpt) por los dos siguientes motivos:

- El coste unitario real (CurT)
- La distancia real recorrida (Dr)

Actualmente existen varias herramientas que nos suministran la mejor ruta a realizar como con un *software* de optimización de rutas o algunos servicios gratuitos sencillos *online* en *internet* que nos suministran las rutas óptimas, que combinado con la utilización del GPS para realizar la ruta planificada, es prácticamente la distancia mínima real a recorrer, por lo que recorrer menor distancia real que la planificada es muy difícil.

Pero se puede recorrer más distancia que la planificada por el uso indebido del vehículo, que el conductor se pierda o por el uso del vehículo con fines particulares, para evitar esta situación se hace imprescindible la utilización de un servicio telemático que guía al conductor por la ruta realizar (GPS), y nos reporta si el conductor se ha salido de la ruta planificada, así como de los usos indebidos y particulares del vehículo.

La tabla 17 muestra las diferentes posibilidades de cómo el coste real varía en el instante  $T_{x+1}$ , atendiendo a los incrementos o decrementos del coste unitario y la distancia recorrida real para un periodo  $P_x$ .

| Concepto         | Distancia recorrida + | Distancia recorrida = | Distancia recorrida - |
|------------------|-----------------------|-----------------------|-----------------------|
| Coste unitario + | +                     | +                     | +, =, -               |
| Coste unitario = | +                     | =                     | -                     |
| Coste unitario - | +, =, -               | -                     | -                     |

Tabla 17: variación del coste real respecto a los planificados en el periodo  $P_x$ .

La mejor situación es aquella en la que el coste unitario y la distancia real son menores que los planificados. La peor situación es aquella en la que el coste unitario y la distancia real son mayores que los planificados.

Hay dos situaciones que son: el coste unitario es menor pero la distancia recorrida es mayor, o el coste unitario es mayor pero la distancia recorrida es menor. El coste real será mayor, igual o menor que el planificado dependiendo de la cuantía del coste unitario y la distancia recorrida real.

Hay que tener en consideración como se establece la distancia planificada a recorrer y depende principalmente de los siguientes casos de flotas.

- Flota con rutas planificadas, la distancia planificada a recorrer en cada periodo  $P_x$  viene determinada por las rutas a realizar.
- Flotas con demanda aleatoria de los vehículos (alquiler de vehículos, servicios de emergencia, taxis etc.) o un vehículo asignado a un usuario/actividad (comerciales, directivos etc.), hay que establecer la distancia planificada a recorrer en cada periodo  $P_x$  en el instante  $T_x$ , para cumplir con el presupuesto y/o los costes variables de operación de la flota.

El primer paso es establecer los costes variables de operación planificados en el periodo  $T_x$ , por tipo de vehículo, ya que tienen diferentes valores de los mismos, para ello utilizaremos la siguiente tabla 17.

| Concepto                                                                                             | Precio planificado | Cantidad planificada | Coste unitario planificado | Coste planificado |
|------------------------------------------------------------------------------------------------------|--------------------|----------------------|----------------------------|-------------------|
| Combustible                                                                                          | Pp1                | Cp1                  | $Cup1=Pp1/Cp1$             | $Cpt1=Cup1*Dp$    |
| Neumáticos                                                                                           | Pp2                | Cp2                  | $Cup2=Pp2/Cp2$             | $Cpt2=Cup2*Dp$    |
| Mantenimientos                                                                                       | Pp3                | Cp3                  | $Cup3=Pp3/Cp3$             | $Cpt3=Cup3*Dp$    |
| Averías                                                                                              | Pp4                | Cp4                  | $Cup4=Pp4/Cp4$             | $Cpt4=Cup4*Dp$    |
| Accidentes                                                                                           | Pp5                | Cp5                  | $Cup5=Pp5/Cp5$             | $Cpt5=Cup5*Dp$    |
| Multas                                                                                               | Pp6                | Cp6                  | $Cup6=Pp6/Cp6$             | $Cpt6=Cup6*Dp$    |
| Peajes                                                                                               | Pp7                | Cp7                  | $Cup7=Pp7/Cp7$             | $Cpt7=Cup7*Dp$    |
| Dietas                                                                                               | Pp8                | Cp8                  | $Cup8=Pp8/Cp8$             | $Cpt8=Cup8*Dp$    |
| Incentivos                                                                                           | Pp9                | Cp9                  | $Cup9=Pp9/Cp9$             | $Cpt9=Cup9*Dp$    |
| <b>Total</b>                                                                                         |                    |                      | $CupT=Cup1+...+Cup9$       | $Cpt=CupT*Dp$     |
| Distancia planificada: Dp                                                                            |                    |                      |                            |                   |
| Precio planificado en Euros; Cantidad planificada en kilómetros; Distancia planificada en Kilómetros |                    |                      |                            |                   |

Tabla 17: costes variables de operación planificados en el instante  $T_x$ .

Para calcular los costes variables de operación planificados, primero tenemos que establecer el precio, la cantidad y la distancia planificada y a continuación calculamos el coste unitario y el coste planificado según la tabla 17.

El precio planificado es un precio medio de cada concepto en el instante  $T_x$ , por ejemplo el precio medio de un mantenimiento o la reparación de una avería. La cantidad planificada es cada cuantos kilómetros se produce un concepto, por ejemplo se produce un accidente cada 15.000 Km. o consumimos un litro de combustible cada 13 Km. El coste unitario planificado de cada concepto es el precio planificado dividido por la cantidad planificada. El coste planificado total es la multiplicación del coste unitario planificado por la distancia planificada.

Las fuentes de la información para calcular los costes variables de operación planificados pueden ser: un histórico de la flota; realizar estimaciones; otras flotas de vehículos; terceras compañías; instituciones u organismos oficiales; o los fabricantes de los vehículos.

El segundo paso es recopilar los costes reales, los precios medios reales y la distancia real recorrida para el periodo  $P_x$  en el instante  $T_{x+1}$ . Con estos datos calculamos el coste unitario real y la cantidad real según la tabla 18.



| Concepto                                                                                                    | Precio real | Cantidad real | Coste unitario real | Coste real        |
|-------------------------------------------------------------------------------------------------------------|-------------|---------------|---------------------|-------------------|
| Combustible                                                                                                 | Pr1         | Cr1=Pr1/Cur1  | Cur1= Crt1/Dr       | Crt1              |
| Neumáticos                                                                                                  | Pr2         | Cr2= Pr2/Cur2 | Cur2= Crt2/Dr       | Crt2              |
| Mantenimientos                                                                                              | Pr3         | Cr3= Pr3/Cur3 | Cur3= Crt3/Dr       | Crt3              |
| Averías                                                                                                     | Pr4         | Cr4= Pr4/Cur4 | Cur4= Crt4/Dr       | Crt4              |
| Accidentes                                                                                                  | Pr5         | Cr5= Pr5/Cur5 | Cur5= Crt5/Dr       | Crt5              |
| Multas                                                                                                      | Pr6         | Cr6= Pr6/Cur6 | Cur6= Crt6/Dr       | Crt6              |
| Peajes                                                                                                      | Pr7         | Cr7= Pr7/Cur7 | Cur7= Crt7/Dr       | Crt7              |
| Dietas                                                                                                      | Pr8         | Cr8= Pr8/Cur8 | Cur8= Crt8/Dr       | Crt8              |
| Incentivos                                                                                                  | Pr9         | Cr9= Pr9/Cur9 | Cur9= Crt9/Dr       | Crt9              |
| <b>Total</b>                                                                                                |             |               | CurT=Cur1 +...+Cur9 | Crt=Crt1+...+Crt9 |
| Distancia real recorrida: Dr; Precio en Euros; Coste real en Euros; Distancia real recorrida en kilómetros. |             |               |                     |                   |

Tabla 18: costes variables de operación reales en el instante  $T_{x+1}$ .

El siguiente análisis desglosa que parte de las variaciones del coste real provienen de las variaciones del coste unitario o de la distancia recorrida, según muestran las siguientes tablas 18 y 19.

Una vez calculados y/o recopilados el coste unitario planificado, el coste unitario real, la distancia planificada y real por tipo de vehículo, se calculan los datos de la siguiente tabla 18.

| Tipo de vehículo | Nº de vehículos | Coste unitario planificado | Coste unitario real | Distancia planificada | Distancia real |
|------------------|-----------------|----------------------------|---------------------|-----------------------|----------------|
| A                | n1              | CupTA                      | CurTA               | DpA                   | DrA            |
| B                | n2              | CupTB                      | CurtB               | DpB                   | DrB            |
| ....             | ....            | ....                       | ....                | ....                  | ....           |
| N                | nn              | CupTN                      | CurTN               | DpN                   | DrN            |

Tabla 18: principales variables por tipo de vehículo en el periodo  $P_x$ .

Con los resultados de la tabla 18 obtenemos los datos de la tabla 19.

| Tipo de vehículo                                                                                                               | Costes planificados | Costes reales       | Desviación total | Desviación coste unitario | Desviación distancia   |
|--------------------------------------------------------------------------------------------------------------------------------|---------------------|---------------------|------------------|---------------------------|------------------------|
| A                                                                                                                              | $CTPA=CupTA*DpA$    | $CTRA=CurTA*DrA$    | $DTA=CTRA-CTPA$  | $DTCUA=(CurTA-CupTA)*DrA$ | $DTDA=(DrA-DpA)*CupTA$ |
| B                                                                                                                              | $CTPB=CupTB*DpB$    | $CTRB=CurTB*DrB$    | $DTB=CTRB-CTPB$  | $DTCUB=(CurTB-CupTB)*DrB$ | $DTDB=(DrB-DpB)*CupTB$ |
| ....                                                                                                                           | ....                | ....                | ....             | ....                      | ....                   |
| N                                                                                                                              | $CTPN=CupTN*DpN$    | $CTRN=CurTN*DrN$    | $DTN=CTRN-CTPN$  | $DTCUN=(CurTN-CupTN)*DrN$ | $DTDN=(DrN-DpN)*CupTN$ |
| Total                                                                                                                          | $CTP=CTPA+...+CTPN$ | $CTR=CTRA+...+CTRN$ | $DT=DTA+...+DTN$ | $DTCU=DTCUA+...+DTCUN$    | $DTD=DTDA+...+DTDN$    |
| CTP= costes totales planificados; CTR= costes totales reales; DT= desviación total entre los costes reales y los planificados; |                     |                     |                  |                           |                        |
| DTCU= desviación debida al coste unitario; DTD= desviación debida a la distancia recorrida; DT=DTCU+DTD.                       |                     |                     |                  |                           |                        |

Tabla 19: desviación entre los costes planificados y los reales en el periodo  $P_x$ .

La tabla 19 muestra la desviación total producida para la flota y por tipos de vehículos entre los costes reales y los planificados, así como la desviación producida debida al coste unitario y la distancia recorrida.

El rango de la desviación que se produce entre los costes variables planificados y reales en términos absolutos es mayor cuantos más vehículos y/o costes variables planificados tenga la flota, ya que las cantidades son mayores y por lo tanto tenemos más margen para reducir los costes variables.

En una flota de 50 vehículos la desviación en términos absolutos de los costes variables planificados y reales serán menores que para una flota de 500 vehículos.

Si analizamos y representamos en un gráfico estas desviaciones en términos absolutos obtendríamos conclusiones erróneas, por lo tanto necesitamos un indicador para medir la desviación de los costes variables de operación independientemente del tamaño de la flota y la cuantía de los costes variables.

El método propuesto es calcular el % de desviación que se produce entre los costes variables reales con los planificados según la tabla 20. Con los resultados de la tabla 19 obtenemos los datos de la tabla 20:

| Tipo de vehículo                                                             | % desviación total | % desviación coste unitario | % desviación distancia |
|------------------------------------------------------------------------------|--------------------|-----------------------------|------------------------|
| Tipo A                                                                       | $(DTA/CTP)*100$    | $(DTCUA/CTP)*100$           | $(DTDA/CTP)*100$       |
| Tipo B                                                                       | $(DTB/CTP)*100$    | $(DTCUB/CTP)*100$           | $(DTDB/CTP)*100$       |
| ...                                                                          | ...                | ...                         | ...                    |
| Tipo N                                                                       | $(DTN/CTP)*100$    | $(DTCUN/CTP)*100$           | $(DTDN/CTP)*100$       |
| Total                                                                        | $(DT/CTP)*100$     | $(DTCU/CTP)*100$            | $(DTD/CTP)*100$        |
| % desviación total= % desviación entre los costes reales y los planificados; |                    |                             |                        |

Tabla 20: % desviación entre los costes planificados y los reales en el periodo  $P_x$ .

La tabla 20 muestra el porcentaje de desviación total producida para la flota entre los costes reales y los planificados, así como el porcentaje de desviación producida por el coste unitario y la distancia recorrida por tipo de vehículo.

Con los datos obtenidos hay que realizar un análisis en profundidad con los siguientes objetivos:

- Conocer las causas de las desviaciones en los costes variables de operación.
- Priorizar las medidas a tomar en aquellos tipos de vehículos, conductores y partidas que nos están causando las mayores desviaciones.
- Identificar que vehículos nos están provocando las desviaciones.

El análisis hay que realizarlo desde lo más genérico a lo más específico según el siguiente gráfico 28 para los costes variables de operación.

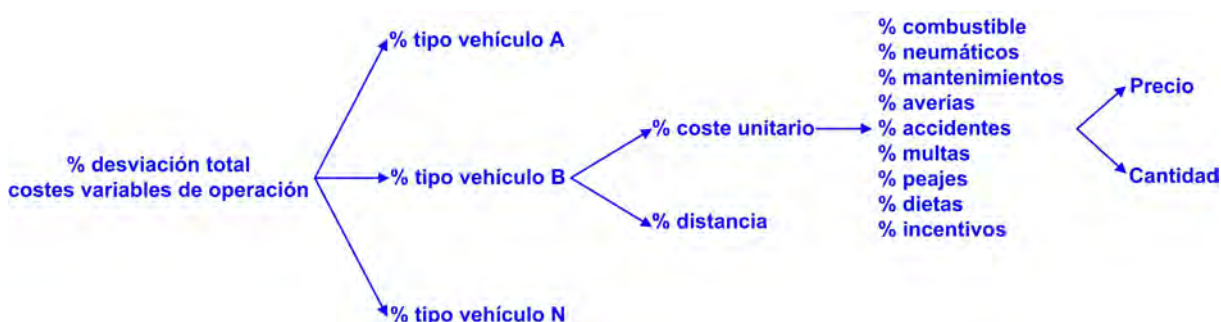


Gráfico 28: estructura de las desviaciones en los costes variables de operación.

El primer paso es conocer el % de desviación de los costes variables de operación por tipo de vehículo, el segundo paso es conocer el % de desviación debido al coste unitario y a la distancia por tipo de vehículo, utilizando la tabla 20.

Conociendo la desviación producida por la distancia recorrida hay que identificar que vehículos han realizado más kilómetros que los planificados, estudiar la causa que lo ha provocado y tomar las medidas adecuadas para que no se vuelva a producir.

En aquellos vehículos que han recorrido menos kilómetros de los planificados hay que identificar la causa que lo ha provocado con el objetivo de aplicarlo al resto de vehículos de la flota como una buena práctica y/o modelo a seguir.

El tercer paso es conocer el desglose de la desviación producida por los costes unitarios en sus diferentes partidas por tipo de vehículo, según muestra la tabla 21:

| Concepto                                                      | % desviación                                                 |
|---------------------------------------------------------------|--------------------------------------------------------------|
| Combustible                                                   | $((\text{Cur1}-\text{Cup1}) * \text{Dr} * 100) / \text{CTP}$ |
| Neumáticos                                                    | $((\text{Cur2}-\text{Cup2}) * \text{Dr} * 100) / \text{CTP}$ |
| Mantenimientos                                                | $((\text{Cur3}-\text{Cup3}) * \text{Dr} * 100) / \text{CTP}$ |
| Averías                                                       | $((\text{Cur4}-\text{Cup4}) * \text{Dr} * 100) / \text{CTP}$ |
| Accidentes                                                    | $((\text{Cur5}-\text{Cup5}) * \text{Dr} * 100) / \text{CTP}$ |
| Multas                                                        | $((\text{Cur6}-\text{Cup6}) * \text{Dr} * 100) / \text{CTP}$ |
| Peajes                                                        | $((\text{Cur7}-\text{Cup7}) * \text{Dr} * 100) / \text{CTP}$ |
| Dietas                                                        | $((\text{Cur8}-\text{Cup8}) * \text{Dr} * 100) / \text{CTP}$ |
| Incentivos                                                    | $((\text{Cur9}-\text{Cup9}) * \text{Dr} * 100) / \text{CTP}$ |
| Dr es la distancia real total recorrida por tipo de vehículo. |                                                              |

Tabla 21: % de desviación de los costes unitarios

Con los datos obtenidos de la tabla 21, conocemos que costes unitarios tienen desviaciones positivas, negativas o no tienen. En aquellos costes unitarios con desviaciones positivas hay que identificar el motivo que la provoco, si es por los precios, la cantidad o ambos a la vez tal como muestra la tabla 17, e identificar que vehículos han provocado esta desviación y tomar las medidas adecuadas para que no se vuelvan a producir.

En aquellos costes unitarios que tienen desviaciones negativas hay que identificar las causas y los vehículos que las han provocado con el objetivo de aplicarlo al resto de vehículos de la flota como una buena práctica y/o modelo a seguir.

Los tiempos totales de operación y las velocidades medias por tipo de vehículo son de gran utilidad para analizar los resultados obtenidos, la tablas 22 y 23 muestran los tiempos totales y las velocidades medias planificadas y reales en los instantes  $T_x$  y  $T_{x+1}$  para el periodo  $P_x$  por tipo de vehículo.

| Tipo de vehículo                                                                                      | Tiempo planificado      | Tiempo real             | Diferencia             | % desviación                |
|-------------------------------------------------------------------------------------------------------|-------------------------|-------------------------|------------------------|-----------------------------|
| A                                                                                                     | $T_{pa}$                | $T_{ra}$                | $D_{ta}=T_{ra}-T_{pa}$ | $(D_{ta}/T_{pa}) \cdot 100$ |
| B                                                                                                     | $T_{pb}$                | $T_{rb}$                | $D_{tb}=T_{rb}-T_{pb}$ | $(D_{tb}/T_{pb}) \cdot 100$ |
| ...                                                                                                   | ...                     | ...                     | ...                    | ...                         |
| N                                                                                                     | $T_{pn}$                | $T_{rn}$                | $D_{tn}=T_{rn}-T_{pn}$ | $(D_{tn}/T_{pn}) \cdot 100$ |
| Total                                                                                                 | $TTP=T_{pa}+...+T_{pn}$ | $TTR=T_{ra}+...+T_{rn}$ | $DTT=TTR-TTP$          | $(DTT/TTP) \cdot 100$       |
| Tiempo planificado, es la suma de los tiempos planificados de todos vehículos para el periodo $P_x$ . |                         |                         |                        |                             |
| Tiempo real, es la suma de los tiempos reales de todos los vehículos para el periodo $P_x$ .          |                         |                         |                        |                             |

Tabla 22: tiempos reales y planificados de operación por tipo de vehículo en el periodo  $P_x$ .

La tabla 23 muestra las velocidades medias planificadas y reales en los instantes  $T_x$  y  $T_{x+1}$  para el periodo  $P_x$  por tipo de vehículo.

| Tipo de vehículo | Distancia planificada   | Velocidad media planificada | Distancia real          | Velocidad media real    | Diferencia               | % diferencia                 |
|------------------|-------------------------|-----------------------------|-------------------------|-------------------------|--------------------------|------------------------------|
| A                | $D_{pa}$                | $V_{mpa}=D_{pa}/T_{pa}$     | $D_{ra}$                | $V_{mra}=D_{ra}/T_{ra}$ | $D_{va}=V_{mra}-V_{mpa}$ | $(D_{va}/V_{mpa}) \cdot 100$ |
| B                | $D_{pb}$                | $V_{mpb}=D_{pb}/T_{pb}$     | $D_{rb}$                | $V_{mrb}=D_{rb}/T_{rb}$ | $D_{vb}=V_{mrb}-V_{mpb}$ | $(D_{vb}/V_{mpb}) \cdot 100$ |
| ...              | ...                     | ...                         | ...                     | ...                     | ...                      | ...                          |
| N                | $D_{pn}$                | $V_{mpn}=D_{pn}/T_{pn}$     | $D_{rn}$                | $V_{mrn}=D_{rn}/T_{rn}$ | $D_{vn}=V_{mrn}-V_{mpn}$ | $(D_{vn}/V_{mpn}) \cdot 100$ |
| Total            | $DPT=D_{pa}+...+D_{pn}$ | $VMPT=DPT/TPT$              | $DRT=D_{ra}+...+D_{rn}$ | $VRPT=DRT/TTR$          | $DVT=VRPT-VMPT$          | $(DVT/VMPT) \cdot 100$       |

Tabla 23: velocidades medias planificadas y reales por tipo de vehículo en el periodo  $P_x$

### 3.2.1. Caso práctico

Se desarrolla un ejemplo práctico en una flota con rutas planificadas en tres periodos de tiempo según el gráfico 29.

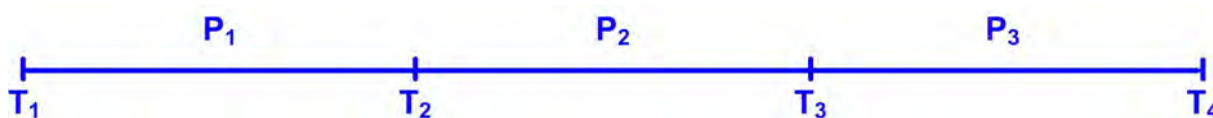


Gráfico 29: ejemplo práctico considerando tres periodos

Consideramos una flota que realiza transporte y distribución de mercancía compuesta por dos tipos de vehículos que utilizan el mismo combustible:

- El tipo A es un vehículo pesado que realiza el transporte de mercancías entre la fabrica donde recoge el producto y los almacenes principales de la organización, realiza rutas interurbanas y de la larga distancia mayoritariamente por autovías y autopistas.
- El tipo B es un vehículo ligero dedicado a la distribución entre los almacenes y el cliente final, y realiza rutas urbanas e interurbanas de media-corta distancia.

Las tablas y gráficos de los siguientes epígrafes muestran las condiciones iniciales y los resultados de cada periodo, en el anexo están desarrollados todos los datos iniciales y resultados para cada periodo.

### 3.2.2. Periodo 1

Para el periodo  $P_1$  las condiciones planificadas en el instante  $T_1$  y las reales en el instante  $T_2$  son las mostradas en la tabla 24.

| Tipo de vehículo | Nº vehículos | Costes unitarios planificados T1 | Costes unitarios reales T2 | Distancia planificada T1 | Distancia real T2 |
|------------------|--------------|----------------------------------|----------------------------|--------------------------|-------------------|
| A                | 20           | 0,502                            | 0,52                       | 200.000                  | 201.000           |
| B                | 80           | 0,195                            | 0,193                      | 600.000                  | 680.000           |
| Total            | 100          |                                  |                            | 800.000                  | 881.000           |

Tabla 24: datos planificados y reales en el periodo  $P_1$

Con los datos de la tabla 24 y la metodología propuesta obtenemos los datos mostrados en la tabla 25.

| Tipo de vehículo | % desviación total | % desviación costes unitarios | % desviación distancia |
|------------------|--------------------|-------------------------------|------------------------|
| A                | 1,957%             | 1,726%                        | 0,231%                 |
| B                | 6,579%             | -0,605%                       | 7,184%                 |
| Total            | 8,536%             | 1,121%                        | 7,415%                 |

Tabla 25: % desviaciones de los costes reales respecto a los planificados en el periodo P<sub>1</sub>

El gráfico 30 muestra el % de desviación desglosado por tipo de vehículo, coste unitario, distancia y partida.

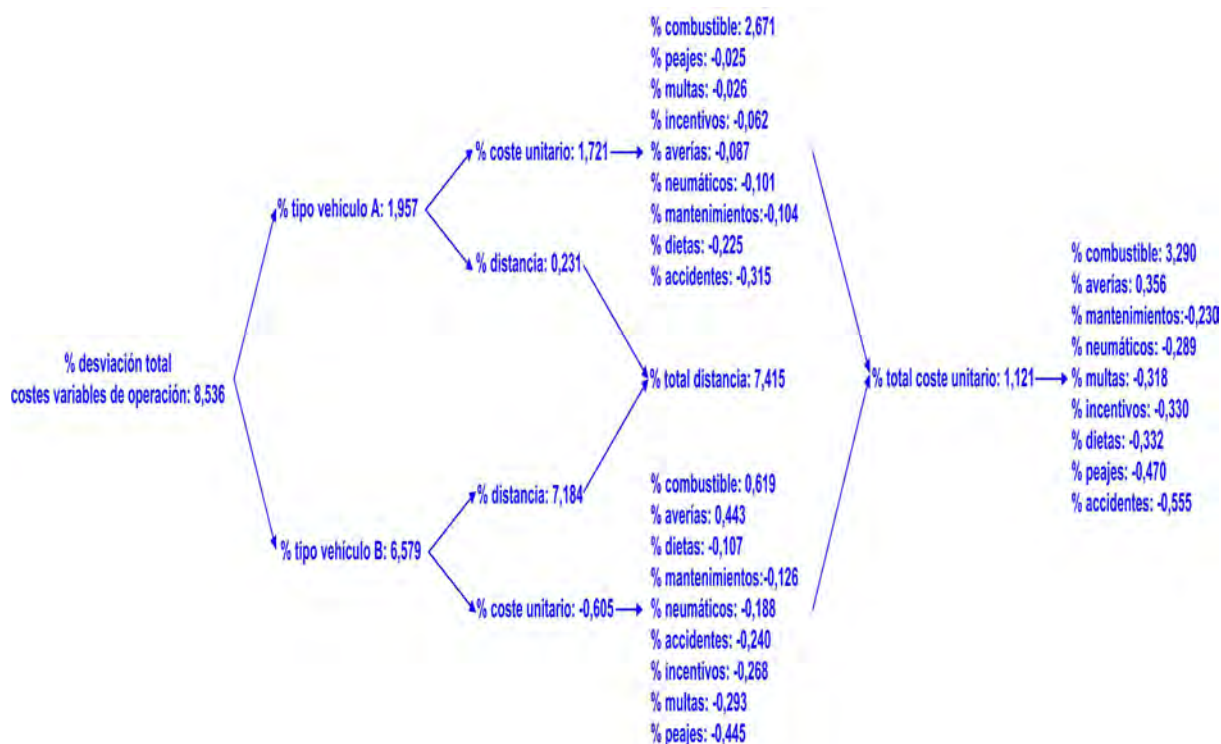


Gráfico 30: % desviación total costes variables de operación en el periodo P<sub>1</sub>

En el primer periodo hemos obtenido una desviación positiva del 8,536% de los costes variables de operación, debido principalmente al tipo de vehículo B y la distancia recorrida.

Analizando el tipo de vehículo B, la mayor desviación corresponde a la distancia recorrida, por que hemos realizado más kilómetros que los planificados. La desviación en el coste

unitario ha tenido una ligera mejoría, aunque en el concepto de combustible y averías han empeorado ligeramente. En el caso del combustible es debido a un considerable incremento en su consumo (tablas 26 y 27) por que la velocidad media (tabla 28) se ha incrementado ligeramente, y en el caso de las averías debido a que los precios se han incrementado y el kilometraje para que se produzca una avería ha decrecido (tablas 26 y 27).

Analizando el tipo de vehículo A, la mayor desviación corresponde al coste unitario, debido al incremento en el consumo de combustible, por que la velocidad media (tabla 28) se ha incrementado considerablemente, en el resto de partidas se han producido ligeras mejoras que compensan una parte el incremento del consumo de combustible. Se puede considerar que no ha habido desviación en la distancia al ser esta de pequeña cuantía.

La principal conclusión que obtenemos para este primer periodo es la siguiente:

- Hemos obtenido un incremento de los costes variables de operación debido principalmente a la mayor distancia recorrida por el tipo de vehículo B.

La organización tiene que investigar por que se ha producido el incremento de la velocidad de los vehículos del tipo A, y la distancia recorrida por los vehículos del tipo B, así como identificar que vehículos han provocado estos incrementos con el objetivo de tomar las medidas adecuadas para corregir esta situación y no vuelvan a suceder en los sucesivos periodos.

### 3.2.3. Periodo 2

Las condiciones planificadas en el instante  $T_2$  y las reales en el instante  $T_3$  son las mostradas en la tabla 29.

| Tipo de vehículo | Nº de vehículos | Costes unitarios planificados T2 | Costes unitarios reales T3 | Distancia planificada T2 | Distancia real T3 |
|------------------|-----------------|----------------------------------|----------------------------|--------------------------|-------------------|
| A                | 20              | 0,452                            | 0,456                      | 200.000                  | 198.000           |
| B                | 80              | 0,179                            | 0,179                      | 600.000                  | 630.000           |
| Total            | 100             |                                  |                            | 800.000                  | 828.000           |

Tabla 29: datos planificados y reales plazo en el periodo  $P_2$

Con los datos de la tabla 29 y la metodología propuesta, obtenemos los datos mostrados en la tabla 30.



| Tipo de vehículo | % desviación total | % desviación costes unitarios | % desviación distancia |
|------------------|--------------------|-------------------------------|------------------------|
| A                | 0,013%             | 0,470%                        | -0,457%                |
| B                | 2,789%             | 0,073%                        | 2,716%                 |
| Total            | 2,803%             | 0,543%                        | 2,259%                 |

Tabla 30: % desviaciones de los costes planificados en el corto plazo en el periodo P<sub>2</sub>

El gráfico 31 muestra el % de desviación desglosado por tipo de vehículo, coste unitario, distancia y partida.

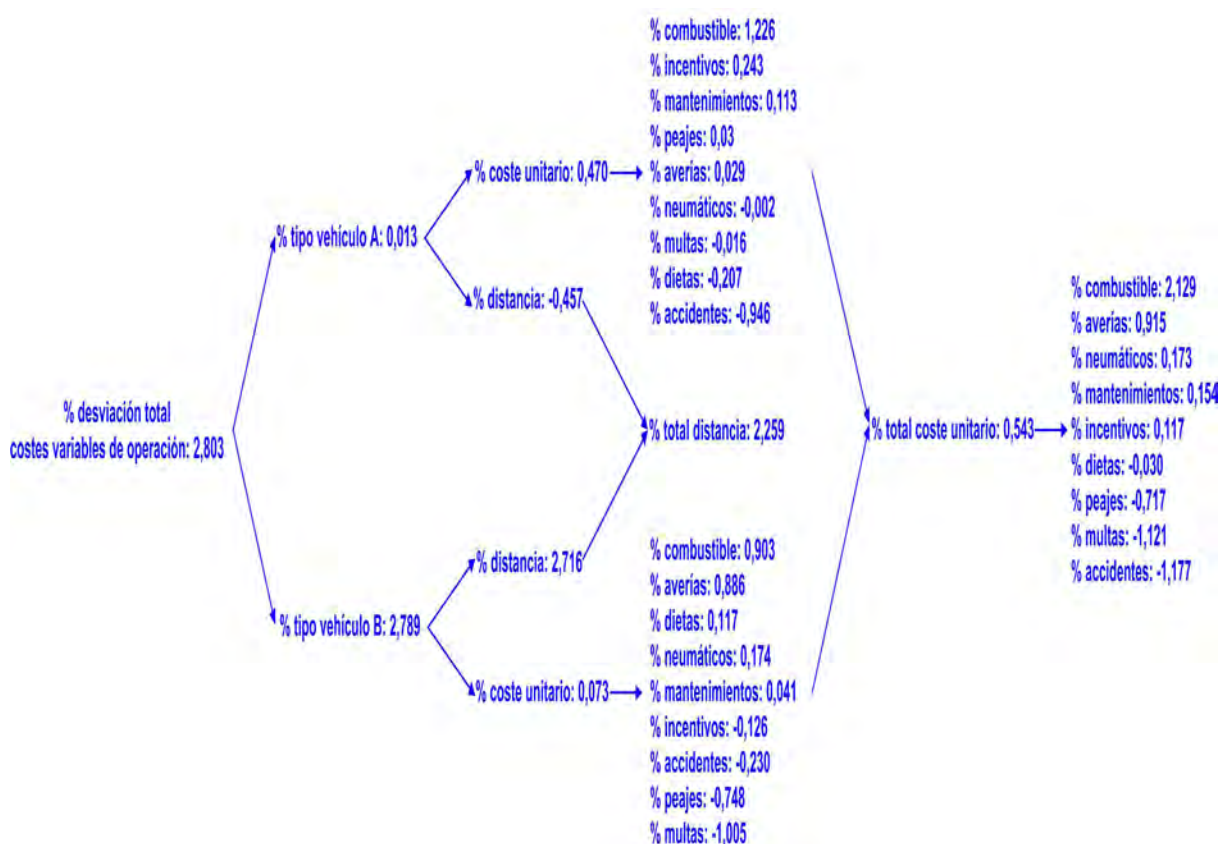


Gráfico 31: % desviación total costes variables de operación en el corto plazo en el periodo P<sub>2</sub>

En el segundo periodo hemos obtenido una desviación positiva del 2,803% de los costes variables de operación, debido principalmente al tipo de vehículo B y la distancia recorrida.

Analizando el tipo de vehículo B, la mayor desviación corresponde a la distancia recorrida, por que hemos realizado más kilómetros que los planificados. En el coste unitario

prácticamente no hemos tenido desviación, aunque en los conceptos de combustible y averías han empeorado ligeramente (tablas 31 y 32). En el caso del combustible es debido a un ligero incremento en el precio real del combustible provocado a que una parte de los vehículos han repostado combustible en estaciones de servicio, en vez de realizarlo en nuestro propio depósito de combustible, y a un ligero incremento en la velocidad media (tabla 33). En el caso de las averías debido a que los precios se han incrementado y el kilometraje para que se produzca una avería ha decrecido (tablas 31 y 32). Hay que recalcar una ligera mejoría en las multas de tráfico debido a que la frecuencia de ocurrencia ha aumentado ligeramente (tablas 31 y 32).

Analizando el tipo de vehículo A, prácticamente no hay tenido ninguna desviación respecto a lo planificado. En el coste unitario prácticamente no ha tenido desviación, aunque en el concepto de combustible ha empeorado ligeramente debido a un ligero incremento en el precio real del combustible provocado a que una parte de los vehículos han repostado combustible en estaciones de servicio, en vez de realizarlo en nuestro propio depósito de combustible y a un ligero incremento en la velocidad media (tabla 33). Hay que recalcar una ligera mejoría en los accidentes de tráfico debido a que la frecuencia de ocurrencia ha aumentado ligeramente (tablas 34 y 35).

Las conclusiones que obtenemos para este segundo periodo son las siguientes:

- Hemos obtenido un ligero incremento de los costes variables de operación debido principalmente a la mayor distancia recorrida por el tipo de vehículo B.

La organización tiene que investigar por que se ha producido el ligero incremento de la distancia recorrida de los por los vehículos del tipo B, así como identificar que vehículos han provocado estos incrementos con el objetivo de tomar las medidas adecuadas para corregir esta situación y no vuelvan a suceder en los sucesivos periodos.

#### *3.2.4. Periodo 3*

Debido a que nuestro servicio tiene mayor demanda y tenemos que realizar más rutas de reparto, hemos adquirido tres vehículos del tipo B y uno del tipo A.

Las condiciones planificadas en el instante  $T_3$  y las reales en el instante  $T_4$  son las mostradas en la tabla 36.

| Tipo de vehículo | Nº de vehículos | Costes unitarios planificados T3 | Costes unitarios reales T4 | Distancia planificada T3 | Distancia real T4 |
|------------------|-----------------|----------------------------------|----------------------------|--------------------------|-------------------|
| A                | 23              | 0,387                            | 0,386                      | 207.500                  | 199.500           |
| B                | 81              | 0,147                            | 0,146                      | 614.000                  | 605.000           |
| Total            | 104             |                                  |                            | 821.500                  | 804.500           |

Tabla 36: datos planificados y reales en el periodo  $P_3$

Con los datos de la tabla 36 y la metodología propuesta obtenemos los siguientes datos mostrados en la tabla 37.

| Tipo de vehículo | % desviación total | % desviación costes unitarios | % desviación distancia |
|------------------|--------------------|-------------------------------|------------------------|
| A                | -1,980%            | -0,166%                       | -1,814%                |
| B                | -1,160%            | -0,383%                       | -0,776%                |
| Total            | -3,140%            | -0,550%                       | -2,590%                |

Tabla 37: % desviaciones de los costes planificados en el corto plazo en el periodo  $P_3$

El gráfico 32 muestra el % de desviación desglosado por tipo de vehículo, coste unitario, distancia y partida.

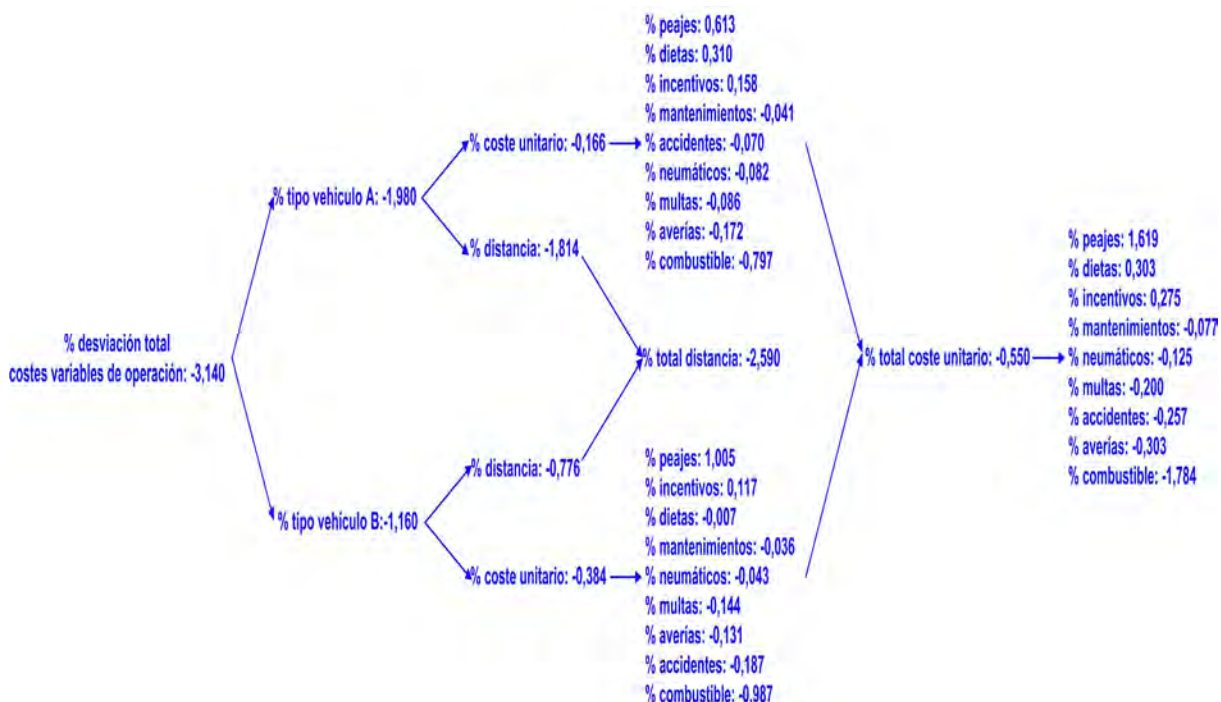


Gráfico 32: % desviación total costes variables de operación en el corto plazo en el periodo  $P_3$

En el tercer periodo en el corto plazo hemos obtenido una desviación negativa del -3,140% de los costes variables de operación, debido principalmente a la distancia recorrida real ha sido menor que la planificada, provocado por un aumento de la utilización de peajes como muestran las tablas 38, 39,40 y 41. La velocidad media ha disminuido ligeramente provocado un decremento del consumo de combustible y un aumento en el tiempo total como muestra la tabla 42.

Las conclusiones que obtenemos en el tercer periodo son las siguientes:

- Hemos obtenido un decremento de los costes variables de operación, principalmente por la reducción en la distancia recorrida por el vehículo del tipo A, debido a la utilización de peajes.

### 3.2.5. Análisis de los resultados

Agrupando los resultados de los tres periodos, obtenemos la tabla 43.

| Periodo | % desviación total | % desviación costes unitarios | % desviación distancia |
|---------|--------------------|-------------------------------|------------------------|
| 1º      | 8,536%             | 1,121%                        | 7,415%                 |
| 2º      | 2,803%             | 0,543%                        | 2,259%                 |
| 3º      | -3,140%            | -0,550%                       | -2,590%                |
| Media   | 2,730%             | 0,372%                        | 3,970%                 |

Tabla 43: % de desviación total costes unitarios en el corto plazo

El gráfico 33 muestra la representación de la desviación de los costes variables de operación, utilizando unos márgenes del 3%.

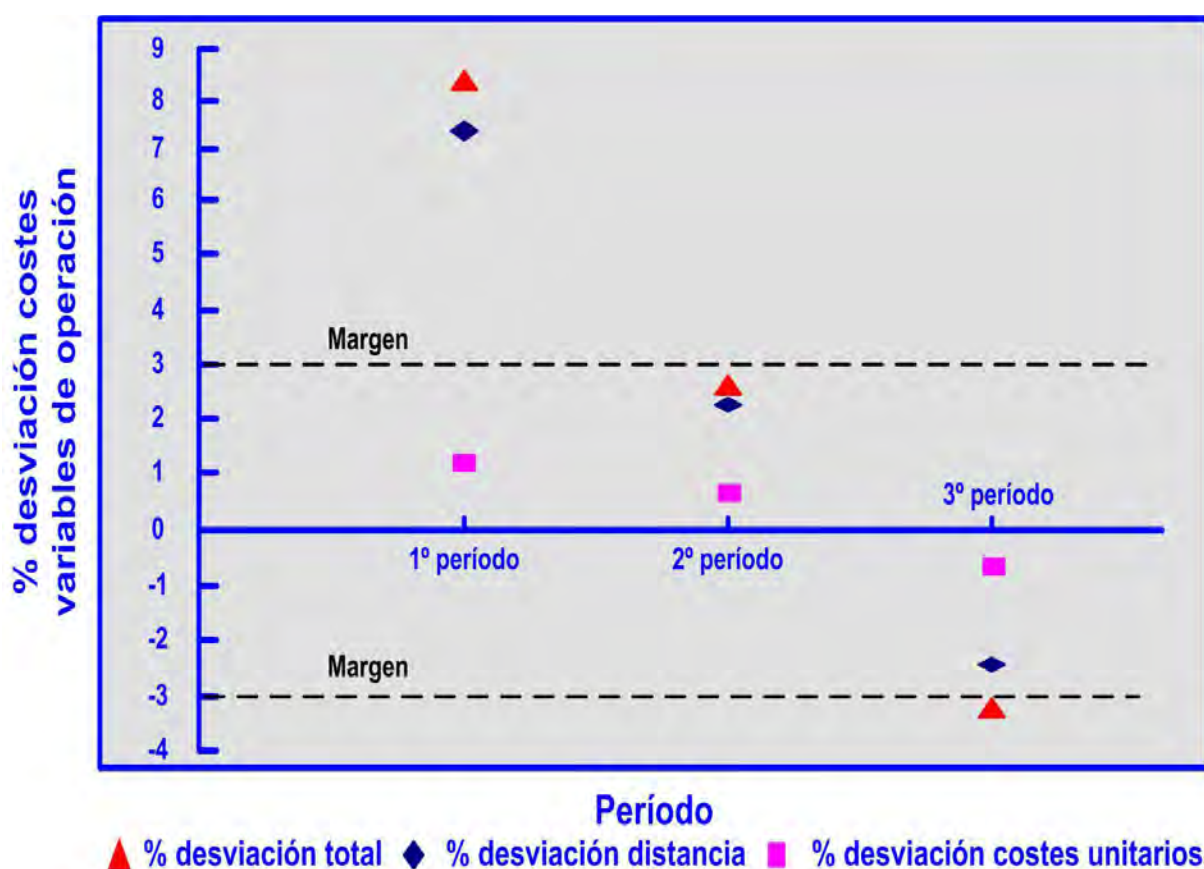


Gráfico 33: desviaciones de los costes variables de operación

En el primer periodo hemos obtenido una desviación positiva de los costes variables de operación debido a la mayor distancia recorrida que la planificada, en el segundo periodo debido a una ligera reducción de los costes unitarios y de la distancia recorrida hemos obtenido una ligera desviación positiva de los costes variables de operación, pero dentro de los márgenes establecidos, y en el tercer periodo debido a la reducción de la distancia recorrida y los costes unitarios hemos obtenido una reducción en los costes variables de operación.

La evolución de las desviaciones de los costes variables, han pasado de ser positiva a negativa en los periodos analizados, debido a que se ha actuado en la reducción de la distancia recorrida, la cual ha sido la variable que más ha influido en los costes variables de operación.

### 3.2.6. Conclusiones

Las principales conclusiones que obtenemos de este caso práctico, y que son aplicables a cualquier tipo de flota son las siguientes:

- Para realizar un control y seguimiento de los costes variables de operación de la flota efectivo, es necesario medir la distancia recorrida y la velocidades medias de los vehículos, por lo que un servicio telemático es imprescindible.
- El coste total unitario permanece constante en varios periodos, si los incrementos en ciertas variables son compensados por los decrementos en otras variables.
- Durante estos tres periodos se han aplicado diferentes medidas para reducir los costes variables de operación; se han identificado los inconvenientes y los vehículos que nos han provocado desviaciones positivas y se han tomado las medidas apropiadas para su control, reducción y mejora, esta es una buena práctica que debe ser realizada en todos los periodos.
- De entre todas las variables involucradas en la gestión de la flota, tenemos que identificar cuales son las que más nos influyen en los costes variables de operación con el objetivo de controlar y priorizar las medidas a realizar en estas variables.
- Hay que priorizar las medidas a tomar para reducir los costes variables de operación, el análisis hay que realizarlo de lo más genérico a lo más específico para identificar las causas que nos están provocando las mayores desviaciones en los costes variables de operación.

Primero tenemos que conocer que tipo de vehículo, segundo si es por los costes unitarios o por la distancia recorrida, tercero si esta provocado por los costes unitarios hay que identificar que conceptos, cuarto una vez identificado estos conceptos si es por el precio, la cantidad o ambas a la vez, así mismo identificar que vehículos y/o conductores nos están provocando las desviaciones tanto las positivas como las negativas.

## 4. CUADRO DE MANDO

---

El cuadro de mando es una herramienta fundamental en la gestión de la flota, por que nos permite conocer, controlar y seguir la información más importante de una forma rápida y sencilla. El cuadro de mando esta compuesto por un conjunto de indicadores que son calculados y/o recopilados del sistema de información de la organización.

Un cuadro de mando muy amplio y con multitud de indicadores puede ser un gran obstáculo en la operativa de la flota por la cantidad de información a recopilar y analizar, por el contrario un cuadro de mando con unos pocos indicadores no suministrará la información necesaria para la gestión de la misma. Por lo tanto la organización tiene que establecer la cantidad de indicadores más apropiados y valiosos que mejor se adapten a las características, operativa, presupuesto y objetivos de la organización.

Para realizar el cuadro de mando de los costes de la flota de vehículos hay que recopilar todas las partidas mostradas en el gráfico 1, así mismo con estos datos podremos desarrollar más cuadros de mando e indicadores en otras áreas de la gestión de la flota.

El cuadro de mando hay que realizarlo de lo más genérico a lo más específico, para ello hay que calcular un indicador general para toda la flota, por tipo de vehículo y el origen del servicio, ya que por ejemplo en el transporte de viajeros existe transporte regular, discrecional etc. con el objetivo de conocer donde están los mayores costes, desviaciones y priorizar donde tomar las medidas adecuadas.

Hay que obtener el indicador cada semana, mes etc. por lo que hay que establecer esta frecuencia y conocer su tendencia en el tiempo, para ello hay que representar la serie del indicador en varios periodos de tiempo.

A continuación se desarrolla un cuadro de mando de costes genérico para cualquier tipo de flota, dependiendo del tipo de flota de vehículos habrá que desarrollar otros indicadores más específicos de cada sector.

Lo más importante del cuadro de mando es la información que suministra, se pueden utilizar multitud de gráficos para representar esta información, por lo que los gráficos utilizados a continuación son un ejemplo de cómo realizar un cuadro de mando, pudiéndose utilizar otros gráficos para representar la misma información. El siguiente cuadro de mando, es para una flota compuesta de tres tipos de vehículos. El vehículo A es un vehículo pesado, el vehículo es C es un vehículo ligero, y el vehículo B es un vehículo entre pesado y ligero.



- Coste total de la flota desglosado según las partidas del gráfico 1 y representando según la tabla 2, además hay que representarlo según los gráficos 34 y 35.

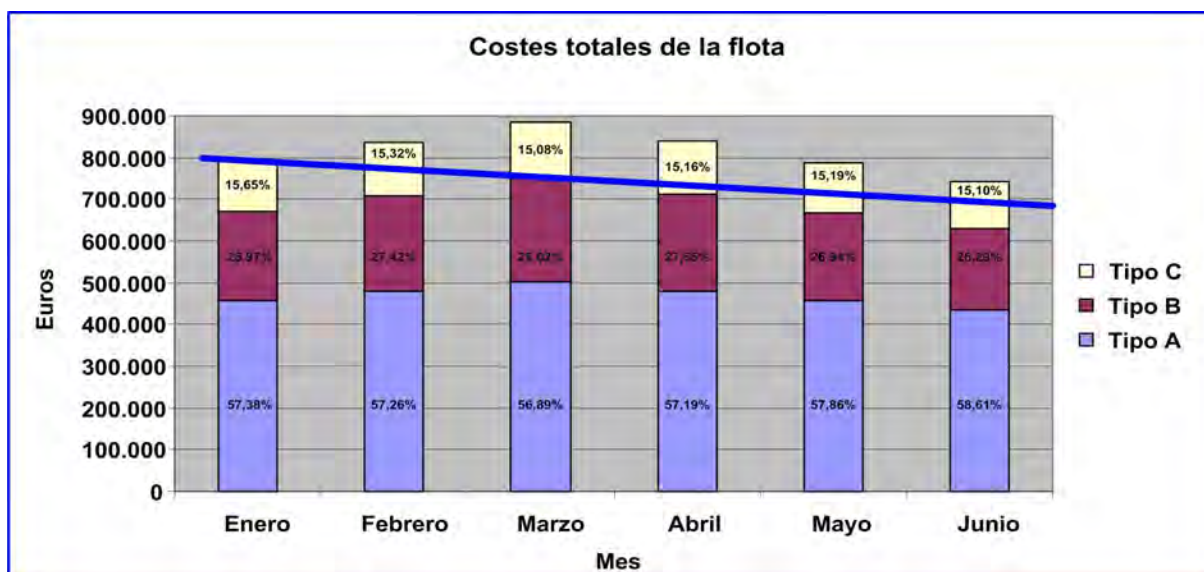


Gráfico 34: costes totales de la flota

El tipo de vehículo A es el mayor coste total de la flota, seguido del tipo B y C. Los costes totales se han incrementado de los meses de enero a marzo, obteniéndose su máximo valor en marzo, para a continuación decrecer, la tendencia de los costes totales es decreciente. El gráfico 35 representa los costes totales desglosados por el tipo de vehículo.

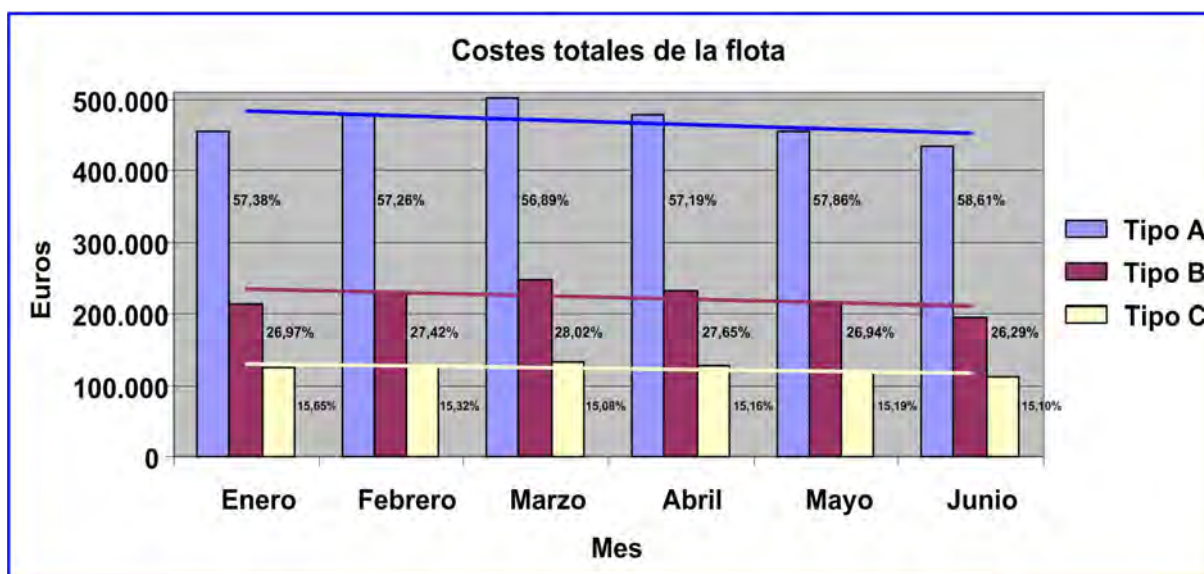


Gráfico 35: costes totales de la flota por tipo de vehículo

Los costes totales de los tres tipos de la flota, se han incrementado de los meses de enero a marzo, obteniéndose su máximo valor en marzo, para a continuación decrecer, la tendencia de los costes totales en los tres tipos de flotas es decreciente.

- $\% \text{ coste de la flota respecto de los costes totales de la organización} = \frac{\text{coste total de la flota}}{\text{costes totales de la organización}}$  según el gráfico 1-tabla 2 / costes totales de la organización.

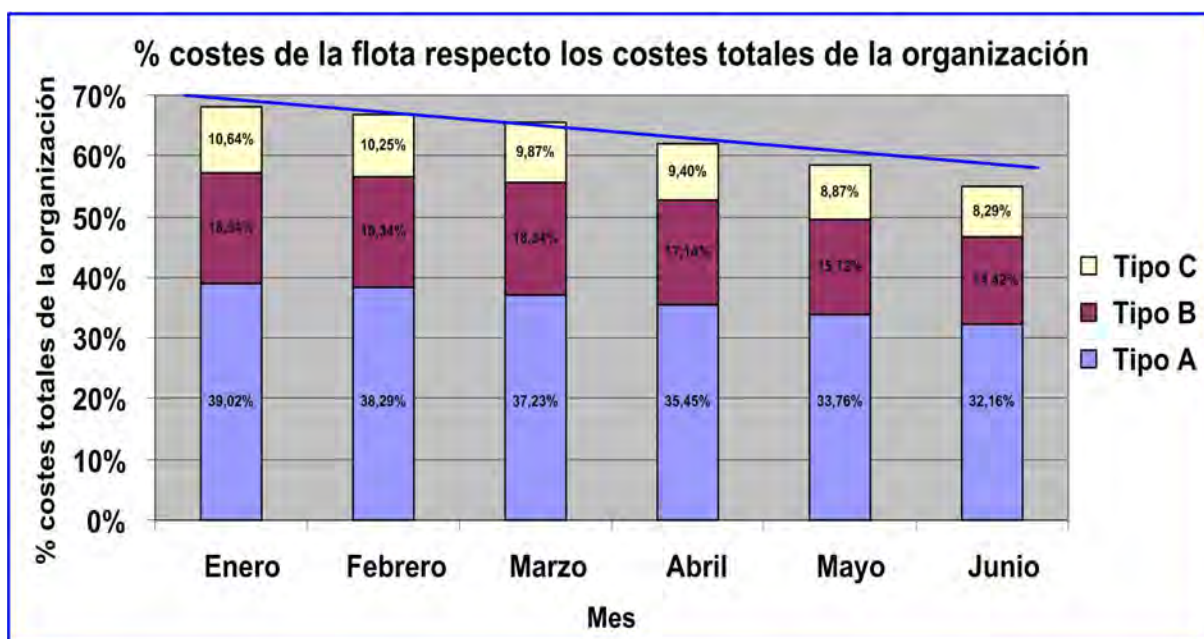


Gráfico 36: % costes de la flota respecto a los costes totales de la organización

El % de los costes totales de la flota respecto a los de la organización ha decrecido durante los meses analizados, y puede ser por varios motivos, como que para el mismo tamaño de flota la organización ha tenido más costes de estructura, o por el contrario el tamaño de la flota y su estructura para gestionarla ha disminuido, en todo caso hay que averiguar por qué ha ocurrido.

- $\% \text{ coste de la flota respecto a la facturación de la compañía} = \frac{\text{costes totales de la flota}}{\text{Facturación de la organización}}$

El gráfico 37 es para flotas de vehículos en los que la facturación total se obtiene utilizando varios tipos de vehículos conjuntamente. En aquellas flotas en los que se obtiene una facturación independiente por cada tipo de vehículo, el indicador es  $\frac{\text{costes totales de cada tipo de vehículo}}{\text{facturación por cada tipo de vehículo}}$ .

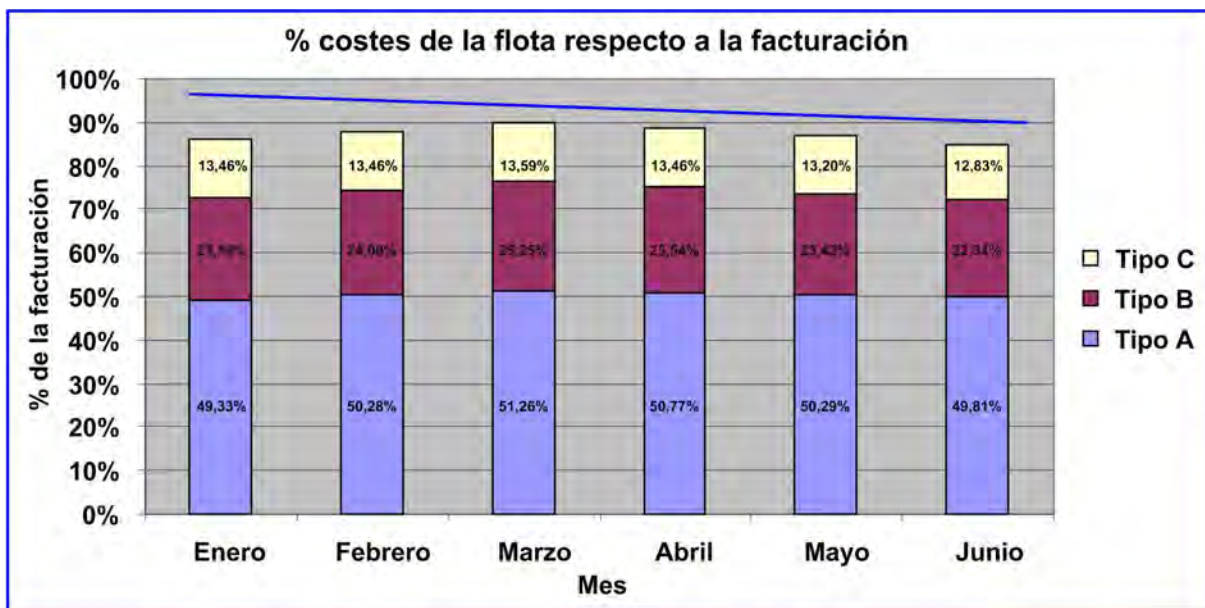


Gráfico 37: % costes de la flota respecto a la facturación

El % de los costes de la flota respecto a la facturación se ha incrementado de los meses de enero a marzo, alcanzado su máximo valor para a continuación decrecer, la tendencia es decreciente.

- % beneficios de la organización respecto a los costes de la flota= beneficios después de impuestos/ costes totales de la flota

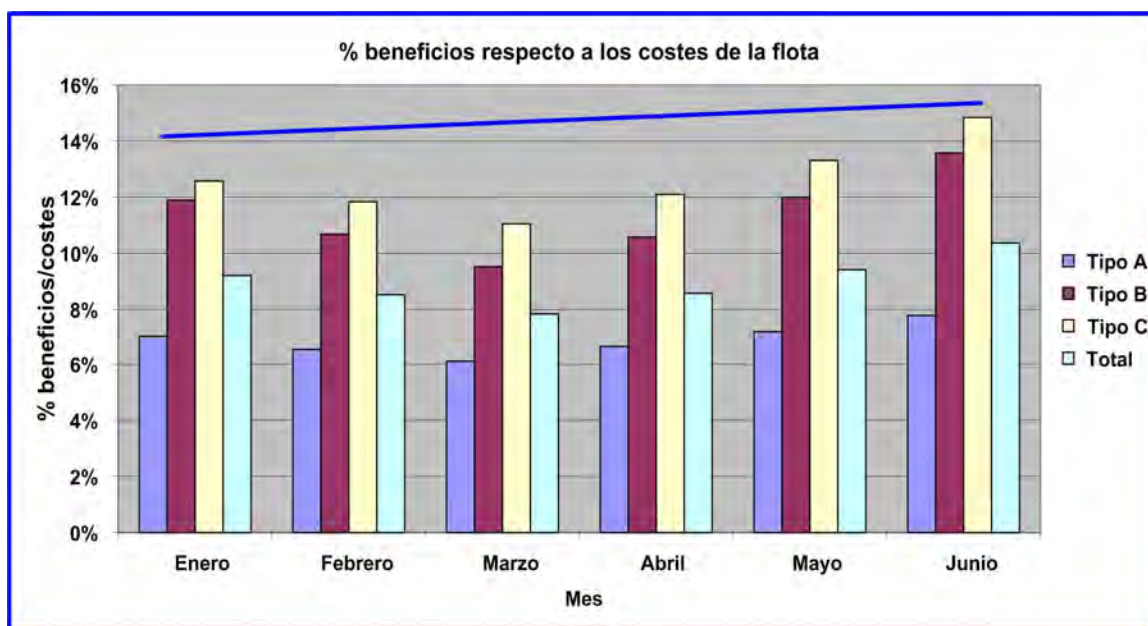


Gráfico 38: % beneficios respecto a los costes de la flota

El % de beneficios respecto a los costes de la flota ha sido decreciente de enero a marzo, obteniéndose el valor mínimo en marzo, para a continuación incrementarse, la tendencia es creciente.

- Hay que representar la evolución de la estructura de costes de la flota de vehículos: costes directos, variables e indirectos según el gráfico 1/tabla 2.

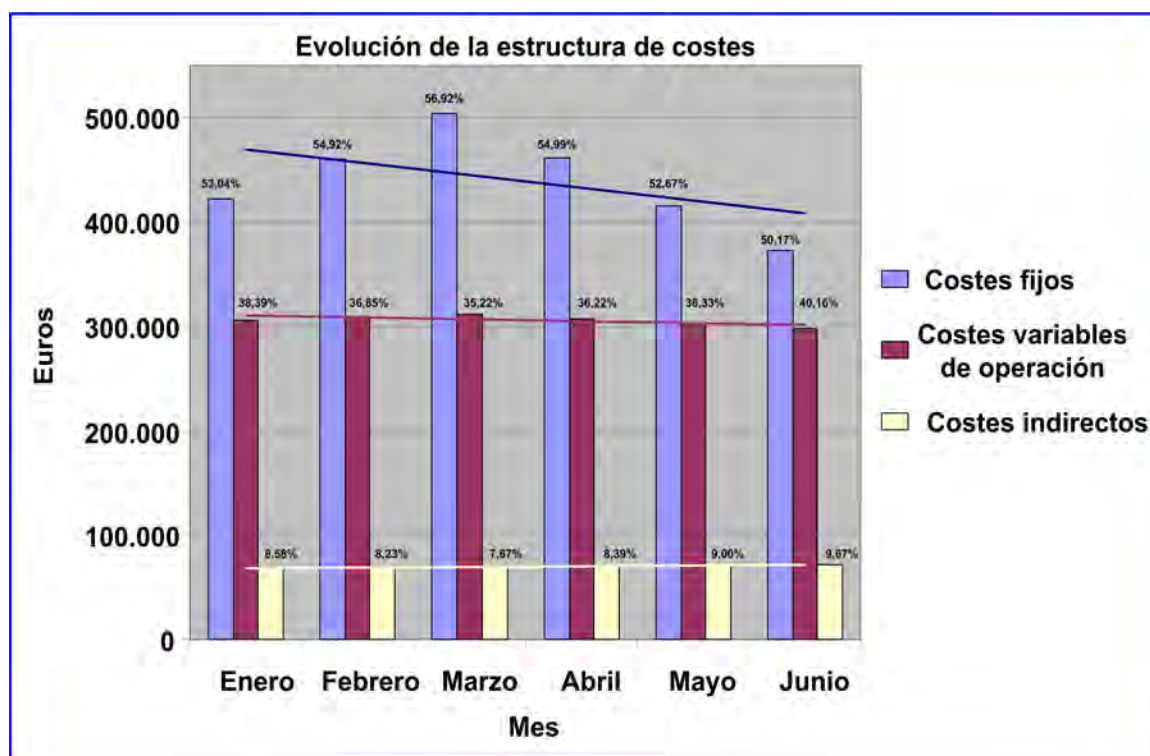


Gráfico 38: evolución de la estructura de costes para toda la flota

Los costes fijos son los mayores costes de la flota seguidos de los costes variables de operación e indirectos. Los costes fijos han sido crecientes de enero a marzo, obteniéndose el máximo en marzo para a continuación a decrecer, y son los responsables del valor máximo de los costes totales obtenidos en el gráfico 34, su tendencia es decreciente.



- Hay que representar la evolución del % de la estructura de costes de la flota de vehículos: costes directos, variables o indirectos / costes totales, según el gráfico 1/tabla 2.

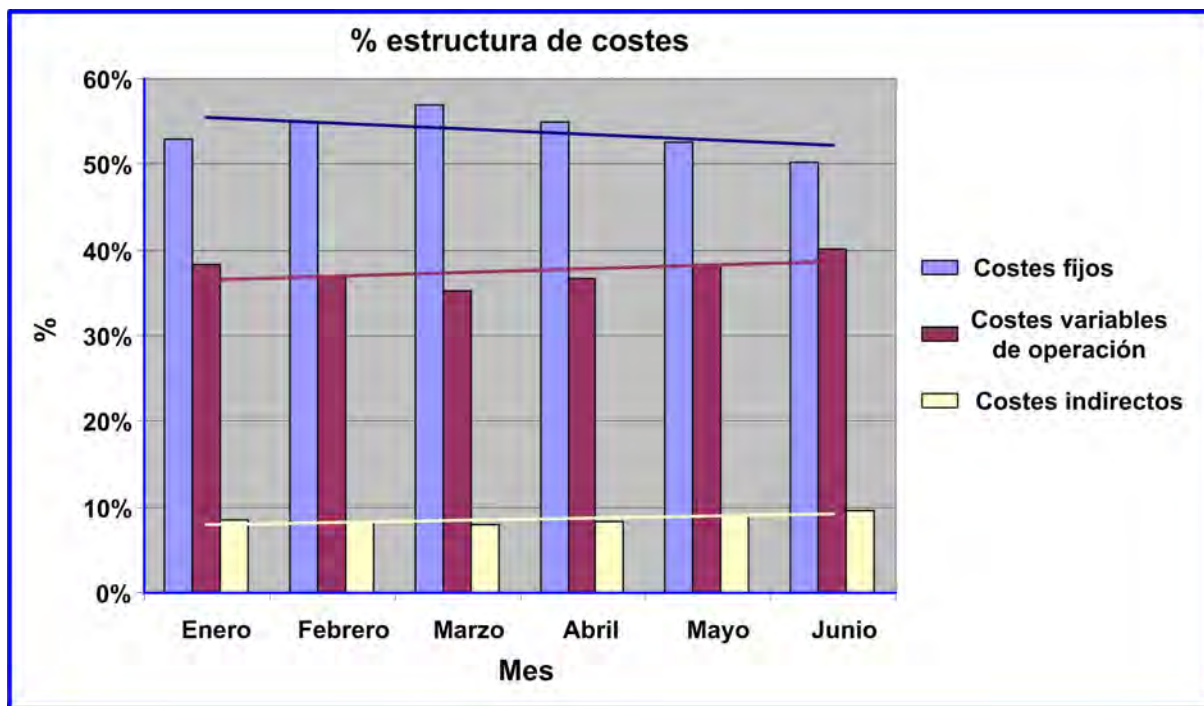


Gráfico 39: evolución de la estructura de costes para toda la flota

Los costes fijos han crecido hasta el mes de marzo y posteriormente ha disminuido, al contrario que los variables de operación que han decrecido hasta alcanzar el mínimo en marzo para posteriormente aumentar. Los costes indirectos prácticamente han permanecido constantes. La tendencia de los costes fijos es decreciente, mientras que los costes variables de operación e indirectos son prácticamente constantes.

Como los costes indirectos son prácticamente constantes, los aumentos o decrementos en el % de los costes fijos han sido compensados por los aumentos o decrementos en los costes variables de operación.

- Las desviaciones producidas en los costes variables de operación del modelo desarrollado en el capítulo 3.

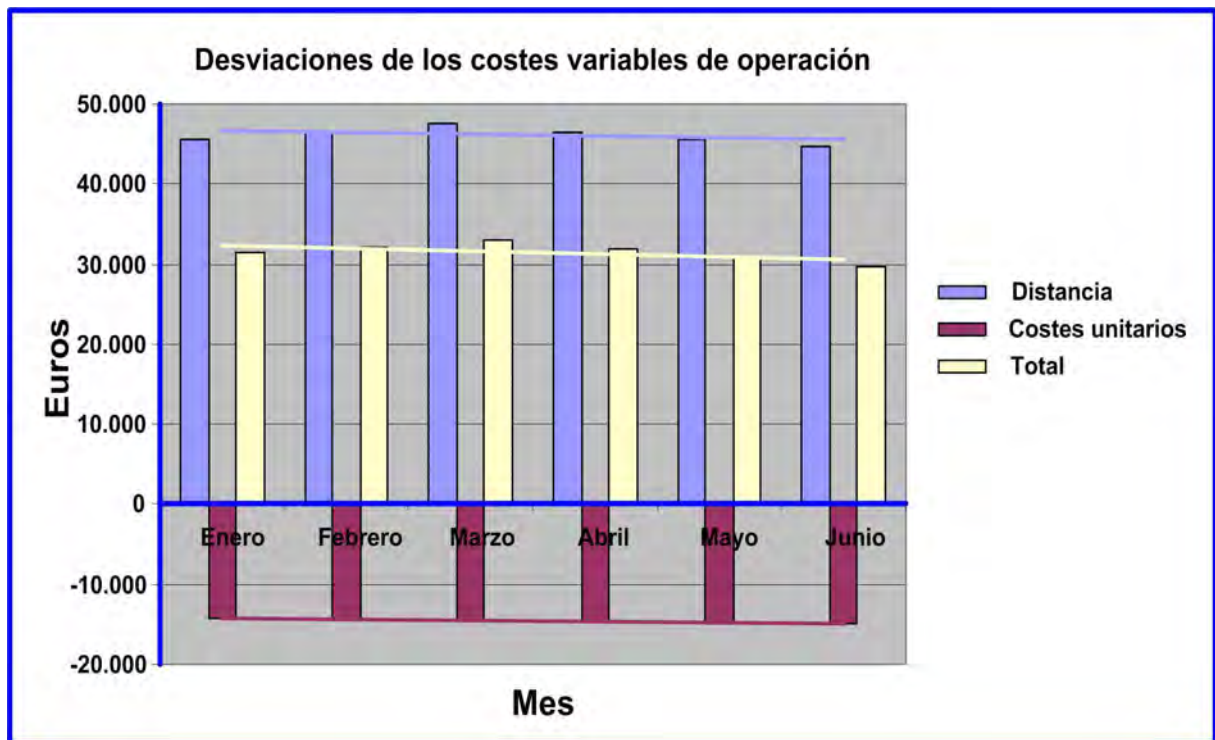


Gráfico 39: desviaciones de los costes variables de operación

Las desviaciones totales en los costes variables de operación han sido positivas debido a las desviaciones positivas en la distancia, pero las desviaciones producidas en los costes unitarios han sido negativas. La tendencia es ligeramente decreciente en el total, la distancia y los costes unitarios.

- % de las desviaciones producidas en los costes variables de operación del modelo desarrollado en el capítulo 3.

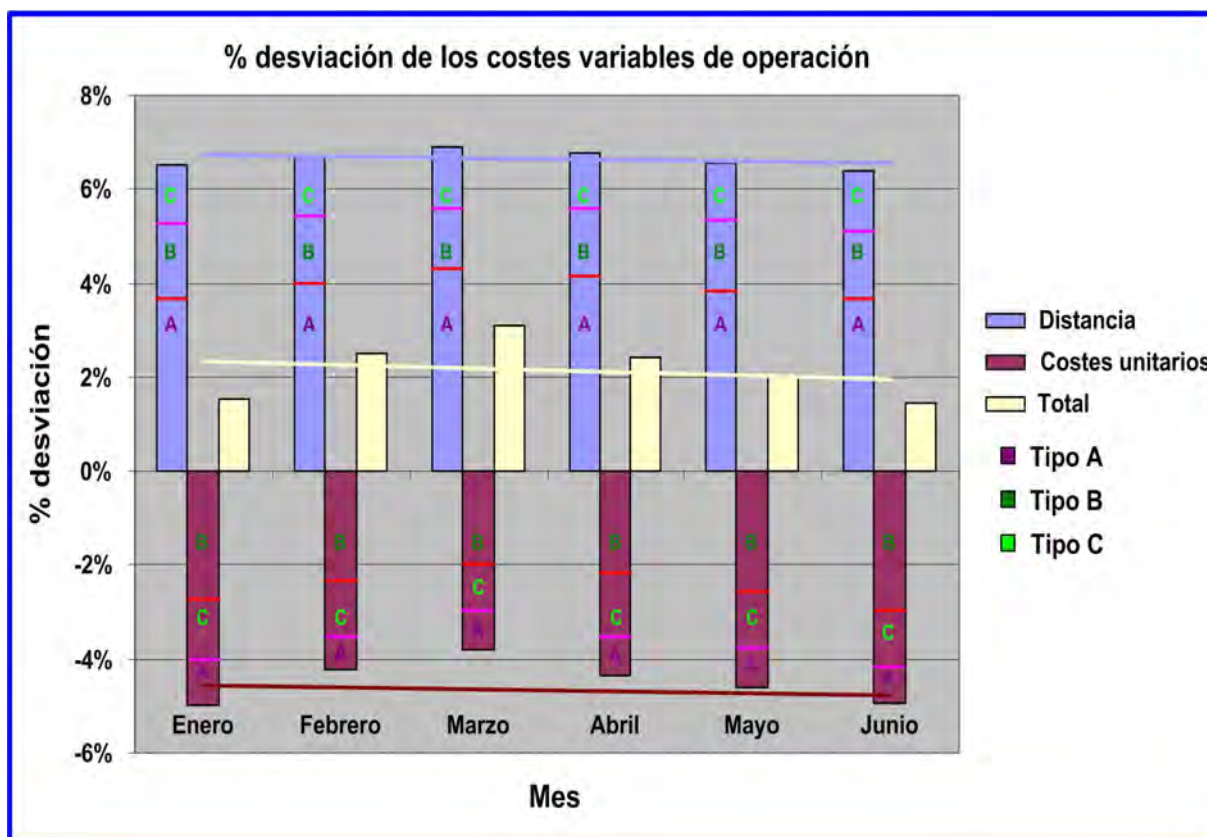


Gráfico 39: % desviaciones de los costes variables de operación

Las desviaciones totales en el % de los costes variables de operación han sido positivas debido a las desviaciones positivas en la distancia causado principalmente por el tipo de vehículo A, pero las desviaciones producidas en los costes unitarios han sido negativas. La tendencia es ligeramente decreciente en el total, la distancia y los costes unitarios.

- Coste hundido, el indicador es: coste fijos + indirectos. Este ratio nos mide el coste hundido utilizemos los vehículos o no.

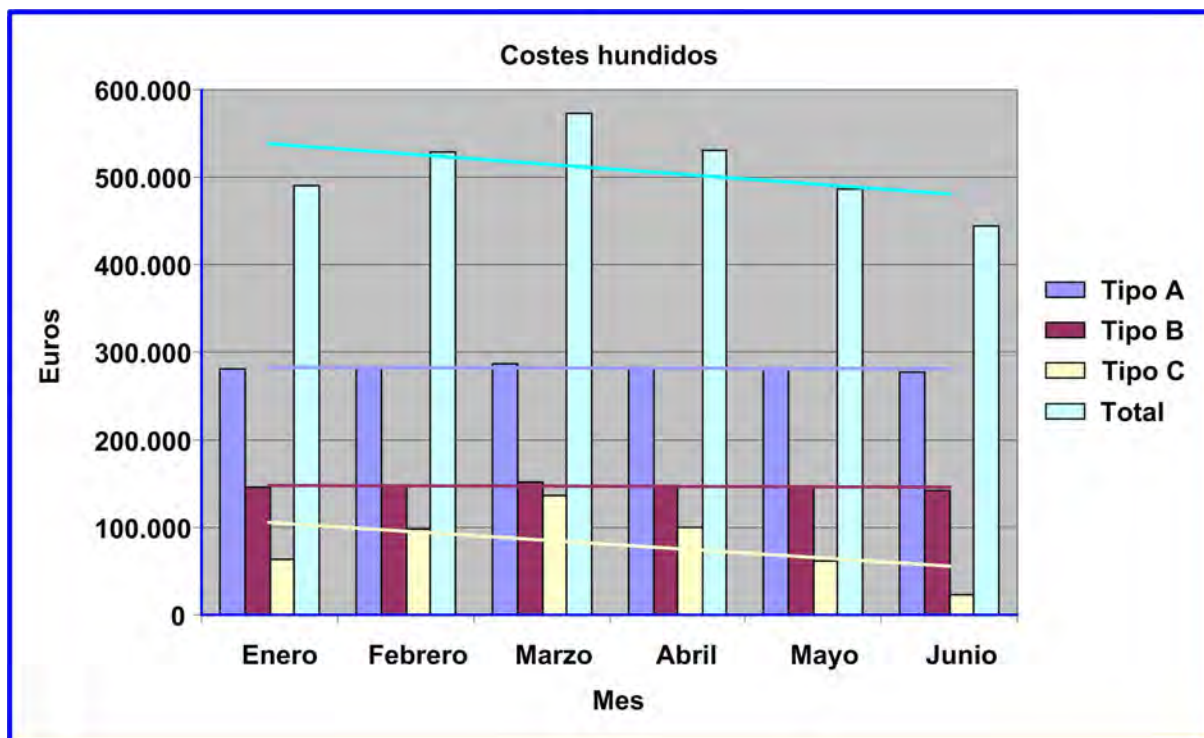


Gráfico 40: evolución de los costes hundidos

La evolución de los costes totales hundidos ha sido creciente hasta el mes de marzo para posteriormente decrecer, este comportamiento ha sido provocado por la flota del tipo C ya que los costes hundidos de los vehículos del tipo A y B han sido prácticamente constantes.



- % Coste hundido, el indicador es:  $\text{coste fijos} + \text{indirectos} / \text{Costes totales}$ .

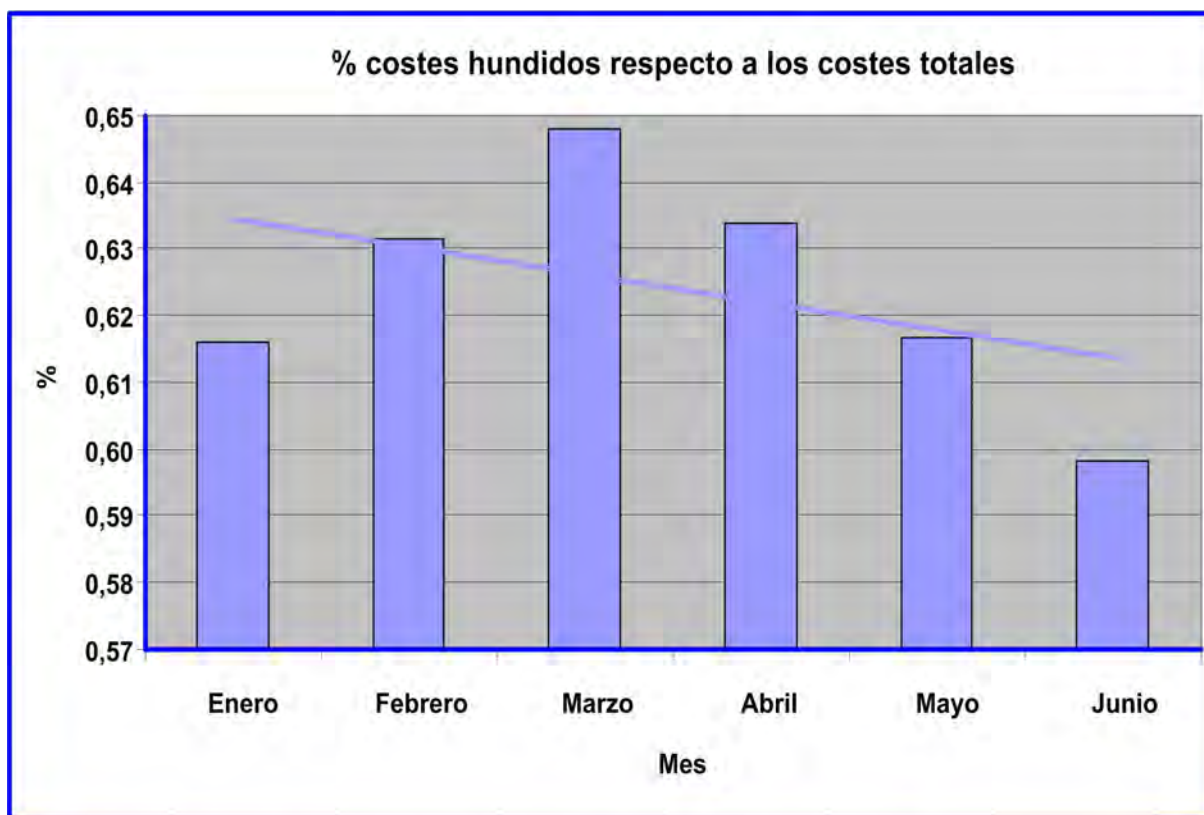


Gráfico 41: evolución del % de los costes hundidos respecto a los costes totales

El % de los costes hundidos respecto los costes totales ha sido creciente hasta el mes de marzo para posteriormente decrecer, la tendencia es decreciente.

- Coste hundido por tiempo según las tablas 2 y 3, el indicador es:  $\text{coste fijos} + \text{indirectos} / (\text{número de días u horas})$ . Este ratio nos mide el coste hundido por día u horas utilizemos los vehículos o no.

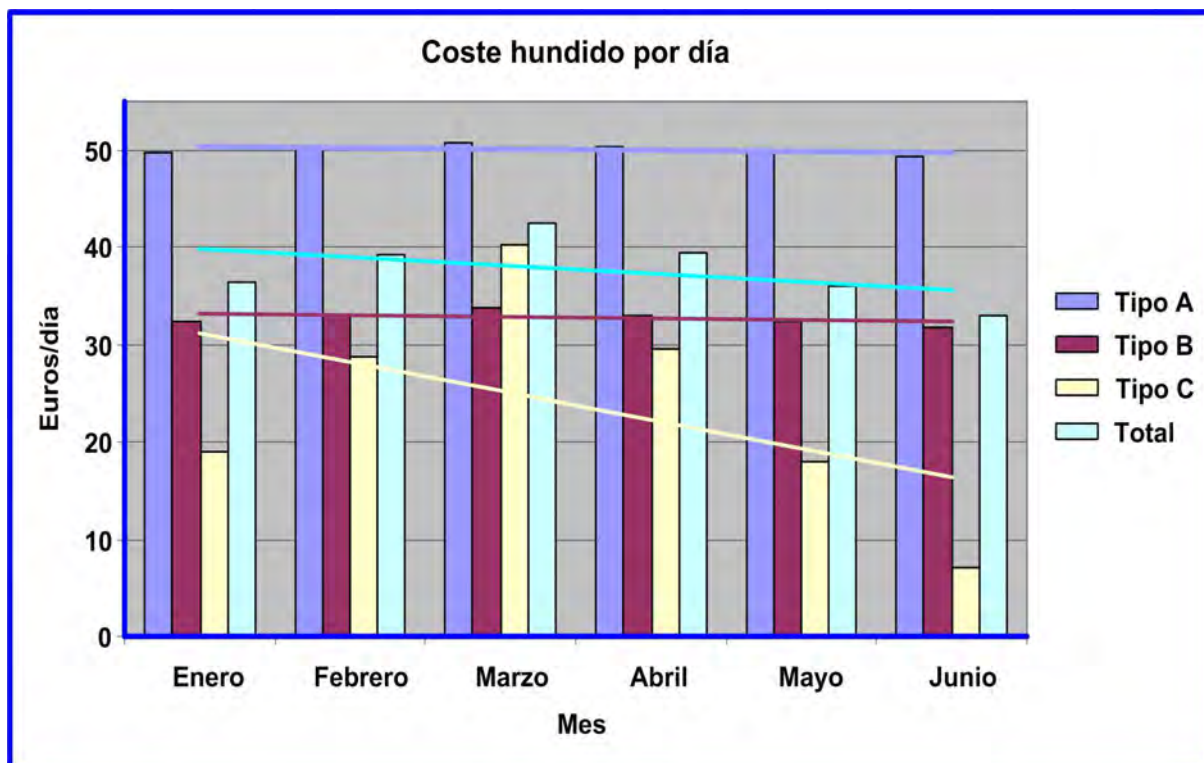


Gráfico 42: evolución del coste hundido por día

La evolución del coste hundido por día total ha sido creciente hasta el mes de marzo para posteriormente decrecer, este comportamiento ha sido provocado por la flota del tipo C ya que los costes hundidos por día de los vehículos del tipo A y B han sido prácticamente constantes.

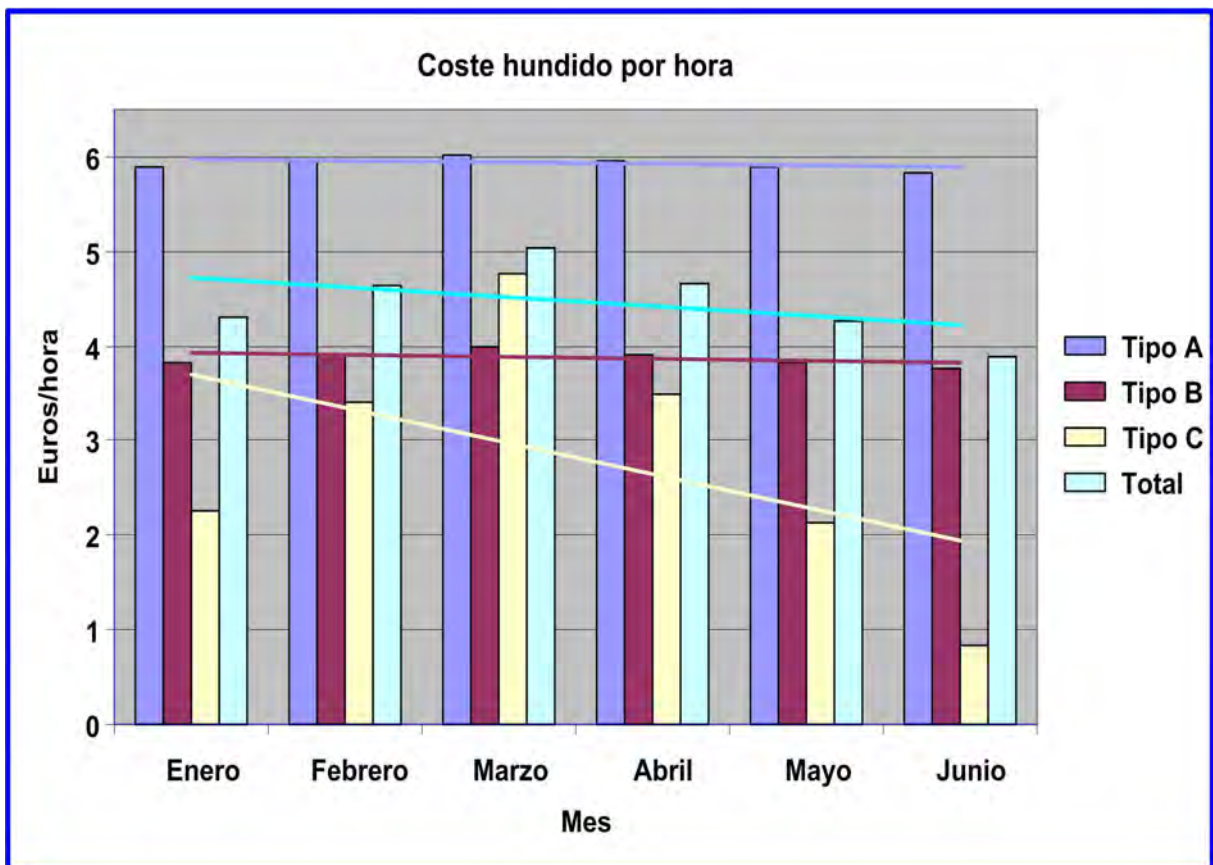


Gráfico 43: evolución del coste hundido por hora

La evolución del coste hundido por hora total ha sido creciente hasta el mes de marzo para posteriormente decrecer, este comportamiento ha sido provocado por la flota del tipo C ya que los costes hundidos por hora de los vehículos del tipo A y B han sido prácticamente constantes.

- Coste total por Km. recorrido según la tabla 2. El indicador es= costes directos + indirectos/Km. recorridos totales, en aquellas flotas en los que el vehículo esta parado prestando el servicio hay que realizarlo además por el número de horas de funcionamiento del motor.

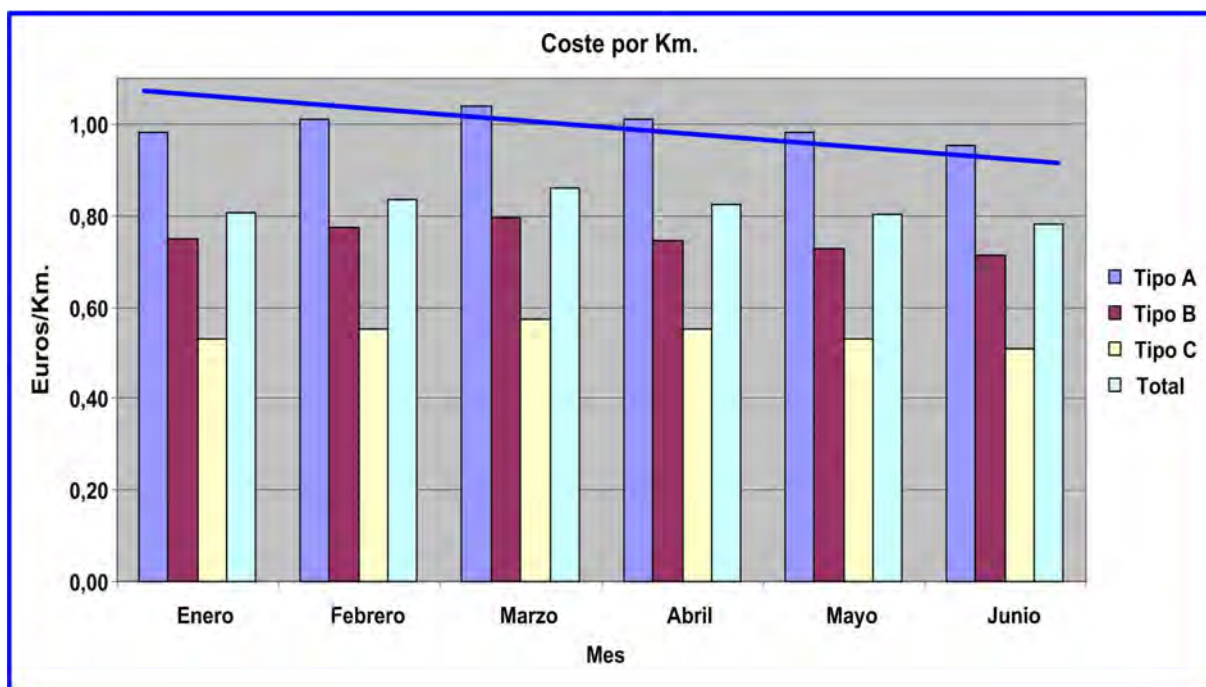


Gráfico 44: coste por Km.

El mayor coste por Km. corresponde a la flota del tipo A, seguido de la B y C. El coste por Km. ha sido creciente de enero a marzo, alcanzado el máximo en marzo, para a continuación decrecer. La evolución del coste por Km. es decreciente.

- Coste por Km. de cada partida (neumáticos, mantenimientos etc.) según lo representado en la tabla 2. El indicador es= Coste de cada partida/ Km. y su representación es como la del gráfico 44.

- Hay que incluir *rankings*, como los 10 vehículos con mayor: coste por Km. consumo de combustible, accidentes, conductores con conducción no eficiente etc. como la tabla 44.

| Nº | Id vehículo | Tipo de vehículo | Consumo (L/100 Km.) |
|----|-------------|------------------|---------------------|
| 1  | A101        | A                | 38,45               |
| 2  | A236        | A                | 37,33               |
| 3  | A25         | A                | 37,01               |
| 4  | A145        | A                | 36,89               |
| 5  | A69         | A                | 36,78               |
| 6  | A78         | A                | 36,45               |
| 7  | A236        | A                | 36,12               |
| 8  | A214        | A                | 35,89               |
| 9  | A321        | A                | 35,56               |
| 10 | A45         | A                | 35,43               |

Tabla 44: ranking de vehículos del tipo A con mayor consumo

- Coste total medio por vehículo. El ratio es = Coste total / nº de vehículos

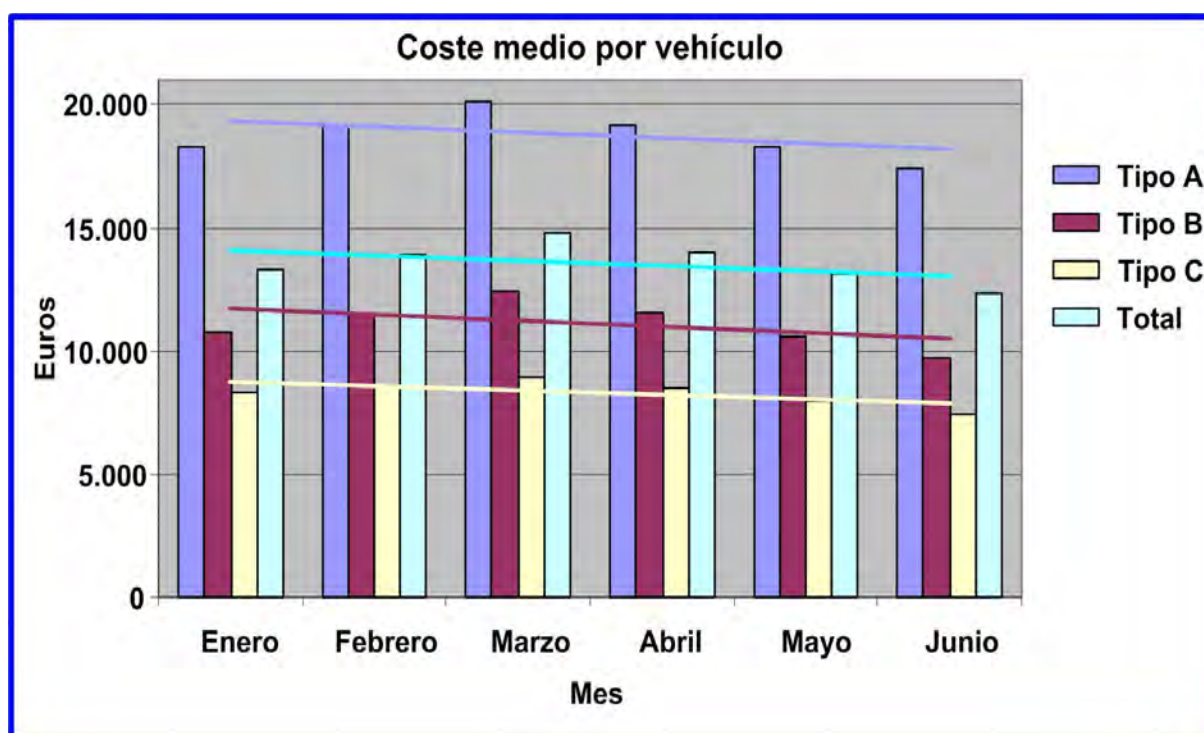


Gráfico 45: coste medio por vehículo

El mayor coste total por vehículo corresponde al tipo de vehículo A seguido del tipo B y C. El coste medio ha sido creciente de Enero a Marzo, obteniéndose el máximo en Marzo, para a continuación decrecer, la tendencia es decreciente.

- Coste de la tonelada transportada por Km. recorrido

El siguiente indicador nos suministra la información de cómo la flota esta optimizada y utilizamos los recursos disponibles. Tal como muestra la tabla 7, dependiendo del tipo de flota este indicador varía. En este caso práctico hemos representado el caso para una compañía de transporte de mercancías.

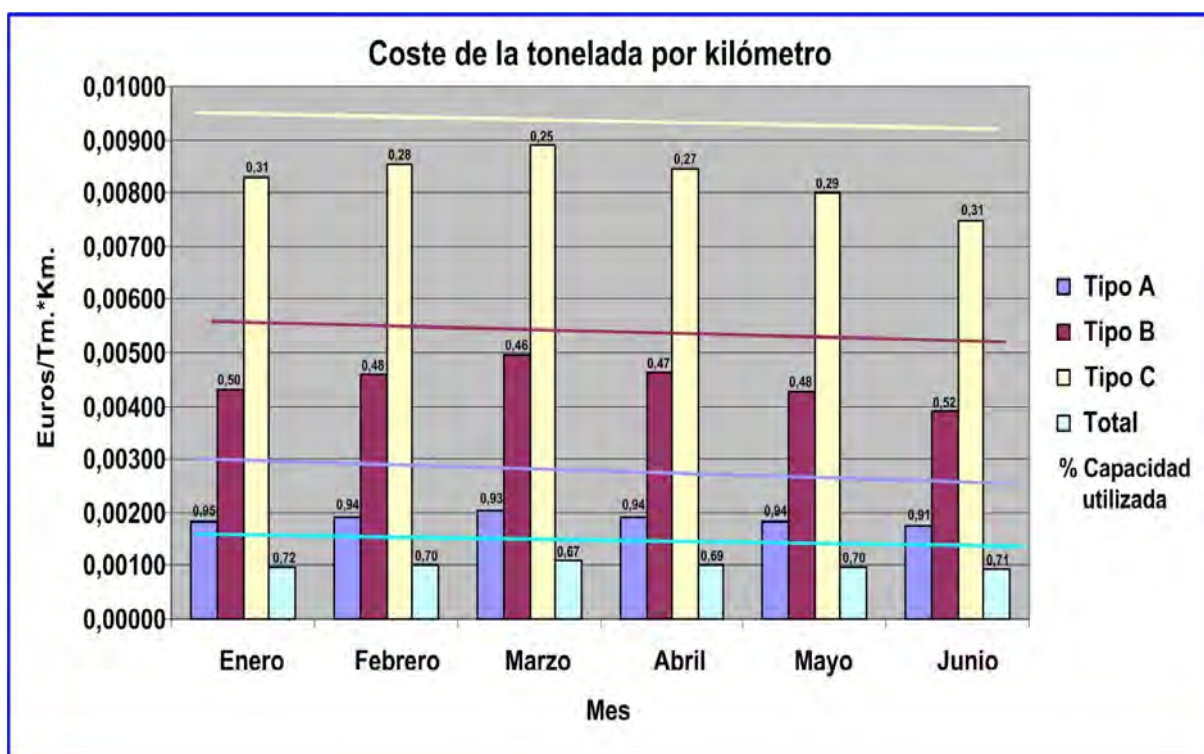


Gráfico 46: coste por tonelada kilómetro

El coste por tonelada transportada por kilómetro recorrido para el total de la flota ha sido creciente de enero a marzo, al alcanzándose el máximo en marzo, para a continuación decrecer, la tendencia es decreciente.

La flota del tipo C tiene el mayor coste por tonelada y kilómetro recorrido, y ha sido debido a que la capacidad utilizada ha sido del alrededor del 30%, lo que indica que este tipo de flota no esta optimizada.



La flota del tipo C es la que menor coste por Km. tiene, pero como solamente se utiliza el 30% de su capacidad el coste por tonelada y Km. es el más alto.

- Desviación total del TCO por periodo, este indicador nos informa cuanto nos estamos desviando del TCO real respecto al teórico según la tabla 13, así mismo es recomendable representarlo por cada partida del TCO (tabla 13).

El indicador es:  $\% \text{ desviación TCO} = \frac{\text{TCO real} - \text{TCO teórico}}{\text{TCO teórico}}$

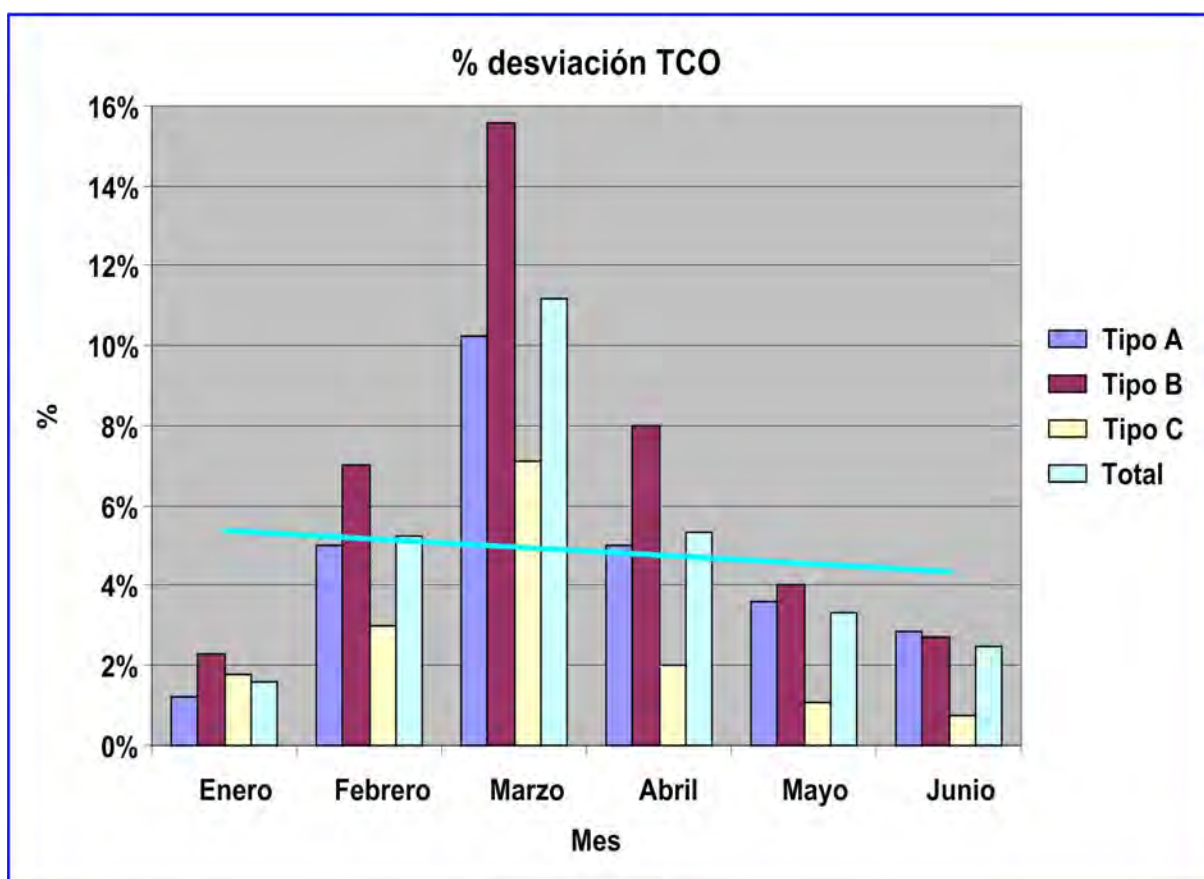


Gráfico 47: desviación del TCO

La desviación producida en el TCO para el total de la flota ha sido mayor de lo esperado para los meses de febrero, marzo y abril con un repunte en el mes de marzo aunque la tendencia es decreciente. Esta desviación del TCO ha sido provocada mayoritariamente por el vehículo del tipo B, con una gran desviación en el mes de marzo. No hay que considerar el coste de oportunidad para calcular la desviación del TCO.

- Desviación acumulada del TCO por año. Como el TCO se calcula por año, este ratio se ha de representar por año natural, empezando por enero, y nos informa de la cantidad total acumulada desviada respecto al TCO mes a mes, así mismo es recomendable representarlo por cada partida del TCO (tabla 13).

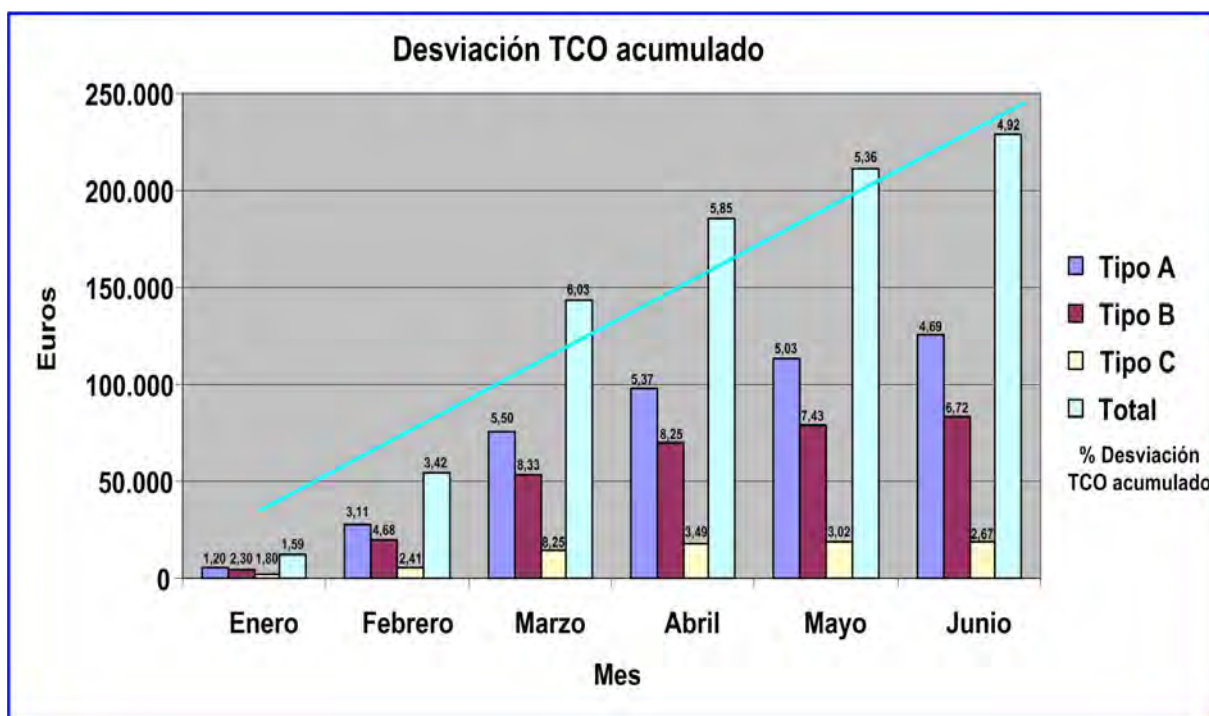


Gráfico 48: desviación acumulada del TCO en un año

La desviación acumulada del TCO para el total de la flota es creciente debido a las desviaciones positivas que hemos obtenido durante el año. Las mayores desviaciones se producen en el tipo de flota A debido a que cuantitativamente son mayores que en el resto de tipo de vehículos, aunque el tipo B tiene mayor % de desviación del TCO como sucedía en el gráfico.

Este indicador hay que representarlo según la columna % de la tabla 13 para conocer en que partida se nos esta produciendo las mayores desviaciones del TCO.

- Desviación total del presupuesto por periodo, este indicador nos informa cuanto nos estamos desviando del presupuesto real respecto al teórico según la tabla 13, así mismo es recomendable representarlo por cada partida del presupuesto (gráfico 22), su representación es el mismo gráfico 47 que para el TCO.



- Desviación acumulada del presupuesto por año. Como el presupuesto se calcula por año, este ratio se ha de representar por año natural, empezando por enero, y nos informa de la cantidad total acumulada desviada respecto al presupuesto mes a mes, así mismo es recomendable representarlo por cada partida del presupuesto (gráfico 22), su representación es el mismo gráfico 48 que para el TCO.

Con la información de este cuadro de mando las conclusiones son las siguientes:

- Como principal conclusión es que hay desviaciones positivas en los costes, aunque la tendencia es decreciente.
- Ha habido dos periodos claramente diferenciados; el periodo 1º de enero a marzo donde los costes se han incrementado, alcanzando su máximo en marzo para a continuación decrecer, debido principalmente por la mayor distancia recorrida y al aumento de los costes fijos del vehículo del tipo A; el 2º periodo de abril a junio los costes han decrecido, en general los decrementos del segundo periodo han tenido más peso que los del 1º periodo resultando la tendencia total en los costes ligeramente decreciente.
- Hemos obtenido desviaciones positivas en la distancia planificada y negativas en los costes unitarios, como resultado hemos obtenido desviaciones positivas en los costes variables de operación por que la distancia ha tenido más peso que los costes unitarios y la tendencia es decreciente.
- Hemos obtenido desviaciones positivas en el TCO, aunque la tendencia es decreciente.
- El mayor coste de la flota corresponde al vehículo del tipo A, seguido del vehículo B y C.
- El % de los costes de la flota respecto a los de la organización son decrecientes.
- El % de los costes de la flota respecto a la facturación son decrecientes.
- El % de los beneficios respecto a los costes de la flota son crecientes.

- El % de los costes fijos es decreciente, y los costes variables de operación son crecientes.
- La tendencia del coste hundido es decreciente, aunque el vehículo del tipo C ha tenido grandes variaciones.
- El coste por Km. en todo tipo de vehículos es decreciente.
- El coste medio por vehículo en todo tipo de vehículos es decreciente.
- El coste por tonelada transportada por Km. recorrido es decreciente en todo tipo de vehículos.
- Los tipos de vehículos B y C no están optimizados tal como muestra el gráfico 46, ya que sus tasas de ocupación son de alrededor del 50% y 30% respectivamente.
- La desviación del TCO ha sido positiva, aunque su tendencia es decreciente, hay que resaltar que el vehículo de tipo B, ha tenido una gran desviación en el mes de marzo.
- La desviación del TCO acumulado durante el año es positiva y creciente.

De la información suministrada por el cuadro de mando, las principales medidas a tomar son:

- Controlar y disminuir la distancia recorrida por el vehículo A y sus costes fijos.
- Conocer en que partidas del TCO se están produciendo las desviaciones y por qué.
- Optimizar el % de utilización de los tipos de vehículos B y C.

## 5. ANEXO

---

## 5.1. CASO PRÁCTICO

### 5.1.1. Periodo 1

| Concepto                                                                                                                                                  | Precio planificado | Cantidad planificada | Coste unitario planificado | Coste planificado | %       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|----------------------|----------------------------|-------------------|---------|
| Combustible                                                                                                                                               | 1                  | 5                    | 0,2                        | 40.000,00         | 39,863% |
| Accidentes                                                                                                                                                | 3.000              | 35.000               | 0,086                      | 17.142,86         | 17,084% |
| Neumáticos                                                                                                                                                | 700                | 10.000               | 0,07                       | 14.000,00         | 13,952% |
| Averías                                                                                                                                                   | 2.000              | 30.000               | 0,067                      | 13.333,33         | 13,288% |
| Mantenimientos                                                                                                                                            | 1.500              | 30.000               | 0,05                       | 10.000,00         | 9,966%  |
| Dietas                                                                                                                                                    | 70                 | 6.000                | 0,012                      | 2.333,33          | 2,325%  |
| Incentivos                                                                                                                                                | 20                 | 3.000                | 0,007                      | 1.333,33          | 1,329%  |
| Multas                                                                                                                                                    | 90                 | 15.000               | 0,006                      | 1.200,00          | 1,196%  |
| Peajes                                                                                                                                                    | 15                 | 3.000                | 0,005                      | 1.000,00          | 0,997%  |
| <b>Total</b>                                                                                                                                              |                    |                      | 0,502                      | 100.342,86        | 100%    |
| Tipo de vehículo A; Distancia planificada: 200.000; Precio planificado en Euros; Cantidad planificada en kilómetros; Distancia planificada en Kilómetros. |                    |                      |                            |                   |         |

Tabla 45: costes planificados para el vehículo del tipo A en el instante  $T_1$

| Concepto                                                                                                                      | Precio real | Cantidad real | Coste unitario real | Coste real | %       |
|-------------------------------------------------------------------------------------------------------------------------------|-------------|---------------|---------------------|------------|---------|
| Combustible                                                                                                                   | 1           | 4,37          | 0,229               | 46.012,26  | 43,989% |
| Accidentes                                                                                                                    | 2.757       | 33.494,78     | 0,082               | 16.542,36  | 15,815% |
| Neumáticos                                                                                                                    | 698         | 10.129,65     | 0,069               | 13.850,23  | 13,241% |
| Averías                                                                                                                       | 1.986       | 30.212,27     | 0,066               | 13.210,25  | 12,629% |
| Mantenimientos                                                                                                                | 1.450       | 29.673,18     | 0,049               | 9.823,56   | 9,391%  |
| Dietas                                                                                                                        | 68          | 7.362,44      | 0,009               | 1.856,45   | 1,775%  |
| Incentivos                                                                                                                    | 18          | 3.003,59      | 0,006               | 1.204,56   | 1,152%  |
| Multas                                                                                                                        | 95          | 16.597,85     | 0,006               | 1.150,45   | 1,100%  |
| Peajes                                                                                                                        | 14          | 2.960,70      | 0,005               | 950,45     | 0,909%  |
| <b>Total</b>                                                                                                                  |             |               | 0,52                | 104.600,57 | 100%    |
| Tipo de vehículo A; Distancia real: 201.000; Precio real en Euros; Cantidad real en kilómetros; Distancia real en Kilómetros. |             |               |                     |            |         |

Tabla 46: costes reales para el vehículo del tipo A en el instante  $T_2$

| Concepto                                                                                                                                                  | Precio planificado | Cantidad planificada | Coste unitario planificado | Coste planificado | %       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|----------------------|----------------------------|-------------------|---------|
| Combustible                                                                                                                                               | 1                  | 13                   | 0,077                      | 46.153,85         | 39,370% |
| Accidentes                                                                                                                                                | 500                | 13.000               | 0,038                      | 23.076,92         | 19,685% |
| Averías                                                                                                                                                   | 300                | 15.000               | 0,02                       | 12.000,00         | 10,236% |
| Multas                                                                                                                                                    | 90                 | 6.000                | 0,015                      | 9.000,00          | 7,677%  |
| Peajes                                                                                                                                                    | 15                 | 1.000                | 0,015                      | 9.000,00          | 7,677%  |
| Dietas                                                                                                                                                    | 70                 | 6.000                | 0,012                      | 7.000,00          | 5,971%  |
| Neumáticos                                                                                                                                                | 100                | 15.000               | 0,007                      | 4.000,00          | 3,412%  |
| Incentivos                                                                                                                                                | 20                 | 3.000                | 0,007                      | 4.000,00          | 3,412%  |
| Mantenimientos                                                                                                                                            | 150                | 30.000               | 0,005                      | 3.000,00          | 2,559%  |
| Total                                                                                                                                                     |                    |                      | 0,195                      | 117.230,77        | 100%    |
| Tipo de vehículo B; Distancia planificada: 600.000; Precio planificado en Euros; Cantidad planificada en kilómetros; Distancia planificada en Kilómetros. |                    |                      |                            |                   |         |

Tabla 26: costes planificados para el vehículo del tipo B en el instante  $T_1$

| Concepto                                                                                                                      | Precio real | Cantidad real | Coste unitario real | Coste real | %       |
|-------------------------------------------------------------------------------------------------------------------------------|-------------|---------------|---------------------|------------|---------|
| Combustible                                                                                                                   | 1           | 12,67         | 0,079               | 53.654,23  | 40,788% |
| Accidentes                                                                                                                    | 475         | 12.601,32     | 0,038               | 25.632,23  | 19,485% |
| Averías                                                                                                                       | 305         | 14.241,35     | 0,021               | 14.563,23  | 11,071% |
| Multas                                                                                                                        | 110         | 7.821,63      | 0,014               | 9.563,23   | 7,270%  |
| Peajes                                                                                                                        | 17          | 1.252,27      | 0,014               | 9.231,23   | 7,018%  |
| Dietas                                                                                                                        | 70          | 6.181,61      | 0,011               | 7.700,26   | 5,854%  |
| Neumáticos                                                                                                                    | 90          | 14.835,93     | 0,006               | 4.125,12   | 3,136%  |
| Incentivos                                                                                                                    | 20          | 3.442,93      | 0,006               | 3.950,12   | 3,003%  |
| Mantenimientos                                                                                                                | 145         | 31.546,35     | 0,005               | 3.125,56   | 2,376%  |
| Total                                                                                                                         |             |               | 0,193               | 131.545,21 | 100%    |
| Tipo de vehículo B; Distancia real: 680.000; Precio real en Euros; Cantidad real en kilómetros; Distancia real en Kilómetros. |             |               |                     |            |         |

Tabla 27: costes reales para el vehículo del tipo B en el instante  $T_2$

| Tipo de vehículo | Nº de vehículos | Costes unitarios planificados T1 | Costes unitarios reales T2 | Distancia planificada T1 | Distancia real T2 | Costes totales planificados T1 | Costes totales reales T2 | Diferencia total | Diferencia costes | Diferencia distancia |
|------------------|-----------------|----------------------------------|----------------------------|--------------------------|-------------------|--------------------------------|--------------------------|------------------|-------------------|----------------------|
| A                | 20              | 0,502                            | 0,52                       | 200.000                  | 201.000           | 100.342,86                     | 104.600,57               | 4.257,71         | 3.756,00          | 501,71               |
| B                | 80              | 0,195                            | 0,193                      | 600.000                  | 680.000           | 117.230,77                     | 131.545,21               | 14.314,44        | -1.316,33         | 15.630,77            |
| Total            | 100             |                                  |                            | 800.000                  | 881.000           | 217.573,63                     | 236.145,78               | 18.572,15        | 2.439,67          | 16.132,48            |

Tabla 47: desviaciones de los costes reales respecto a los planificados

| Tipo de vehículo | Tiempo total planificado | Tiempo total real | Diferencia | % diferencia |
|------------------|--------------------------|-------------------|------------|--------------|
| A                | 3.080                    | 2.684             | -396       | -12,86       |
| B                | 12.320                   | 13.728            | 1.408      | 11,43        |
| Total            | 15.400                   | 16.412            | 1.102      | 6,57         |
| Tiempo en horas. |                          |                   |            |              |

Tabla 48: tiempo total planificado y real por tipo de vehículo

| Tipo de vehículo                                                                | Distancia planificada | Tiempo planificado | Velocidad media planificada | Distancia real | Tiempo real | Velocidad real | Diferencia | % diferencia |
|---------------------------------------------------------------------------------|-----------------------|--------------------|-----------------------------|----------------|-------------|----------------|------------|--------------|
| A                                                                               | 200.000               | 3.080              | 64,94                       | 201.000        | 2.684       | 74,89          | 9,95       | 15,33%       |
| B                                                                               | 600.000               | 12.320             | 48,7                        | 680.000        | 13.728      | 49,53          | 0,83       | 1,71%        |
| Total                                                                           | 800.000               | 15.400             | 51,95                       | 881.000        | 16.412      | 53,68          | 1,73       | 3,33%        |
| Distancia planificada y real en kilómetros; tiempo planificado y real en horas. |                       |                    |                             |                |             |                |            |              |

Tabla 28: % desviación velocidad media real respecto a lo planificado

### 5.1.2. Periodo 2

| Concepto                                                                                                                                                  | Precio planificado | Cantidad planificada | Coste unitario planificado | Coste planificado | %      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|----------------------|----------------------------|-------------------|--------|
| Combustible                                                                                                                                               | 0,75               | 5                    | 0,15                       | 30.000,00         | 33,21% |
| Accidentes                                                                                                                                                | 3.000              | 35.000               | 0,086                      | 17.142,86         | 18,98% |
| Neumáticos                                                                                                                                                | 700                | 10.000               | 0,07                       | 14.000,00         | 15,50% |
| Averías                                                                                                                                                   | 2.000              | 30.000               | 0,067                      | 13.333,33         | 14,76% |
| Mantenimientos                                                                                                                                            | 1.500              | 30.000               | 0,05                       | 10.000,00         | 11,07% |
| Dietas                                                                                                                                                    | 70                 | 6.000                | 0,012                      | 2.333,33          | 2,58%  |
| Incentivos                                                                                                                                                | 20                 | 3.000                | 0,007                      | 1.333,33          | 1,48%  |
| Multas                                                                                                                                                    | 90                 | 15.000               | 0,006                      | 1.200,00          | 1,33%  |
| Peajes                                                                                                                                                    | 15                 | 3.000                | 0,005                      | 1.000,00          | 1,11%  |
| <b>Total</b>                                                                                                                                              |                    |                      | 0,452                      | 90.342,86         | 100%   |
| Tipo de vehículo A; Distancia planificada: 200.000; Precio planificado en Euros; Cantidad planificada en kilómetros; Distancia planificada en Kilómetros. |                    |                      |                            |                   |        |

Tabla 49: costes planificados para el vehículo del tipo A en el instante T<sub>2</sub>

| Concepto                                                                                                                      | Precio real | Cantidad real | Coste unitario real | Coste real | %      |
|-------------------------------------------------------------------------------------------------------------------------------|-------------|---------------|---------------------|------------|--------|
| Combustible                                                                                                                   | 0,78        | 4,81          | 0,162               | 32.125,00  | 35,55% |
| Accidentes                                                                                                                    | 2.800       | 36.714,94     | 0,076               | 15.100,12  | 16,71% |
| Neumáticos                                                                                                                    | 702         | 10.031,30     | 0,07                | 13.856,23  | 15,33% |
| Averías                                                                                                                       | 2.002       | 29.901,13     | 0,067               | 13.256,89  | 14,67% |
| Mantenimientos                                                                                                                | 1.896       | 37.082,61     | 0,051               | 10.123,56  | 11,20% |
| Dietas                                                                                                                        | 71          | 7.397,20      | 0,01                | 1.900,45   | 2,10%  |
| Incentivos                                                                                                                    | 25          | 2.749,14      | 0,009               | 1.800,56   | 1,99%  |
| Multas                                                                                                                        | 93          | 15.924,66     | 0,006               | 1.156,32   | 1,28%  |
| Peajes                                                                                                                        | 16          | 3.016,48      | 0,005               | 1.050,23   | 1,16%  |
| <b>Total</b>                                                                                                                  |             |               | 0,456               | 90.369,36  | 100%   |
| Tipo de vehículo A; Distancia real: 198.000; Precio real en Euros; Cantidad real en kilómetros; Distancia real en Kilómetros. |             |               |                     |            |        |

Tabla 50: costes reales para el vehículo del tipo A en el instante T<sub>3</sub>

| Concepto                                                                                                                                                  | Precio planificado | Cantidad planificada | Coste unitario planificado | Coste planificado | %           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|----------------------|----------------------------|-------------------|-------------|
| Combustible                                                                                                                                               | 0,75               | 13                   | 0,058                      | 34.615,38         | 32,22%      |
| Accidentes                                                                                                                                                | 475                | 13.000               | 0,037                      | 21.923,08         | 20,41%      |
| Averías                                                                                                                                                   | 305                | 15.000               | 0,02                       | 12.200,00         | 11,36%      |
| Multas                                                                                                                                                    | 110                | 6.000                | 0,018                      | 11.000,00         | 10,24%      |
| Peajes                                                                                                                                                    | 17                 | 1.000                | 0,017                      | 10.200,00         | 9,49%       |
| Dietas                                                                                                                                                    | 70                 | 6.000                | 0,012                      | 7.000,00          | 6,52%       |
| Incentivos                                                                                                                                                | 20                 | 3.000                | 0,007                      | 4.000,00          | 3,72%       |
| Neumáticos                                                                                                                                                | 90                 | 15.000               | 0,006                      | 3.600,00          | 3,35%       |
| Mantenimientos                                                                                                                                            | 145                | 30.000               | 0,005                      | 2.900,00          | 2,70%       |
| <b>Total</b>                                                                                                                                              |                    |                      | <b>0,179</b>               | <b>107.438,46</b> | <b>100%</b> |
| Tipo de vehículo B; Distancia planificada: 600.000; Precio planificado en Euros; Cantidad planificada en kilómetros; Distancia planificada en Kilómetros. |                    |                      |                            |                   |             |

Tabla 31: costes planificados para el vehículo del tipo B en el instante  $T_2$

| Concepto                                                                                                                      | Precio real | Cantidad real | Coste unitario real | Coste real        | %           |
|-------------------------------------------------------------------------------------------------------------------------------|-------------|---------------|---------------------|-------------------|-------------|
| Combustible                                                                                                                   | 0,8         | 13,22         | 0,061               | 38.132,65         | 33,76%      |
| Accidentes                                                                                                                    | 469         | 13.095,01     | 0,036               | 22.563,56         | 19,98%      |
| Averías                                                                                                                       | 308         | 13.323,97     | 0,023               | 14.563,23         | 12,89%      |
| Multas                                                                                                                        | 108         | 7.114,75      | 0,015               | 9.563,23          | 8,47%       |
| Peajes                                                                                                                        | 21          | 1.433,18      | 0,015               | 9.231,23          | 8,17%       |
| Dietas                                                                                                                        | 68          | 5.563,45      | 0,012               | 7.700,26          | 6,82%       |
| Neumáticos                                                                                                                    | 91          | 13.897,78     | 0,007               | 4.125,12          | 3,65%       |
| Incentivos                                                                                                                    | 23          | 3.668,24      | 0,006               | 3.950,12          | 3,50%       |
| Mantenimientos                                                                                                                | 142         | 28.622,07     | 0,005               | 3.125,56          | 2,77%       |
| <b>Total</b>                                                                                                                  |             |               | <b>0,179</b>        | <b>112.954,96</b> | <b>100%</b> |
| Tipo de vehículo B; Distancia real: 630.127; Precio real en Euros; Cantidad real en kilómetros; Distancia real en Kilómetros. |             |               |                     |                   |             |

Tabla 32: costes reales para el vehículo del tipo B en el instante  $T_3$



| Tipo de vehículo | Nº de vehículos | Costes unitarios planificados T1 | Costes unitarios reales T2 | Distancia planificada T1 | Distancia real T2 | Costes totales planificados T1 | Costes totales reales T2 | Diferencia total | Diferencia costes | Diferencia distancia |
|------------------|-----------------|----------------------------------|----------------------------|--------------------------|-------------------|--------------------------------|--------------------------|------------------|-------------------|----------------------|
| A                | 20              | 0,452                            | 0,456                      | 200.000                  | 198.000           | 90.342,86                      | 90.369,36                | 26,5             | 929,93            | -903,43              |
| B                | 80              | 0,179                            | 0,179                      | 600.000                  | 630.000           | 107.438,46                     | 112.954,96               | 5.516,50         | 144,58            | 5.371,92             |
| Total            | 100             |                                  |                            | 800.000                  | 828.000           | 197.781,32                     | 203.324,32               | 5.543,00         | 1.074,51          | 4.468,49             |

Tabla 51: desviaciones de los costes reales respecto a los planificados

| Tipo de vehículo | Tiempo total planificado | Tiempo total real | Diferencia | % desviación |
|------------------|--------------------------|-------------------|------------|--------------|
| A                | 3.080                    | 3.036             | -44        | -1,429%      |
| B                | 12.320                   | 12.496            | 176        | 1,429%       |
| Total            | 15.400                   | 15.532            | 132        | 0,857%       |

Tabla 52: tiempo total planificado y real por tipo de vehículo

| Tipo de vehículo                                                                | Distancia planificada | Tiempo planificado | Velocidad media planificada | Distancia real | Tiempo real | Velocidad real | Diferencia | % diferencia |
|---------------------------------------------------------------------------------|-----------------------|--------------------|-----------------------------|----------------|-------------|----------------|------------|--------------|
| A                                                                               | 200.000               | 3.080              | 64,94                       | 198.000        | 3.036       | 65,22          | 0,28       | 0,43%        |
| B                                                                               | 600.000               | 12.320             | 48,7                        | 630.000        | 12.496      | 50,42          | 1,71       | 3,52%        |
| Total                                                                           | 800.000               | 15.400             | 51,95                       | 828.000        | 15.532      | 53,31          | 1,36       | 2,62%        |
| Distancia planificada y real en kilómetros; tiempo planificado y real en horas. |                       |                    |                             |                |             |                |            |              |

Tabla 33: % desviación velocidad media real respecto a lo planificado

### 5.1.3. Periodo 3

| Concepto                                                                                                                                                                | Precio planificado | Cantidad planificada | Coste unitario planificado | Coste planificado | %      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|----------------------|----------------------------|-------------------|--------|
| Combustible                                                                                                                                                             | 0,75               | 5                    | 0,15                       | 31.125,00         | 38,73% |
| Neumáticos                                                                                                                                                              | 700                | 10.000               | 0,07                       | 14.525,00         | 18,07% |
| Averías                                                                                                                                                                 | 1.600              | 30.000               | 0,053                      | 11.066,67         | 13,77% |
| Accidentes                                                                                                                                                              | 2.400              | 50.000               | 0,048                      | 9.960,00          | 12,39% |
| Mantenimientos                                                                                                                                                          | 1.100              | 30.000               | 0,037                      | 7.608,33          | 9,47%  |
| Dietas                                                                                                                                                                  | 70                 | 6.000                | 0,012                      | 2.420,83          | 3,01%  |
| Incentivos                                                                                                                                                              | 20                 | 3.000                | 0,007                      | 1.383,33          | 1,72%  |
| Multas                                                                                                                                                                  | 90                 | 15.000               | 0,006                      | 1.245,00          | 1,55%  |
| Peajes                                                                                                                                                                  | 15                 | 3.000                | 0,005                      | 1.037,50          | 1,29%  |
| <b>Total</b>                                                                                                                                                            |                    |                      | 0,387                      | 80.371,67         | 100%   |
| Tipo de vehículo A: 21 Vehículos; Distancia planificada: 207.500; Precio planificado en Euros; Cantidad planificada en kilómetros; Distancia planificada en Kilómetros. |                    |                      |                            |                   |        |

Tabla 38: costes planificados para el vehículo del tipo A en el instante  $T_3$

| Concepto                                                                                                                                    | Precio real | Cantidad real | Coste unitario real | Coste real | %      |
|---------------------------------------------------------------------------------------------------------------------------------------------|-------------|---------------|---------------------|------------|--------|
| Combustible                                                                                                                                 | 0,75        | 5,24          | 0,143               | 28.563,65  | 37,10% |
| Neumáticos                                                                                                                                  | 702         | 10.130,45     | 0,069               | 13.824,56  | 17,96% |
| Averías                                                                                                                                     | 1.564       | 30.163,66     | 0,052               | 10.345,69  | 13,44% |
| Accidentes                                                                                                                                  | 2.315       | 48.830,74     | 0,047               | 9.456,23   | 12,28% |
| Mantenimientos                                                                                                                              | 1.050       | 28.917,61     | 0,036               | 7.245,65   | 9,41%  |
| Dietas                                                                                                                                      | 75          | 5.237,34      | 0,014               | 2.856,89   | 3,71%  |
| Peajes                                                                                                                                      | 20          | 1.950,57      | 0,01                | 2.045,56   | 2,66%  |
| Incentivos                                                                                                                                  | 25          | 3.116,90      | 0,008               | 1.600,15   | 2,08%  |
| Multas                                                                                                                                      | 85          | 16.140,01     | 0,005               | 1.050,65   | 1,36%  |
| <b>Total</b>                                                                                                                                |             |               | 0,386               | 76.989,03  | 100%   |
| Tipo de vehículo A: 21 vehículos; Distancia real: 199.500; Precio real en Euros; Cantidad real en kilómetros; Distancia real en Kilómetros. |             |               |                     |            |        |

Tabla 39: costes reales para el vehículo del tipo A en el instante  $T_4$

| Concepto                                                                                                                                                                | Precio planificado | Cantidad planificada | Coste unitario planificado | Coste planificado | %      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|----------------------|----------------------------|-------------------|--------|
| Combustible                                                                                                                                                             | 1                  | 15,00                | 0,05                       | 30.700,00         | 33,94% |
| Multas                                                                                                                                                                  | 110                | 6.000,00             | 0,018                      | 11.256,67         | 12,44% |
| Accidentes                                                                                                                                                              | 360                | 20.000,00            | 0,018                      | 11.052,00         | 12,22% |
| Peajes                                                                                                                                                                  | 17                 | 1.000,00             | 0,017                      | 10.438,00         | 11,54% |
| Averías                                                                                                                                                                 | 240                | 15.000,00            | 0,016                      | 9.824,00          | 10,86% |
| Dietas                                                                                                                                                                  | 70                 | 6.000                | 0,012                      | 7.163,33          | 7,92%  |
| Incentivos                                                                                                                                                              | 20                 | 3.000                | 0,007                      | 4.093,33          | 4,52%  |
| Neumáticos                                                                                                                                                              | 90                 | 15.000               | 0,006                      | 3.684,00          | 4,07%  |
| Mantenimientos                                                                                                                                                          | 110                | 30.000               | 0,004                      | 2.251,33          | 2,49%  |
| Total                                                                                                                                                                   |                    |                      | 0,147                      | 90.462,67         | 100%   |
| Tipo de vehículo B: 83 vehículos; Distancia planificada: 614.000; Precio planificado en Euros; Cantidad planificada en kilómetros; Distancia planificada en Kilómetros. |                    |                      |                            |                   |        |

Tabla 40: costes planificados para el vehículo del tipo B en el instante  $T_3$

| Concepto                                                                                                                                    | Precio real | Cantidad real | Coste unitario real | Coste real | %      |
|---------------------------------------------------------------------------------------------------------------------------------------------|-------------|---------------|---------------------|------------|--------|
| Combustible                                                                                                                                 | 0,75        | 16            | 0,047               | 28.563,26  | 32,28% |
| Peajes                                                                                                                                      | 20          | 1.008         | 0,02                | 12.002,36  | 13,56% |
| Multas                                                                                                                                      | 104         | 5.774         | 0,018               | 10.896,36  | 12,31% |
| Accidentes                                                                                                                                  | 326         | 18.660        | 0,017               | 10.569,89  | 11,95% |
| Averías                                                                                                                                     | 234         | 14.970        | 0,016               | 9.456,89   | 10,69% |
| Dietas                                                                                                                                      | 75          | 6.439         | 0,012               | 7.046,67   | 7,96%  |
| Incentivos                                                                                                                                  | 25          | 3.573         | 0,007               | 4.232,65   | 4,78%  |
| Neumáticos                                                                                                                                  | 88          | 14.970        | 0,006               | 3.556,56   | 4,02%  |
| Mantenimientos                                                                                                                              | 106         | 29.733        | 0,004               | 2.156,89   | 2,44%  |
| Total                                                                                                                                       |             |               | 0,146               | 88.481,53  | 100%   |
| Tipo de vehículo B: 83 vehículos; Distancia real: 605.000; Precio real en Euros; Cantidad real en kilómetros; Distancia real en Kilómetros. |             |               |                     |            |        |

Tabla 41: costes reales para el vehículo del tipo B en el instante  $T_4$

| Tipo de vehículo | Nº de vehículos | Costes unitarios planificados | Costes unitarios reales | Distancia planificada | Distancia real | Costes planificados |
|------------------|-----------------|-------------------------------|-------------------------|-----------------------|----------------|---------------------|
| A                | 23              | 0,387                         | 0,386                   | 207.500               | 199.500        | 80.371,67           |
| B                | 81              | 0,147                         | 0,146                   | 614.000               | 605.000        | 90.462,67           |
| Total            | 104             |                               |                         | 821.500               | 804.500        | 170.834,33          |

Tabla 53: desviaciones de los costes reales respecto a los planificados

| Tipo de vehículo | Tiempo total planificado | Tiempo total real | Diferencia | % diferencia |
|------------------|--------------------------|-------------------|------------|--------------|
| A                | 3.234                    | 3.188             | -46        | -1,429%      |
| B                | 12.782                   | 12.965            | 183        | 1,429%       |
| Total            | 16.016                   | 16.152            | 136        | 0,852%       |

Tabla 42: tiempo total planificado y real por tipo de vehículo

| Tipo de vehículo | Distancia planificada | Tiempo planificado | Velocidad media planificada | Distancia real | Tiempo real | Velocidad real | Diferencia | % diferencia |
|------------------|-----------------------|--------------------|-----------------------------|----------------|-------------|----------------|------------|--------------|
| A                | 207.500               | 3.234              | 64,16                       | 199.500        | 3.188       | 62,58          | -1,58      | -2,46%       |
| B                | 614.000               | 12.782             | 48,04                       | 605.000        | 12.965      | 46,67          | -1,37      | -2,85%       |
| Total            | 821.500               | 16.016             | 51,29                       | 804.500        | 16.152      | 49,81          | -1,49      | -2,90%       |

Tabla 54: % desviación velocidad media real respecto a lo planificado

## 6. REFERENCIAS

---

Adam Redmer. 2009. Optimisation of the exploitation period of individual vehicles in freight transportation companies. *Transportation Research Part E: Logistics and Transportation Review*. Volume 45, Issue 6, 978–987.

B.W. Simms, B.G. Lamarre, A.K.S. Jardine. 1984. Optimal buy, operate and sell policies for fleets of vehicles. *European Journal of Operational Research*. Volume 15, Issue 2, 183–195.

Parthana Parthanadeea, Jirachai Buddhakulsomsirib, Peerayuth Charnsethikulc. 2012. A study of replacement rules for a parallel fleet replacement problem based on user preference utilization pattern and alternative fuel considerations. *Computers & Industrial Engineering*. Volume 63, Issue 1, 46–57.

S. Eilon, J.R King, D.E. Hutchinson. 1966. A Study in Equipment Replacement. *Journal of the Operational Research Society* 17, 59–71.





# **Desarrollo de una herramienta de gestión de flotas de vehículos eléctricos**



# DESARROLLO DE UNA HERRAMIENTA DE GESTIÓN DE FLOTAS DE VEHÍCULOS ELÉCTRICOS

**JORGE LEÓN BELLO**

**EMILIO GONZÁLEZ VIOSCA**

**JUAN DE DIOS DÍAZ MARQUÉS**

**JUAN JOSÉ SORLÍ CASTELLÓ**

ITENE - Instituto Tecnológico del Embalaje,  
Transporte y Logística (Valencia)

Que el vehículo eléctrico ha venido para quedarse es un hecho. Cada vez está más presente en nuestras ciudades, y no sólo entre el público en general sino también entre las empresas que se dedican a la distribución urbana de mercancías. Si bien para desplazamientos interurbanos el cambio de motos convencionales a eléctrico se dará a medio plazo,

lo que está claro es que hoy en día el vehículo eléctrico aparece como solución eficiente, respetuosa y capaz de satisfacer las necesidades diarias de movilidad en entornos urbanos y metropolitanos. Y esto, no sólo aplicado a transporte de pasajeros, sino también aplicado al transporte de mercancías en lo que generalmente se conoce como los desplazamientos de «última milla». En este sentido, para el transporte de mercancías en entornos urbanos, el vehículo eléctrico encaja perfectamente con las características de los desplazamientos de «última milla» (tráfico congestionado, continuas paradas y arranques, radios de actuación limitados, necesidad de tecnologías limpias para cumplir con los límites de contaminación del aire en ciudades, etc.).

La distribución urbana de mercancías es básica, fundamental y prioritaria para la actividad económica de cualquier ciudad. En este sentido es importante resaltar una serie de aspectos que caracterizan nuestros entornos urbanos y los retos que debe abordar el transporte de mercancías. Entre estos aspectos resaltar que: el 72% de la población vive en ciudades y alrededores, con previsiones del 80% en 2020; que el transporte urbano de mercancías es un componente importante del tráfico en ciudades, con el equivalente a porcentajes de entre el 10% y el 15% de kilómetros por vehículo recorridos; que los factores de carga en los vehículos de reparto son bajos (por ejemplo, del 38%

en furgonetas en Londres); o que el reparto de mercancías aparece como responsable de una parte importante de la contaminación acústica en ciudades (ETRAC, 2014). Por otra parte, a nivel nacional, algunos datos del caso particular de la ciudad Madrid pueden servir para ilustrar los desafíos que la distribución urbana de mercancías representa. En este sentido destacar que, si bien se ha reducido en los últimos años, el porcentaje de vehículos comerciales que estacionan ilegalmente es todavía el 43%, mientras que los que estacionan en zonas de carga y descarga se sitúa en un 40% (Ayuntamiento de Madrid, 2014). Asimismo, de acuerdo a Informe del Estado de la Movilidad de la Ciudad de Madrid, esta mayor ocupación también se debe al crecimiento de la duración del estacionamiento de los vehículos comerciales, con un 30% del total de vehículos que estacionan más de 30 minutos. Estas duraciones superan la limitación de la ordenanza de circulación y suponen, a medio plazo, una amenaza para la capacidad de estas zonas.

Pero además de los problemas de congestión que indican estas cifras, la adopción de tecnologías menos contaminantes tiene una repercusión clara en uno de los aspectos que más preocupa a los ciudadanos: la contaminación y la calidad del aire que respiramos que afecta negativamente a la salud. A nivel mundial, aproximadamente el 22% de las emisiones de CO<sub>2</sub> se deben al sector transporte (IEA, 2014). A nivel europeo,

el transporte de mercancías es responsable del 25% de las emisiones de CO<sub>2</sub> relativas al transporte urbano y responsable además de entre el 30% y el 50% de otros contaminantes derivados del transporte como partículas PM y óxidos de nitrógeno NO<sub>x</sub> (ERTRAC, 2014). A nivel nacional, y de acuerdo al Plan de Calidad del Aire de España (Ministerio de Agricultura, Alimentación y Medio Ambiente, 2013), los niveles de contaminación actuales indican que existen varios contaminantes que superan los límites indicados por el Real Decreto 102/2011 (BOE, 2011). Estos contaminantes son el Dióxido de Azufre (SO<sub>2</sub>), el Dióxido de Nitrógeno (NO<sub>2</sub>), las partículas (PM<sub>10</sub>) y el Ozono. Entre los factores a los que se deben estos niveles de contaminación, son diversas las fuentes que generan estos contaminantes. En el caso de las emisiones de Dióxido de Azufre (SO<sub>2</sub>), los factores principales son la producción de energía (37%) seguido del transporte por carretera (23%). En el caso de las emisiones de Dióxido de Nitrógeno (NO<sub>2</sub>), la mayoría son generadas por el transporte por carretera (70%), llegando a alcanzar el 88% en áreas urbanas. Respecto a las partículas (PM<sub>10</sub>), las principales fuentes de estos contaminantes son las actividades industriales (41%) y el tráfico (35%). Estas cifras resaltan la influencia de la actividad de transporte como responsable de la contaminación del aire, la cual no sólo afecta al medioambiente sino también a la salud de las personas. En este sentido, de acuerdo al último informe de Ecologistas en Acción (2014), y considerando los niveles de calidad del aire recomendados por la Organización Mundial de la Salud (OMS, 2014), aproximadamente 45 millones de personas en España (es decir, el 95% de la población) respira aire contaminado lo que les pone en situación de riesgo de problemas de salud a largo plazo.

Por estos motivos, tanto desde las administraciones públicas como desde las empresas privadas, se viene realizando un esfuerzo para adoptar estrategias alternativas que permitan una movilidad más sostenible como pueden ser las tecnologías de movilidad eléctrica, y muy especialmente en un sector tan fundamental para cualquier ciudad como es la distribución de mercancías y la logística. En este sentido, el proyecto FREVUE (2013) ha logrado aunar a varias de las capitales y grandes ciudades europeas junto con empresas logísticas y proveedores de vehículos eléctricos para poner en marcha iniciativas con el ánimo de avanzar en modelos logísticos más sostenibles y basados en vehículos eléctricos.

#### PROYECTO FREVUE

El proyecto FREVUE «Freight Electric Vehicles in Urban Europe» -Vehículos eléctricos para la distribución en áreas urbanas de Europa- tiene como principal objetivo demostrar que la distribución con vehículos eléctricos puede ser una alternativa viable a los vehículos de combustión convencionales (diésel o gasolina).

El proyecto está cofinanciado por 7º Programa Marco de I+D+I de la Unión Europea y tiene una duración de 4 años y medio: desde Marzo de 2013 a Septiembre

de 2017. En el proyecto FREVUE participan importantes ciudades europeas como Ámsterdam (Países Bajos), Lisboa (Portugal), Londres (Reino Unido), Milán (Italia), Oslo (Noruega), Rotterdam (Países Bajos), Estocolmo (Suecia) y Madrid (España). En todas estas ciudades se están llevando a cabo una serie de pilotos demostradores para la distribución urbana de mercancías mediante vehículos eléctricos. Proyectos europeos como FREVUE ayudan a demostrar la viabilidad de esta tecnología de automoción no sólo desde el punto de vista operacional sino también financiero y económico, fomentando una estrategia «win-win» (ganar-ganar) entre las administraciones públicas y el sector privado.

El aumento de la población en las ciudades europeas genera grandes oportunidades económicas, sociales y culturales para sus ciudadanos. Para cubrir este creciente aumento de la demanda de productos, servicios y movilidad, las ciudades sufren un incremento significativo de emisiones de aire y ruido, así como una congestión en aumento.

El objetivo del proyecto FREVUE (Vehículos eléctricos para la distribución en áreas urbanas de Europa) es demostrar a la industria, consumidores y legisladores, cómo la distribución con vehículos eléctricos puede proporcionar una solución a muchos de estos problemas. FREVUE trata de ayudar al desarrollo sostenible, gracias a la utilización de vehículos eléctricos para el reparto urbano en las grandes ciudades, que es donde se concentra la mayor contaminación ambiental.

En total, considerando todos los países europeos que intervienen en el proyecto, 127 vehículos eléctricos de mercancías se expondrán al rigor diario de las condiciones logísticas urbanas con el fin de probar que la actual generación de furgones y camiones eléctricos suponen una alternativa viable a los vehículos diésel, especialmente cuando se combinan con soluciones logísticas urbanas, programas informáticos para la gestión logística y políticas locales bien diseñadas.

Dentro del piloto de Madrid, ITENE –el Instituto Tecnológico del Embalaje, Transporte y Logística– está desarrollando una herramienta de gestión de flotas de vehículos eléctricos que permita la monitorización en tiempo real de los parámetros más relevantes en la conducción y operativa de distribución mediante este tipo de vehículos. Esta herramienta permite gestionar eficazmente las recargas eléctricas y las rutas de reparto de «última milla» de los 3 operadores logísticos que participan en el proyecto – SEUR, TNT y CALIDAD PASCUAL–.

Como parte de la política de responsabilidad corporativa de CALIDAD PASCUAL, la estrategia de movilidad sostenible, gracias a acuerdos anteriores con Mercedes Benz e Iveco, es llegar, en un corto-medio plazo, a repartir todos sus productos con camiones eléctricos en la mayoría de los barrios céntricos de las grandes ciudades. Por su parte, SEUR enmarca este proyecto en su apuesta por un Planeta Sostenible. Su objetivo es la reducción de emisiones de CO<sub>2</sub> gracias a un programa por la Movilidad Sostenible, que contempla, entre otros, la incorporación de flota ecológica, oferta de

**CUADRO 1**  
**DATOS DE LA OPERATIVA DIARIA DE CALIDAD PASCUAL EN REVUE**

|                                           |                                                                                               |                |
|-------------------------------------------|-----------------------------------------------------------------------------------------------|----------------|
| Vehículos                                 | ★ IVECO Ecodaily<br>★ Mercedes Vito E-cell                                                    |                |
|                                           | Horas al día trabajando                                                                       | 10             |
|                                           | Franja horaria                                                                                | Mañana y tarde |
| Trabajo diario                            | Número de conductores                                                                         | 2              |
|                                           | Número de entregas                                                                            | 6 toneladas    |
|                                           | Kilómetros                                                                                    | 50-100 km      |
|                                           |                                                                                               |                |
| Tipo de mercancía transportada            | Alimentación y bebidas                                                                        |                |
| Tipo de clientes                          | Comercios, restaurantes y cafeterías                                                          |                |
| Localización y frecuencia de las entregas | Generalmente durante la mañana, empezado a las 5:30 am y finalizando por la tarde a las 19:30 |                |
| Área de influencia                        | Zona de Bajas Emisiones de Madrid                                                             |                |

FUENTE: Elaboración propia.

eco-embalajes o el servicio internacional terrestre más ecológico del mercado, a través de «Total Zero». TNT Express, siguiendo con su compromiso medioambiental y su apuesta por la sostenibilidad, opera flotas con vehículos eléctricos en España, Reino Unido, Francia, Suiza, Italia, Países Bajos, China, Hong Kong, República Checa y Turquía. En España, TNT Express ya comenzó a utilizar triciclos eléctricos dentro del programa «City Logistics» de reducción de emisiones CO<sub>2</sub> en Barcelona y Madrid, que evitan la emisión de 1 tonelada de CO<sub>2</sub> anual.

Asimismo, otro de los pilares fundamentales de este innovador proyecto FREVUE es poner en funcionamiento un centro de consolidación o plataforma logística en el centro de Madrid, desde el que distribuir mercancías por medio de vehículos eléctricos a zonas de la capital medioambientalmente delicadas. Durante esa distribución se están recogiendo cuantos datos ayudan a estudiar la mejora del uso de puntos de recarga en la ciudad de Madrid y el manejo de las Tecnologías de Información y Comunicación (TIC) para optimizar la utilización de vehículos eléctricos.

## DESARROLLO DEL PILOTO DEMOSTRADOR DE MADRID

### Solución logística para el reparto de última milla

El objetivo del piloto de Madrid es demostrar que la generación actual de furgonetas y camiones eléctricos puede ofrecer una alternativa viable a los vehículos diésel y gasolina, especialmente cuando se combinan con sistemas de gestión logística innovadores y basados en tecnologías TIC. Este es precisamente el objetivo del desarrollo de la herramienta de gestión de flotas para vehículos eléctricos que ha liderado ITENE.

El proyecto ha establecido un centro de consolidación en Madrid, situado en el antiguo Mercado de Legazpi, desde el cual los vehículos eléctricos llevarán a cabo la distribución de mercancías de última milla de SEUR, TNT y CALIDAD PASCUAL independientemente. Desde ese centro de consolidación se realizará el reparto de

última milla en zonas céntricas de la ciudad de Madrid, utilizando para ello vehículos eléctricos.

Los vehículos eléctricos utilizados para la distribución de última milla son la Vito E-Cell de Mercedes Benz, la Kangoo Z.E. de Renault y la Daily Eléctrica de Iveco. Para la optimización del uso de estos vehículos eléctricos, por parte de ITENE se propone una herramienta de monitorización cuyas características principales se detallan en el siguiente apartado.

### Detalle de la operativa de las empresas

A continuación, se detalla la operativa seguida por cada una de las empresas participantes en el Proyecto FREVUE.(ver cuadro 1, 2 y 3, en la página siguiente)

### Primeros resultados

Uno de los aspectos clave que están contribuyendo al éxito de esta prueba piloto ha sido el establecimiento de una plataforma de consolidación o base micro logística, céntricamente situada, que requiriera de mínimas intervenciones, y a la que pudieran acceder camiones de cierto tamaño para trasvasar la mercancía a la flota eléctrica que se emplearía en el posterior reparto capilar.

Tras un proceso de búsqueda de posibles emplazamientos que comenzó en la primavera de 2013, se acordó la instalación de dicha plataforma logística en Legazpi; concretamente en una parte del antiguo Mercado de Frutas y Verduras cedida temporalmente por el Ayuntamiento madrileño para este fin. En dichas instalaciones se procedió asimismo a la instalación de la infraestructura de carga adecuada para los vehículos que se están utilizando en el proyecto, actuación que ha sido llevada a cabo por la empresa española IBIL.

En concreto, la infraestructura de recarga instalada incluye:

- 1 punto trifásico a 32 Amperios
- 1 punto trifásico a 16 Amperios
- 3 puntos de recarga monofásicos a 16 Amperios.

**CUADRO 2**  
**DATOS DE LA OPERATIVA DIARIA DE TNT EN REVUE**

|                                           |                                                                                               |                |
|-------------------------------------------|-----------------------------------------------------------------------------------------------|----------------|
| Vehículos                                 | ★ Renault Kangoo Z.E.                                                                         |                |
|                                           | Horas al día trabajando                                                                       | 9              |
|                                           | Franja horaria                                                                                | Mañana y tarde |
| Trabajo diario                            | Número de conductores                                                                         | 1              |
|                                           | Número de entregas                                                                            | 6 toneladas    |
|                                           | Kilómetros                                                                                    | 19/48/500      |
| Tipo de mercancía transportada            | Paquetería                                                                                    |                |
| Tipo de clientes                          | Empresas y particulares                                                                       |                |
| Localización y frecuencia de las entregas | Generalmente durante la mañana, empezado a las 9:30 am y finalizando por la tarde a las 17:30 |                |
| Área de influencia                        | Barrio de las Letras-Embajadores                                                              |                |

FUENTE: Elaboración propia.

**CUADRO 3**  
**DATOS DE LA OPERATIVA DIARIA DE SEUR EN REVUE**

|                                           |                                                                                               |                |
|-------------------------------------------|-----------------------------------------------------------------------------------------------|----------------|
| Vehículos                                 | ★ Renault Kangoo Z.E.                                                                         |                |
|                                           | Horas al día trabajando                                                                       | 9              |
|                                           | Franja horaria                                                                                | Mañana y tarde |
| Trabajo diario                            | Número de conductores                                                                         | 1              |
|                                           | Kilómetros                                                                                    | 6 toneladas    |
|                                           | Kilómetros                                                                                    | 50-100 km      |
| Tipo de mercancía transportada            | Paquetería                                                                                    |                |
| Tipo de clientes                          | Empresas y particulares                                                                       |                |
| Localización y frecuencia de las entregas | Generalmente durante la mañana, empezado a las 9:00 am y finalizando por la tarde a las 18:00 |                |
| Área de influencia                        | Desde Plaza de España a Moncloa.                                                              |                |

FUENTE: Elaboración propia.

Estas actividades de reparto comenzaron el pasado 17 de febrero de 2014, y se prolongarán por un periodo de aproximadamente dos años. El proyecto, que cuenta con un presupuesto de casi un millón de euros, del que la Unión Europea aporta más del 50 por ciento, y el resto llega de los socios españoles y el Ayuntamiento. Esto está permitiendo que los operadores logísticos cuenten actualmente con 4 vehículos eléctricos comerciales de distintas tipologías para el desempeño de su actividad diaria.

Los buenos resultados preliminares hacen presagiar que, en términos de gestión de la ciudad, podría ser una medida a replicar en otros emplazamientos a corto o medio plazo. En este sentido, los primeros resultados, que aún están en fase de evaluación, muestran unos datos de ahorro de 4 toneladas de CO<sub>2</sub> por vehículo y año<sup>1</sup>, lo que da una idea del potencial ahorro en emisiones no sólo de CO<sub>2</sub>, sino de óxidos de nitrógeno o partículas si este tipo de soluciones se generalizara. Hay que tener en cuenta que, de acuerdo a datos de 2009, tan sólo el municipio de Madrid contaba con 234.301 furgonetas y camiones censados, cifra que aumentaba hasta los 643.687 para el conjunto de la Comunidad de Madrid, siendo en su gran mayoría vehículos diésel.

Las ventajas no sólo se generan desde el punto de vista ambiental (calidad del aire y ruido), sino también

desde el punto de vista de operatividad y costes. Este segundo aspecto es fundamental para los operadores logísticos. Después de estos primeros meses de funcionamiento, los socios participantes están evaluando los ahorros que supone utilizar flota eléctrica en términos de combustible y mantenimiento de los vehículos, y los números son claramente favorables. A este hecho se une el que la mayoría de las ciudades, Madrid incluida, contemplan incentivos y ventajas para los vehículos comerciales menos contaminantes, lo que añade ventajas operativas en lo que a la definición de la logística diaria se refiere.

En cuanto a cifras de actividad de cada uno de los operadores participantes en el proyecto se tiene que (1):

- Calidad Pascual: 6.000 kg transportados al día en 44 servicios diarios realizados
- TNT: 200 kg transportados al día en 20 servicios diarios realizados
- SEUR: 400 kg transportados al día en 75 servicios diarios realizados

Asimismo, destacar que, por ejemplo, Calidad Pascual está ya trabajando en el desarrollo de dos proyectos pilotos en la misma línea en Barcelona y un tercero en Málaga debido al éxito de la iniciativa pionera de Madrid, mientras que otro de los operadores logísticos colaboradores en el proyecto, TNT, reconoce el ahorro

en transporte que supone centralizar estas tareas de distribución, y ya tiene en marcha la introducción de un segundo vehículo eléctrico.

Desde el punto de vista municipal, y más allá de los motivos ambientales mencionados, la ciudad de Madrid considera que del proyecto pueden derivarse otros interesantes beneficios, tales como:

- Contribuir al desarrollo de nuevos modelos de negocio, a partir de la mejora de la eficiencia en el sistema de distribución urbana de mercancías, probando innovadoras soluciones tecnológicas que contribuyan al desarrollo de nuevas líneas de innovación y dinamización económica.
- Proporcionar mayor visibilidad a nuevas tecnologías de movilidad que aportan beneficios ambientales y contribuyen a sensibilizar a la ciudadanía.
- Posicionar a la ciudad y a las entidades, instituciones y empresas colaboradoras como referencias punteras a nivel nacional y europeo mediante el intercambio de experiencias con otras ciudades.
- Y en definitiva, mantener el impulso municipal de la movilidad sostenible y contribuir a la mejor implantación de las diferentes políticas y estrategias públicas, incluido, por supuesto, el propio Plan de Movilidad Urbana Sostenible de la ciudad.

Uno de los aspectos que está ayudando especialmente a los operadores logísticos a realizar el seguimiento del funcionamiento de la flota eléctrica empleada, y de como ésta se adapta a sus requerimientos, es la utilización de la herramienta desarrollada por ITENE, que permite monitorizar en tiempo real el funcionamiento de los vehículos eléctricos empleados en el proyecto piloto.

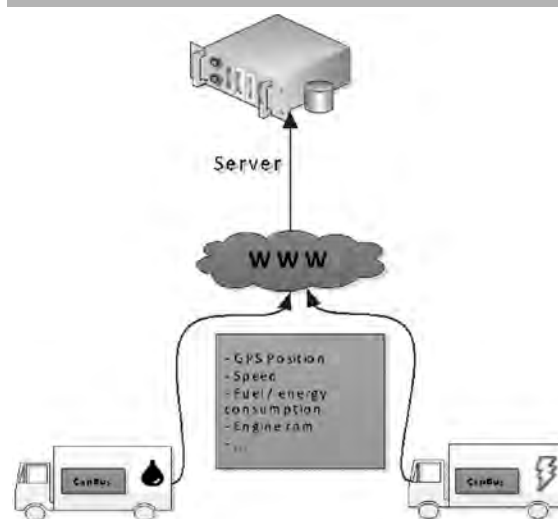
A tal fin, y previo acuerdo con los fabricantes de los vehículos empleados en el proyecto, se han instalado unos *data loggers* que recogen en tiempo real datos tales como la posición GPS, la velocidad, el consumo eléctrico, el nivel de batería, la autonomía restante, las horas de conducción y los arranques y paradas realizados. Toda la información es accesible en tiempo real por los propios operadores logísticos, que pueden así realizar el seguimiento de sus operaciones. Así mismo, la herramienta permite elaborar informes de seguimiento a partir de unas plantillas establecidas, con gráficas de los distintos parámetros medidos, para un mejor control y seguimiento.

## DESARROLLO DE LA HERRAMIENTA DE MONITORIZACIÓN

### Objetivos

Tal como se ha mencionado anteriormente, uno de los objetivos del piloto de Madrid es el desarrollo y testeo de una herramienta de gestión de flotas de vehículos eléctricos que permita la monitorización en tiempo real de los parámetros más relevantes en la conducción y operativa de distribución mediante este tipo de vehículos.

**FIGURA. 1**  
**ESQUEMA DE LA HERRAMIENTA DE GESTIÓN DE FLOTAS**



FUENTE: Elaboración propia.

El objetivo de la herramienta es la monitorización en tiempo real de la actividad y rendimiento de los vehículos eléctricos. Los parámetros claves que se monitorizan son:

- Posición GPS
- Velocidad
- Consumo electricidad
- Nivel de batería
- Autonomía
- Horas de conducción
- Arranques y paradas
- Temperatura

En la actualidad, esta herramienta permite gestionar eficazmente las recargas eléctricas y las rutas de reparto de «última milla» de los 3 operadores logísticos que participan en el proyecto: SEUR, TNT y CALIDAD PAS-CUAL.

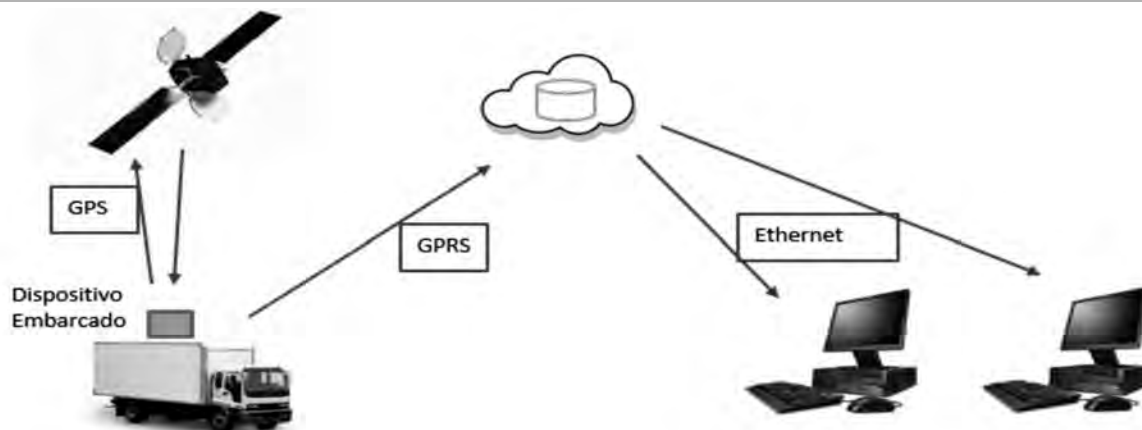
La figura 1 muestra el esquema de la herramienta de gestión de flotas desarrollada que puede ser utilizada tanto en vehículos eléctricos como en vehículos convencionales con el fin de comparar sus rendimientos:

A continuación, en el siguiente apartado, se explican las características técnicas de la herramienta y de los mecanismos para la obtención de datos del rendimiento de los vehículos.

### Características técnicas de la herramienta

La herramienta de monitorización consta de dos elementos principales: un sistema de adquisición de da-

**FIGURA 2**  
**ELEMENTOS PRINCIPALES DE LA HERRAMIENTA DE MONITORIZACIÓN**



FUENTE: Elaboración propia.

tos embarcado en el vehículo y de un *software* de gestión de flotas.

El sistema embarcado extrae los datos de la red CAN BUS (acrónimo del inglés *Controller Area Network*) del vehículo eléctrico. La red CAN BUS es el sistema de transmisión de mensajes en entornos distribuidos que utilizan todos los sensores y nodos del vehículo, y por ella circula todo tipo de información tal como la velocidad, el porcentaje de batería remanente, el consumo eléctrico acumulado, la posición del freno y acelerador, etc. Se puede decir, en términos generales, que el CAN BUS es un protocolo de comunicación que actúa como la columna que vertebra toda la electrónica de los coches, tanto convencionales como eléctricos.

Desde hace unos años, la electrónica se ha hecho un hueco importante en los automóviles. La aplicación masiva de sistemas electrónicos de control y regulación en el vehículo motorizado como por ejemplo el control del cambio, el control electrónico del motor o de la bomba de inyección, el sistema antibloqueo (ABS), el sistema de tracción antideslizante (ASR), el control de estabilidad (ESP), el ordenador de a bordo, etc. requieren una interconexión en red de las diversas unidades de control.

Por este motivo, dado que no es posible conectar los dispositivos electrónicos que se instalan en los vehículos mediante cables directos punto a punto, en 1992 se definió en protocolo de comunicaciones CAN para el sector automoción. CAN es el acrónimo de *Controller Area Network* y el término *bus* se debe a su topología en forma de bus. De esta forma, las interfaces de los sistemas de comunicación desarrollados especialmente para vehículos motorizados, han pasado de ser interfaces convencionales a interfaces en serie como el CAN (*Controller Area Network*).

En términos sencillos, se podría decir que en los vehículos actuales existe un solo que recorre el vehículo al que se van conectando los diferentes aparatos elec-

trónicos que necesitan comunicarse. De esta forma se recude la cantidad de cables que se necesitan en el coche para conectar entre otros los dispositivos como los elevadores eléctricos, el climatizador, el cierre centralizado, el techo solar, los asientos eléctricos, la centralita de la inyección y todos sus sensores, el cuadro de instrumentos, los mandos en el volante o los sistemas multimedia. Cualquier dispositivo electrónico conectado al bus puede mandar mensajes y el resto le escuchan. Cada tipo de mensaje lleva un identificador. Este identificador representa el contenido del mensaje (por ejemplo, el número de revoluciones del motor en vehículos convencionales o el porcentaje de batería en vehículos eléctricos).

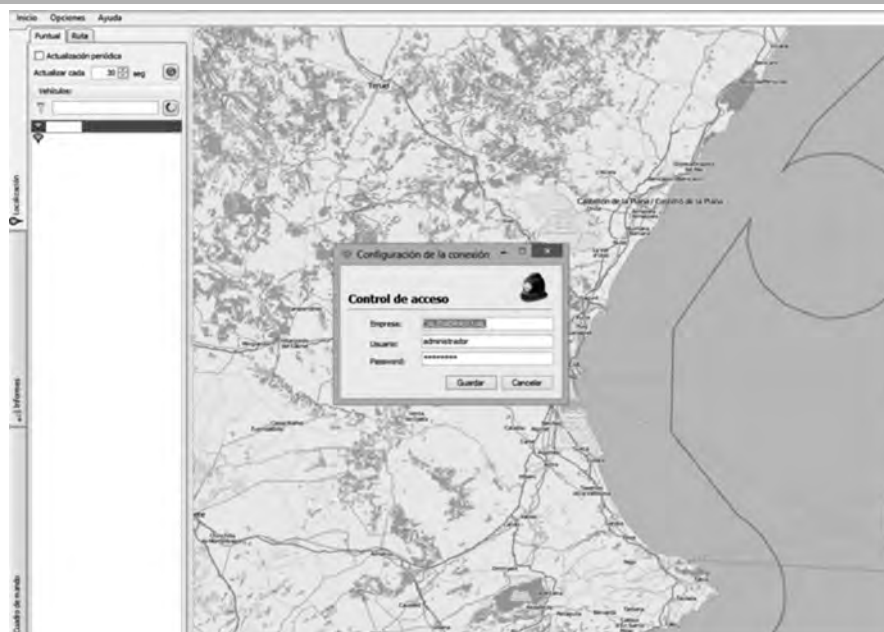
Otro uso de este protocolo es para los servicios de diagnóstico y la toma de datos del vehículo. Los coches tienen un conector especial llamado OBD que suele encontrarse debajo del volante. Este conector permite acceder a los buses CAN del automóvil. Con un adaptador podemos conectar un ordenador, smartphone o similar y así nos enteraremos de todo lo que se cuece en el interior de nuestro coche. De hecho, este conector es el que se ha utilizado para la monitorización de los vehículos eléctricos participantes en FREVUE.

Por otra parte, la herramienta embarcada tiene además un dispositivo de geoposicionamiento GPS que permite localizar inequívocamente el vehículo en tiempo y espacio. Todos estos datos son enviados mediante una conexión GPRS –General Packet Radio Service o Servicio General de Paquetes vía Radio– a un servidor central, y almacenados en tiempo real para el uso por el software de gestión de flotas. Los elementos principales de la herramienta de monitorización se describen en la figura 2.

Hay que tener especial cuidado con el protocolo CAN BUS que utiliza el vehículo, pues generalmente varía según modelo y marca. Para asegurar una correcta adquisición de todos los datos, el sistema de embarcado los convierte antes de ser enviados al estándar FMS



**FIGURA 3**  
**LOGIN DEL USUARIO: APLICACIÓN WEB CON ACCESO RÁPIDO DESDE ESCRITORIO**



FUENTE: Imagen extraída de la herramienta desarrollada por ITENE.

(FMS Standard, 2015), un estándar de comunicación basado es el protocolo de comunicación J1939 para el envío de datos por CAN BUS. El J1939 (SAE, 2015) es un protocolo de mensajería de alto nivel que define el funcionamiento de la comunicación entre las diferentes Unidades de Control Electrónico (ECUs, Electronic Control Units, por sus siglas en inglés) en el CAN BUS físico de un vehículo.

El almacenamiento de datos en el servidor central se basa en un servicio de escucha permanente, que captura los datos llegados al puerto de comunicaciones y los introduce en la base de datos postgresSQL maestra del sistema. Los datos aquí introducidos son redirigidos a una segunda base de datos por empresa para asegurar un funcionamiento autónomo e independiente entre las diferentes empresas que utilicen el servicio.

La aplicación cliente del sistema es la que utilizan los usuarios del sistema para conectarse a la base de datos, extraer la información deseada y procesarla. De esta forma, la herramienta desarrollada permite la monitorización del vehículo en tiempo real desde centro de operaciones de las empresas sin interferir en las actividades diarias de los conductores. En este sentido, otro beneficio de este tipo de herramientas aplicada en este caso a vehículos eléctricos, es el registro automático de datos para análisis de aspectos como tiempos de conducción, rutas de reparto, condiciones de tráfico, productividad de los servicios, costes y beneficios ambientales.

### Funcionalidades ▾

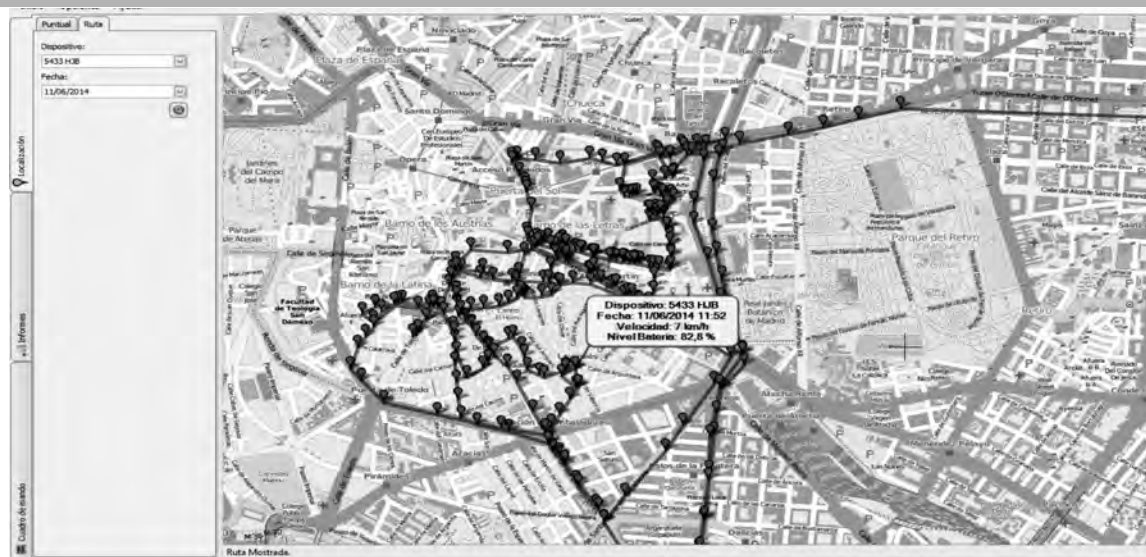
Entre las funcionalidades de la herramienta de gestión de flotas de vehículos eléctricos destacan las siguientes:

- Dispone de un fácil acceso por parte del usuario mediante soporte Web y aplicación de escritorio (ver ejemplo figura 3).
- Dispone de localización de los vehículos en tiempo real (ver ejemplo de la figura 4, en la página siguiente)
- Permite la optimización de rutas a través de la continua monitorización del nivel de batería y autonomía del vehículo .
- Proporciona informes de actividad de los vehículos con la posibilidad de añadir una representación gráfica de aspectos relativos a la conducción eficiente o al efecto que tienen en el rendimiento de los vehículos eléctricos parámetros como la temperatura, la carga transportada, la inclinación de la ruta, las condiciones de tráfico, la vida de la batería, etc.
- Ofrece además la posibilidad de establecer sistema de alertas para detectar excesos de velocidad, de consumos, de duración de paradas, etc.

Asimismo, conviene mencionar también que la herramienta desarrollada, además de fomentar la conducción eficiente, también es aplicable a vehículos convencionales por lo que permite comparar rendimientos de distintos tipos de vehículos en términos de eficiencia, productividad, costes o impacto ambiental.

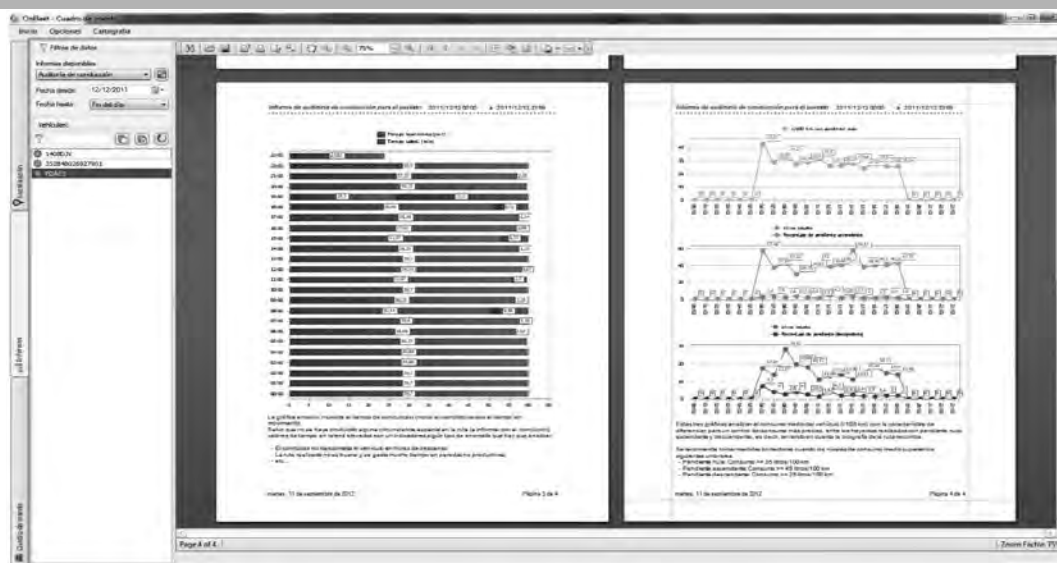
Toda esta información, se traslada a los informes de actividad del vehículo eléctrico que son accesibles para los usuarios de la herramienta. Estos informes presentan los principales parámetros de actividad para cada vehículo eléctrico monitorizado. Los informes de actividad de los vehículos permiten extra por día, semana o mes los siguientes indicadores:

**FIGURA 4**  
**EJEMPLO DE POSICIONAMIENTO DEL VEHÍCULO ELÉCTRICO Y REGISTRO DEL RECORRIDO**



FUENTE: Imagen extraída de la herramienta desarrollada por ITENE.

**FIGURA 5**  
**EJEMPLO DE INFORME DE ACTIVIDAD DEL VEHÍCULO ELÉCTRICO**



FUENTE: Imagen extraída de la herramienta desarrollada por ITENE.

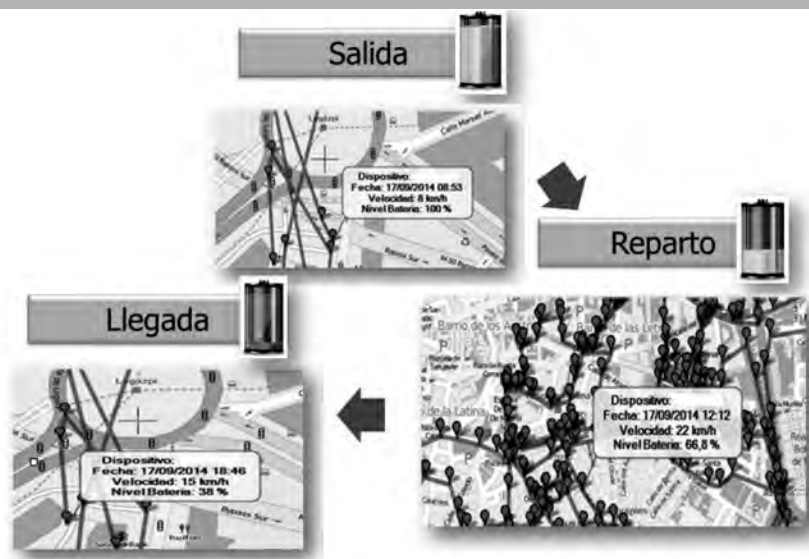
- Kilómetros recorridos (km).
- Consumo de energía (kWh).
- Consumo medio (kWh/100km).
- Tiempo de operación (horas).
- Velocidad media y máxima (km/h).
- Servicios realizados (#).
- Peso transportado (kg).
- Productividad (núm. servicios / km).
- Costes por servicio (€).
- Tiempo medio por servicio (minutos).

De esta forma, tal y como muestra la figura 5, la herramienta permite obtener información gráfica sobre:

- El consumo eléctrico de cada vehículo.
- El efecto de la temperatura en el rendimiento de la batería.
- El efecto de los ciclos de la batería (vida útil) en el rendimiento de la batería.
- El efecto del peso transportado en los consumos eléctricos.
- El efecto de arranques y paradas en el rendimiento de la batería.



**FIGURA 6**  
**EJEMPLO DE MONITORIZACIÓN DE VEHÍCULOS EN TIEMPO REAL**



FUENTE: Elaboración propia.

- El efecto de la pendiente de la ruta en los consumos eléctricos.
- El efecto del estilo de conducción en el funcionamiento del freno regenerativo.

A modo de resumen, entre los principales beneficios de esta herramienta para los operadores logísticos conviene destacar los siguientes:

- La posibilidad de monitorización del vehículo en tiempo real desde centro de operaciones de la empresa.
- La posibilidad de optimización de rutas y servicios a través de:
  - la planificación de las rutas de reparto de la empresa
  - la planificación de los pasos por puntos de recarga
  - Registro automático de datos para análisis de, entre otros, los siguientes aspectos:
    - los tiempos de conducción
    - las rutas
    - las condiciones de tráfico
    - la conducción eficiente por parte de los conductores
    - la productividad de los servicios
    - los costes de los servicios
    - los beneficios ambientales basados en la reducción de emisiones contaminantes (CO<sub>2</sub>, NOX, Partículas, etc.)

Todo esto permite aumentar la eficiencia y productividad de las entregas y recogidas a realizar por parte de los conductores de las empresas participantes en el proyecto como son SEUR, TNT y CALIDAD PASCUAL, teniendo información en todo momento del estado de la batería desde el centro de operaciones de la empresa tal y como se muestra en la figura 6.

En la figura 6 se pueden observar los parámetros monitorizados en todo momento como son la fecha y hora, la velocidad en cada instante y el nivel de batería, factor crítico a controlar en el caso particular de los vehículos eléctricos cuya autonomía es limitada. En este sentido, cabe añadir que el sistema puede servir de herramienta de aprendizaje para los conductores quienes no están acostumbrados a conducir este tipo de vehículos. Disponer de los rendimientos de la batería en función de la ruta, carga, hora del día puede ser de mucha utilidad de cara a optimizar al máximo la autonomía de los vehículos y a fomentar la conducción eficiente por parte de los conductores.

Asimismo, es una herramienta de mucha utilidad para los jefes de operaciones quienes pueden controlar los rendimientos de distintos vehículos eléctricos de su flota desde el centro de operaciones, así como obtener informes de actividad a posteriori para mejorar la eficiencia de los repartos día a día.

## CONCLUSIONES

A modo de conclusión, es importante resaltar los beneficios de la herramienta de gestión de flotas de vehículos eléctricos desarrollada por ITENE dentro del proyecto FREVUE. Entre estos beneficios se encuentra la optimización de rutas y servicios, a través de la planificación de las rutas de reparto y de los pasos por puntos de recarga gracias a la información en tiempo real que aporta la herramienta. Por otra parte, y al tratarse de vehículos que son nuevos para la mayoría de los conductores y empresas, la herramienta fomenta la conducción eficiente ya que permite el aprendizaje en base al análisis de la actividad del vehículo.

Además, y tal y como se ha mencionado anteriormente, la herramienta desarrollada permite la monitoriza-

ción del vehículo en tiempo real desde el centro de operaciones de las empresas sin interferir en las actividades diarias de los conductores. En este sentido, otro beneficio de este tipo de herramientas aplicada en este caso a vehículos eléctricos, es el registro automático de datos para el análisis de aspectos como tiempos de conducción, rutas de reparto, condiciones de tráfico, productividad de los servicios, costes y beneficios ambientales.

Por último, conviene mencionar también que la herramienta desarrollada, además de fomentar la conducción eficiente, también es aplicable a vehículos convencionales por lo que permite comparar rendimientos de distintos tipos de vehículos en términos de eficiencia, productividad, costes o impacto ambiental.

Para finalizar, conviene remarcar que este tipo de iniciativas en las que las administraciones y el tejido económico y social colaboran estrechamente, permiten desarrollar soluciones innovadoras que ayudan a hacer de nuestras ciudades mejores lugares para vivir, ciudades más amables y sostenibles que contribuyen al mejor desarrollo de nuestra sociedad.

## NOTAS†

- [1] Estimando una distancia media recorrida al día de 75 kilómetros; durante 250 días al año; considerando un factor de emisión del diésel de 2,67 kgCO<sub>2</sub>eq. Por cada litro consumido (Referencia: Norma UNE-EN 16258:2013 «Metodología para el cálculo y la declaración del consumo de energía y de las emisiones de gases de efecto invernadero en los servicios de transporte de mercancías y de pasajeros»); y comparándolo con una furgoneta diésel convencional que consume 8 litros por cada 100km.

## BIBLIOGRAFÍA‡

- AYUNTAMIENTO DE MADRID (2014). Informe del Estado de la Movilidad de la Ciudad de Madrid 2013. 6º Informe del Estado de la Movilidad de la Ciudad de Madrid 2013. Diciembre de 2014. Disponible en < [www.madrid.es/UnidadesDescentralizadas/UDCMovilidadTransportes/MOVILIDAD/InformeEstadoMovilidad/ficheros/Sexto%20Informe%20Estado%20Movilidad%202013.pdf](http://www.madrid.es/UnidadesDescentralizadas/UDCMovilidadTransportes/MOVILIDAD/InformeEstadoMovilidad/ficheros/Sexto%20Informe%20Estado%20Movilidad%202013.pdf) >
- BOE (2011). Real Decreto 102/2011, de 28 de enero, relativo a la mejora de la calidad del aire. Ministerio de la Presidencia, Madrid. Disponible en < [www.boe.es/diario\\_boe/txt.php?id=BOE-A-2011-1645](http://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-1645) >
- ECOLOGISTAS EN ACCIÓN (2014). La calidad del aire en el Estado español durante 2013. Hecho público el 8 de octubre de 2014. Disponible en < [www.ecologistasenaccion.org/IMG/pdf/informe\\_calidad\\_aire\\_2013.pdf](http://www.ecologistasenaccion.org/IMG/pdf/informe_calidad_aire_2013.pdf) >
- ERTRAC (2014). «European Road Transport Research Advisory Council. Urban Freight research roadmap». Consejo Consultivo Europeo de Investigación del Transporte por Carretera. Noviembre 2014. Disponible en: < [www.ertrac.org/uploads/documentsearch/id36/ERTRAC\\_Alice\\_Urban\\_Freight.pdf](http://www.ertrac.org/uploads/documentsearch/id36/ERTRAC_Alice_Urban_Freight.pdf) >
- FMS Standard (2015). Disponible en: < [www.fms-standard.com](http://www.fms-standard.com) >
- FREVUE (2013). Vehículos eléctricos en la Europa Urbana. «Freight Electric Vehicles in Urban Europe». Séptimo Programa Marco de la Unión Europea. «Seventh Framework Programme» (FP7). Grant agreement no.: 321622. Disponible en < [www.frevue.eu](http://www.frevue.eu) >
- IEA (2014). «International Energy Agency. CO<sub>2</sub> emissions from fuel combustion highlights». Agencia Internacional de la Energía. Emisiones de CO<sub>2</sub> de la combustión de combustibles. Disponible en < [www.iea.org/publications/freepublications/publication/CO2EmissionsFromFuelCombustionHighlights2014.pdf](http://www.iea.org/publications/freepublications/publication/CO2EmissionsFromFuelCombustionHighlights2014.pdf) >
- MINISTERIO DE AGRICULTURA, ALIMENTACIÓN Y MEDIO AMBIENTE (2013). Dirección General de Calidad y Evaluación Ambiental y Medio Natural. Subdirección General de Calidad del Aire y Medio Ambiente Industrial. Plan Nacional de Calidad del Aire y Protección de la Atmósfera 2013-2016. Plan AIRE. Disponible en < [www.lamoncloa.gob.es/espana/eh15/medioambiente/Documents/PLAN\\_AIRE\\_2013-2016\\_tcm7-271018.pdf](http://www.lamoncloa.gob.es/espana/eh15/medioambiente/Documents/PLAN_AIRE_2013-2016_tcm7-271018.pdf) >
- OMS (2014). Organización Mundial de la Salud. World Health Organisation. Air quality deteriorating in many of the world's cities. Disponible en < [www.who.int/mediacentre/news/releases/2014/air-quality/en/](http://www.who.int/mediacentre/news/releases/2014/air-quality/en/) >
- SAE (2015). Sociedad de Ingeniería Automotriz SAE. Disponible en < [www.saedigitalibrary.org/corporate/small-business/11939/](http://www.saedigitalibrary.org/corporate/small-business/11939/) >



# **Uniform provisions concerning the approval of motor vehicles with regard to the Event Data Recorder**

21 October 2021

---

## **Agreement**

### **Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations\***

(Revision 3, including the amendments which entered into force on 14 September 2017)

---

#### **Addendum 159 – UN Regulation No. 160**

Date of entry into force as an annex to the 1958 Agreement: 30 September 2021

#### **Uniform provisions concerning the approval of motor vehicles with regard to the Event Data Recorder**

This document is meant purely as documentation tool. The authentic and legal binding text is: ECE/TRANS/WP.29/2020/123/Rev.1.



**UNITED NATIONS**

---

\* Former titles of the Agreement:

Agreement concerning the Adoption of Uniform Conditions of Approval and Reciprocal Recognition of Approval for Motor Vehicle Equipment and Parts, done at Geneva on 20 March 1958 (original version); Agreement concerning the Adoption of Uniform Technical Prescriptions for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these Prescriptions, done at Geneva on 5 October 1995 (Revision 2).

## UN Regulation No. 160

### Uniform provisions concerning the approval of motor vehicles with regard to the Event Data Recorder

#### Contents

|                                                                                                                                   | <i>Page</i> |
|-----------------------------------------------------------------------------------------------------------------------------------|-------------|
| Regulation                                                                                                                        |             |
| 0. Introduction .....                                                                                                             | 4           |
| 1. Scope .....                                                                                                                    | 4           |
| 2. Definitions .....                                                                                                              | 4           |
| 3. Application for approval .....                                                                                                 | 8           |
| 4. Approval .....                                                                                                                 | 8           |
| 5. Requirements.....                                                                                                              | 9           |
| 6. Modification of vehicle type and extension of approval .....                                                                   | 11          |
| 7. Conformity of production .....                                                                                                 | 11          |
| 8. Penalties for non-conformity of production .....                                                                               | 12          |
| 9. Production definitively discontinued.....                                                                                      | 12          |
| 10. Names and addresses of Technical Services responsible for conducting approval tests,<br>and of Type Approval Authorities..... | 12          |
| Annexes                                                                                                                           |             |
| 1 Communication .....                                                                                                             | 13          |
| 2 Information document on the type approval of a vehicle type with regards to its Event<br>Data Recorder (EDR).....               | 14          |
| 3 Arrangements of approval marks .....                                                                                            | 15          |
| 4 Data elements and format.....                                                                                                   | 16          |

## 0. Introduction

- 0.1. The intention of this Regulation is to establish uniform provisions concerning the approval of motor vehicles of the Categories M<sub>1</sub> and N<sub>1</sub> with regard to their Event Data Recorders (EDRs).
- 0.2. The provisions concern the minimum collection, storage and crash survivability of motor vehicle crash event data. It does not include specifications for data retrieval tools and methods as that is subject to national/regional level requirement.
- 0.3. The purpose of these provisions is to ensure that EDRs record, in a readily usable manner, data valuable for effective crash investigations and for analysis of safety equipment performance (e.g., advanced restraint systems). These data will help provide a better understanding of the circumstances in which crashes and injuries occur and will facilitate the development of safer vehicle designs.

## 1. Scope

- 1.1. This Regulation applies to the approval of vehicles of categories M<sub>1</sub> and N<sub>1</sub><sup>1</sup> with regard to their Event Data Recorder (EDR).
- 1.2. This Regulation is without prejudice to requirements of national or regional laws related to privacy, data protection and personal data processing.
- 1.3. The following data elements are excluded from the scope: VIN, associated vehicle details, location/positioning data, information of the driver, and date and time of an event.
- 1.4. If there is no system or sensor designed to provide the data element to be recorded and stored under section 3, in the format (range, resolution, and sample rate) indicated in Annex 4. "DATA ELEMENTS" or it is not operational at the time of recording, this document requires neither recording of such data nor fitting or making such systems or sensors operational. However, if the vehicle is fitted with an original equipment manufacturer sensor or system designed to provide the data element in the format specified in Annex 4. "DATA ELEMENTS", then it is mandatory to report the data element in the specified format when the sensor or system is operational. In the case the reason for not being operational at the time of recording is a failure of this system or sensor, this failure state shall be recorded by the EDR as defined in the data elements Annex 4. Data elements.

## 2. Definitions

For the purposes of these performance elements:

- 2.1. "*ABS activity*" means the anti-lock brake system (ABS) is actively controlling the vehicle's brakes.
- 2.2. "*Air bag warning lamp status*" means whether the air bag malfunction warning lamp is on or off.
- 2.3. "*Capture*" means the process of buffering EDR data in a temporary, volatile storage where it is continuously updated at regular time intervals.

---

<sup>1</sup> As defined in Section 2 of the Consolidated Resolution on the Construction of Vehicles (R.E.3) (document ECE/TRANS/WP.29/78/Rev.6) –<https://unece.org/transport/standards/transport/vehicle-regulations-wp29/resolutions>.

- 2.4. "*Delta-V, lateral*" means the cumulative change in velocity, as recorded by the EDR of the vehicle, along the lateral axis.
- 2.5. "*Delta-V, longitudinal*" means the cumulative change in velocity, as recorded by the EDR of the vehicle, along the longitudinal axis.
- 2.6. "*Deployment time, frontal air bag*" means (for both driver and front passenger) the elapsed time from crash time zero to the deployment command or for multi-staged air bag systems, the deployment command for the first stage.
- 2.7. "*End of event time*" means the moment at which the cumulative delta-V within a 20 ms time period becomes 0.8 km/h or less, or the moment at which the crash detection algorithm of the air bag control unit resets.
- 2.8. "*Engine RPM*" means:
- (a) For vehicles powered by internal combustion engines, the number of revolutions per minute of the main crankshaft of the vehicle's engine, and
  - (b) For vehicles not entirely powered by internal combustion engines, the number of revolutions per minute of the motor shaft at the point at which it enters the vehicle transmission gearbox, and
  - (c) For vehicles not powered by internal combustion engines at all, the number of revolutions per minute of the output shaft of the device(s) supplying motive power.
- 2.9. "*Engine throttle, percent full*" means the driver-requested acceleration as measured by the throttle position sensor on the accelerator control compared to the fully depressed position.
- 2.10. "*Event*" means a crash or other physical occurrence that causes the trigger threshold to be met or exceeded, or any non-reversible deployable restraint to be deployed, whichever occurs first.
- 2.11. "*Event data recorder*" (EDR) means a device or function in a vehicle that records the vehicle's dynamic, time-series data during the time period just prior to an event (e.g., vehicle speed vs. time) or during a crash event (e.g., delta-V vs. time), intended for retrieval after the crash event. For the purposes of this definition, the event data does not include audio and video data.
- 2.12. "*Frontal air bag*" means an inflatable restraint system that requires no action by vehicle occupants and is used to meet the applicable national frontal crash protection requirements.
- 2.13. "*If recorded*" means if data is recorded in non-volatile memory for the purpose of subsequent downloading.
- 2.14. "*Ignition cycle, crash*" means the number (count) of power mode cycles at the time when the crash event occurred since the first use of the EDR.
- 2.15. "*Ignition cycle download*" means the number (count) power mode cycles at the time when the data was downloaded since the first use of the EDR.
- 2.16. "*Lateral acceleration*" means the component of the vector acceleration of a point in the vehicle in the y-direction. The lateral acceleration is positive from left to right, from the perspective of the driver when seated in the vehicle facing the direction of forward vehicle travel.
- 2.17. "*Longitudinal acceleration*" means the component of the vector acceleration of a point in the vehicle in the x-direction. The longitudinal acceleration is positive in the direction of forward vehicle travel.
- 2.18. "*Maximum delta-V, lateral*" means the maximum value of the cumulative change in velocity, as recorded by the EDR, of the vehicle along the lateral axis.

- 2.19. "*Maximum delta-V, longitudinal*" means the maximum value of the cumulative change in velocity, as recorded by the EDR, of the vehicle along the longitudinal axis.
- 2.20. "*Maximum delta-V, resultant*" means the time-correlated maximum value of the cumulative change in velocity, as reported by the EDR, along the vector-added longitudinal and lateral axis.
- 2.21. "*Multi-event crash*" means the occurrence of a minimum of 2 events, the first and last of which begin not more than 5 seconds apart.
- 2.22. "*Non-volatile memory*" means the memory reserved for maintaining recorded EDR data in a semi-permanent fashion. Data recorded in non-volatile memory is retained after a loss of power and can be retrieved with EDR data extraction tools and methods.
- 2.23. "*Normal acceleration*" means the component of the vector acceleration of a point in the vehicle in the z-direction. The normal acceleration is positive in a downward direction.
- 2.24. "*Occupant size classification*" means, for front passenger, the classification of an occupant as an adult and not a child, and for the driver, the classification of the driver as not being of small stature as indicated in the data format.
- 2.25. "*Operational*" means that the system or sensor, at the time of the event, is active or can be activated/deactivated by the driver.
- 2.26. "*Passenger air bag suppression status*" means the status of the passenger air bag (suppressed or not suppressed).
- 2.27. "*Pretensioner*" means a device that is activated by a vehicle's crash sensing system and removes slack from a vehicle safety belt system.
- 2.28. "*Record*" means the process of saving captured EDR data into a non-volatile storage for subsequent retrieval.
- 2.29. "*Safety belt status*" means the feedback from the safety system that the vehicle's safety belt is fastened or unfastened.
- 2.30. "*Seat track position switch, foremost, status*" means the status of the switch that is installed to detect whether the seat is moved to a forward position.
- 2.31. "*Service brake, on and off*" means the status of the device that is installed in or connected to the brake pedal system to detect whether the pedal was pressed. The device can include the brake pedal switch or other driver-operated service brake control.
- 2.32. "*Side air bag*" means any inflatable occupant restraint device that is mounted to the seat or side structure of the vehicle interior, and that is designed to deploy in a side impact crash to help mitigate occupant injury and/or ejection.  
*Note:* Side air bags can also deploy in other crash modes as determined by the vehicle manufacturer.
- 2.33. "*Side curtain/tube air bag*" means any inflatable occupant restraint device that is mounted to the side structure of the vehicle interior, and that is designed to deploy in a side impact crash or rollover and to help mitigate occupant injury and/or ejection.  
*Note:* Side curtain/tube air bags can also deploy in other crash modes as determined by the manufacturer.
- 2.34. "*Speed, vehicle indicated*" means the vehicle speed indicated by a manufacturer-designated subsystem designed to indicate the vehicle's ground travel speed during vehicle operation.
- 2.35. "*Stability control*" means any device that complies with national, "Electronic stability control systems".



- 2.36. "*Steering input*" means the angular displacement of the steering wheel measured from the straight-ahead position (position corresponding to zero average steer angle of a pair of steered wheels).
- 2.37. "*Time from event 1 to 2*" means the elapsed time from time zero of the first event to time zero of the second event of a multi-event crash.
- 2.38. "*Time, maximum delta-V, lateral*" means the time from crash time zero to the point where the maximum value of the cumulative change in velocity is found, as recorded by the EDR, along the lateral axis.
- 2.39. "*Time, maximum delta-V, longitudinal*" means the time from crash time zero to the point where the maximum value of the cumulative change in velocity is found, as recorded by the EDR, along the longitudinal axis.
- 2.40. "*Time, maximum delta-V, resultant*" means the time from crash time zero to the point where the maximum delta-V resultant occurs, as reported by the EDR.
- 2.41. "*Time to deploy, pretensioner*" means the elapsed time from crash time zero to the deployment command for the safety belt pretensioner (for both driver and front passenger).
- 2.42. "*Time to deploy, side air bag/curtain*" means the elapsed time from crash time zero to the deployment command for a side air bag or a side curtain/tube air bag (for both driver and front passenger).
- 2.43. "*Time to first stage*" means the elapsed time between time zero and the time when the first stage of a frontal air bag is commanded to fire.
- 2.44. "*Time to nth stage*" means the elapsed time from crash time zero to the deployment command for the nth stage of a frontal air bag (for both driver and front passenger).
- 2.45. "*Time zero*" is the time reference for the EDR data timestamps of an event.
- 2.46. "*Trigger threshold*" means the appropriate parameter has met the conditions for recording an EDR event.
- 2.47. "*Vehicle roll angle*" means the angle between the vehicle y-axis and the ground plane as determined by the sensing system.
- 2.48. "*Vehicle type with regard to its Event Data Recorder*" means vehicles which do not differ significantly in such essential aspects as:
- (a) The manufacturer's trade name or mark;
  - (b) Vehicle features which significantly influence the performances of the EDR; Addition of new trigger(s), new data (elements), or modification in their format, shall not be considered as "significantly influencing the performance of EDR";
  - (c) The main characteristics and design of the EDR.
- 2.49. "*Volatile memory*" means the memory reserved for buffering of captured EDR data. The memory is not capable of retaining data in a semi-permanent fashion. Data captured in volatile memory is continuously overwritten and is not retained in the event of a power loss or retrievable with EDR data extraction tools.
- 2.50. "*Vulnerable road user secondary safety system*" means a deployable vehicle system outside the occupant compartment designed to mitigate injury consequences to vulnerable road users during a collision.
- 2.51. "*X-direction*" means in the direction of the vehicle's X-axis, which is parallel to the vehicle's longitudinal centerline. The X-direction is positive in the direction of forward vehicle travel.
- 2.52. "*Y-direction*" means in the direction of the vehicle's Y-axis, which is perpendicular to its X-axis and in the same horizontal plane as that axis. The

Y-direction is positive from left to right, from the perspective of the driver when seated in the vehicle facing the direction of forward vehicle travel.

- 2.53. "*Z-direction*" means in the direction of the vehicle's Z-axis, which is perpendicular to the X and Y-axes. The Z-direction is positive in a downward direction.
- 2.54. "*Vehicle roll rate*" means the change in angle over time of the vehicle about its X-axis as determined by the sensing system.
- 2.55. "*Vehicle yaw rate*" means the change in angle over time of the vehicle about its Z-axis as determined by the sensing system.

### **3. Application for approval**

- 3.1. The application for approval of a vehicle type with regard to its EDR shall be submitted by the vehicle manufacturer or by his authorized representative to the approval authority of the Contracting Party according to the provisions of Schedule 3 of the 1958 Agreement.
- 3.2. It shall be accompanied by the following documentation (a model of the information document is given in Annex 2):
  - 3.2.1. A description of the vehicle type with regard to the items specified in paragraph 5 below, in particular related to the location of the EDR in the vehicle, the triggering parameters, storing capacity and the resistance to high deceleration and mechanical stress of a severe impact;
  - 3.2.2. The data elements and format stored in the EDR;
  - 3.2.3. Instructions for retrieving data from the EDR.
- 3.3. A vehicle representative of the vehicle type to be approved shall be submitted to the approval authority or its designated technical service responsible for conducting the approval tests.

### **4. Approval**

- 4.1. If the vehicle type submitted for approval pursuant to this Regulation meets the requirements of paragraph 5. below, approval of that vehicle type shall be granted.
- 4.2. An approval number shall be assigned to each type approved. Its first two digits (at present 00 for the Regulation in its original form) shall indicate the series of amendments incorporating the most recent major technical amendments made to the Regulation at the time of issue of the approval. The same Contracting Party shall not assign the same number to another type of vehicle.
- 4.3. Notice of approval or of extension or of refusal or of withdrawal of approval or of production definitively discontinued of a vehicle type pursuant to this Regulation shall be communicated to the Contracting Parties to the Agreement applying this Regulation by means of a form conforming to the model in Annex 1 to this Regulation and documentation supplied by the applicant being in a format not exceeding A4 (210 × 297mm) and on an appropriate scale or electronic format.
- 4.4. There shall be affixed, conspicuously and in a readily accessible place specified on the approval form, to every vehicle conforming to a vehicle type approved under this Regulation, an international approval mark conforming to the model described in Annex 3, consisting of either:
  - 4.4.1. A circle surrounding the letter "E" followed by:

- (a) The distinguishing number of the country which has granted approval;<sup>2</sup> and
- (b) The number of this Regulation, followed by the letter "R", a dash and the approval number to the right of the circle prescribed in this paragraph;

or

- 4.4.2. An oval surrounding the letters "UI" followed by the Unique Identifier.
- 4.5. The approval mark shall be clearly legible and be indelible.
- 4.6. The approval authority shall verify the existence of satisfactory arrangements for ensuring effective checks on conformity of production before type-approval is granted.

## 5. Requirements

Requirements for vehicles fitted with an EDR include data elements, data format, data capture, and crash test performance and survivability.

- 5.1. Data elements
  - 5.1.1. Each vehicle fitted with an EDR shall record the data elements specified as mandatory and those required under specified minimum conditions during the interval/time and at the sample rate specified in Annex 4, Table 1.
- 5.2. Data format
  - 5.2.1. Each data element recorded shall be reported in accordance with the range, accuracy, and resolution specified in Annex 4, Table 1.
  - 5.2.2. Acceleration Time-History data and format: the longitudinal, lateral, and normal acceleration time-history data, as applicable, shall be filtered either during the recording phase or during the data downloading phase to include:
    - 5.2.2.1. The Time Step (TS) that is the inverse of the sampling frequency of the acceleration data and which has units of milliseconds.
    - 5.2.2.2. The number of the first point (NFP), which is an integer that when multiplied by the TS equals the time relative to time zero of the first acceleration data point.
    - 5.2.2.3. The number of the last point (NLP), which is an integer that when multiplied by the TS equals the time relative to time zero of the last acceleration data point; and
    - 5.2.2.4.  $NLP - NFP + 1$  acceleration values sequentially beginning with the acceleration at time  $NFP * TS$  and continue sampling the acceleration at TS increments in time until the time  $NLP * TS$  is reached.
- 5.3. Data capture

The EDR shall record the captured data in the vehicle and this data shall remain in the vehicle subject to the provisions of paragraph 5.3.4, at least until they are retrieved in compliance with national or regional legislation or they are overwritten in compliance with paragraph 5.3.4.

The EDR non-volatile memory buffer shall accommodate the data related to at least two different events.

<sup>2</sup> The distinguishing numbers of the Contracting Parties to the 1958 Agreement are reproduced in Annex 3 to the Consolidated Resolution on the Construction of Vehicles (R.E.3), document ECE/TRANS/WP.29/78/Rev.6 - <https://unece.org/transport/standards/transport/vehicle-regulations-wp29/resolutions>

The data elements for every event shall be captured and recorded by the EDR, as specified in paragraph 5.1 in accordance with the following conditions and circumstances:

- 5.3.1. Conditions for triggering recording of data
  - An event shall be recorded by the EDR if one of the following threshold values is met or exceeded:
    - 5.3.1.1. Change in longitudinal vehicle velocity more than 8 km/h within a 150 ms or less interval.
    - 5.3.1.2. Change in lateral vehicle velocity more than 8 km/h within a 150 ms or less interval
    - 5.3.1.3. Activation of Non-reversible occupant restraint system.
    - 5.3.1.4. Activation of Vulnerable road user secondary safety system
      - If a vehicle is not fitted with any Vulnerable Road User (VRU) secondary safety system, this document requires neither recording of data nor fitting of such systems. However, if the vehicle is fitted with such a system, then it is mandatory to record the event data following activation of this system.
- 5.3.2. Conditions for triggering locking of data
  - In the circumstances provided below, the memory for the event shall be locked to prevent any future overwriting of the data by subsequent event.
    - 5.3.2.1. In all the cases where a non-reversible occupant restraint system is deployed.
    - 5.3.2.2. In the case of a frontal impact, if the vehicle is not fitted with a non-reversible restraint system for front impact, when the vehicle's velocity change in x-axis direction exceeds 25 km/h within 150ms or less interval.
    - 5.3.2.3. Activation of Vulnerable road user secondary safety system
- 5.3.3. Conditions for establishment of time zero
  - Time zero is established at the time when any of the following first occurs:
    - 5.3.3.1. For systems with "wake-up" air bag control systems, the time at which the occupant restraint control algorithm is activated; or
    - 5.3.3.2. For continuously running algorithms,
      - 5.3.3.2.1. The first point in the interval where a longitudinal, cumulative delta-V of over 0.8 km/h is reached within a 20 ms time period; or
      - 5.3.3.2.2. For vehicles that record "delta-V, lateral," the first point in the interval where a lateral, cumulative delta-V of over 0.8 km/h is reached within a 5 ms time period; or
    - 5.3.3.3. Deployment of a non-reversible deployable restraint or activation of VRU secondary safety protection system.
- 5.3.4. Overwriting
  - 5.3.4.1. If an EDR non-volatile memory buffer void of previous-event data is not available, the recorded data shall, subject to the provisions of paragraph 5.3.2., be overwritten by the current event data, on a first-in first-out basis, or according to different strategies decided by the manufacturer and made available to the relevant authorities of Contracting Parties.
  - 5.3.4.2. Furthermore, if an EDR non-volatile memory buffer void of previous-event data is not available, data originating from non-reversible restraint system or Vulnerable road user secondary safety system deployment events referred to in paragraph 5.3.2 shall always overwrite any other data that is not locked per 5.3.2.
- 5.3.5. Power failure

Data recorded in non-volatile memory is retained after loss of power.

- 5.4. Crash test performance and survivability
  - 5.4.1. Each vehicle subject to the requirements of national or regional frontal crash test regulations, shall conform with the specifications in paragraph 5.4.3.
  - 5.4.2. Each vehicle subject to the requirements of national or regional side impact crash test regulations shall conform with the specifications of paragraph 5.4.3.
  - 5.4.3. The data elements required by paragraph 5.1, shall be recorded in the format specified by paragraph 5.2, exist at the completion of the crash test and the complete data recorded element shall read "yes" after the test. Elements that are not operating normally in crash tests (e.g., those related to engine operation, braking, etc.) are not required to meet the accuracy or resolution requirements in these crash tests.

The data shall be retrievable even after an impact of a severity level set by UN Regulations Nos.94, 95 or 137.
- 5.5. It shall not be possible to deactivate the Event Data Recorder

## **6. Modification of vehicle type and extension of approval**

- 6.1. Every modification of the vehicle type as defined in paragraph 2.x of this Regulation shall be notified to the approval authority which approved the vehicle type. The approval authority may then either:
  - 6.1.1. Consider that the modifications made do not have an adverse effect on the conditions of the granting of the approval and grant an extension of approval;
  - 6.1.2. Consider that the modifications made affect the conditions of the granting of the approval and require further tests or additional checks before granting an extension of approval.
- 6.2. Confirmation or refusal of approval, specifying the alterations, shall be communicated by the procedure specified in paragraph 4.3. above to the Contracting Parties to the Agreement applying this Regulation.
- 6.3. The approval authority shall inform the other Contracting Parties of the extension by means of the communication form which appears in Annex 1 to this Regulation. It shall assign a serial number to each extension, to be known as the extension number.

## **7. Conformity of production**

- 7.1. Procedures for the conformity of production shall conform to the general provisions defined in Article 2 and Schedule 1 to the Agreement (E/ECE/TRANS/505/Rev.3) and meet the following requirements:
- 7.2. A vehicle approved pursuant to this Regulation shall be so manufactured as to conform to the type approved by meeting the requirements of paragraph 5. above;
- 7.3. The approval authority which has granted the approval may at any time verify the conformity of control methods applicable to each production unit. The normal frequency of such inspections shall be once every two years.

## **8. Penalties for non-conformity of production**

- 8.1. The approval granted in respect of a vehicle type pursuant to this Regulation may be withdrawn if the requirements laid down in paragraph 7. above are not complied with.
- 8.2. If a Contracting Party withdraws an approval it had previously granted, it shall forthwith so notify the other Contracting Parties applying this Regulation by sending them a communication form conforming to the model in Annex 1 to this Regulation.

## **9. Production definitively discontinued**

If the holder of the approval completely ceases to manufacture a type of vehicle approved in accordance with this Regulation, he shall so inform the approval authority which granted the approval, which in turn shall forthwith inform the other Contracting Parties to the Agreement applying this Regulation by means of a communication form conforming to the model in Annex 1 to this Regulation.

## **10. Names and addresses of the Technical Services responsible for conducting approval tests and of Type Approval Authorities**

The Contracting Parties to the Agreement applying this Regulation shall communicate to the United Nations Secretariat<sup>3</sup> the names and addresses of the technical services responsible for conducting approval tests and of the approval authorities which grant approval and to which forms certifying approval or extension or refusal or withdrawal of approval are to be sent.

---

<sup>3</sup> Through the online platform ("343 Application") provided by UNECE and dedicated to the exchange of such information [https://apps.unece.org/WP29\\_application/](https://apps.unece.org/WP29_application/)

## Annex 1

### Communication

(Maximum format: A4 (210 x 297 mm))



issued by : (Name of administration)  
.....  
.....  
.....

Concerning: <sup>2</sup>  
Approval granted  
Approval extended  
Approval refused  
Approval withdrawn  
Production definitively discontinued

of a vehicle type with regard to its Event Data Recorder (EDR) pursuant to UN Regulation No. 160

Approval No.: .....

Reason(s) for extension (if applicable): .....

1. Trade name or mark of the vehicle: .....
2. Vehicle type: .....
3. Name and address of manufacturer: .....
4. If applicable, name and address of manufacturer's representative: .....
5. Brief description of vehicle: .....
6. Technical service responsible for conducting the approval tests: .....
- 6.1. Date of report issued by that service: .....
- 6.2. Number of report issued by that service: .....
7. Approval granted/refused/extended/withdrawn:<sup>2</sup>
8. Position of approval mark on the vehicle: .....
9. Place:.....
10. Date:.....
11. Signature: .....
12. The list of documents deposited with the approval authority which has granted approval is annexed to this communication.

<sup>1</sup> Distinguishing number of the country which has granted/extended/refused/withdrawn an approval (see approval provisions in this Regulation).

<sup>2</sup> Strike out what does not apply.

## Annex 2

### Information document on the type approval of a vehicle type with regard to its Event Data Recorder (EDR)

A list of contents shall be included.

Any drawings shall be supplied in appropriate scale and in sufficient detail on size A4 paper or on a folder of A4 format.

Photographs, if any, shall show sufficient detail.

#### General

1. Trade name or mark of vehicle: .....
2. Vehicle type: .....
3. Means of identification of type, if marked on the vehicle: .....
4. Location of the marking:.....
5. Location of and method of affixing the approval mark: .....
6. Category of vehicle: .....
7. Name and address of manufacturer:.....
8. Address(es) of assembly plant(s): .....
9. Photograph(s) and/or drawing(s) of a representative vehicle:.....
10. EDR
- 10.1. Make (trade name of manufacturer):.....
- 10.2. Type and general commercial description(s): .....
- 10.3. Drawing(s) or photographs showing the location and method of attachment of the EDR in the vehicle: .....
- 10.4. Description of the triggering parameter: .....
- 10.5. Description of any other relevant parameter (storing capacity, resistance to high deceleration and mechanical stress of a severe impact, etc.): .....
- 10.6. The data elements and data format stored in the EDR:

| <i>Data element</i> | <i>Recording interval/time (relative to time zero)</i> | <i>Data sample rate (samples per second)</i> | <i>Minimum range</i> | <i>Accuracy</i> | <i>Resolution</i> |
|---------------------|--------------------------------------------------------|----------------------------------------------|----------------------|-----------------|-------------------|
|                     |                                                        |                                              |                      |                 |                   |
|                     |                                                        |                                              |                      |                 |                   |
|                     |                                                        |                                              |                      |                 |                   |

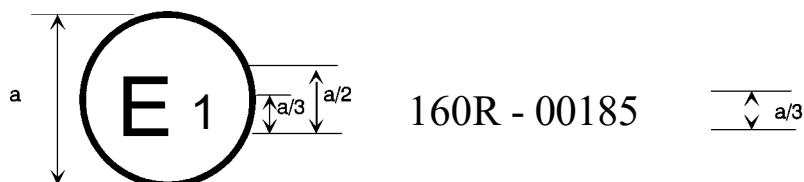
- 10.7. Instructions for retrieving data from the EDR: .....



## Annex 3

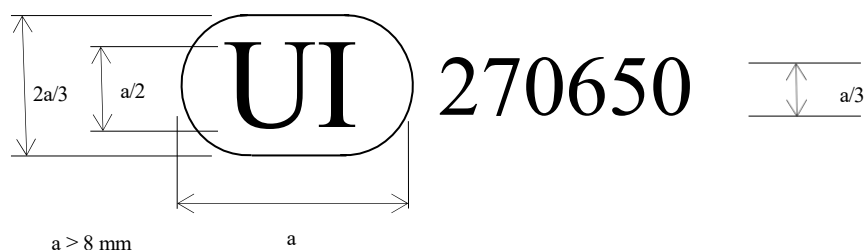
### Arrangements of approval marks

(see paragraphs 4.4. to 4.4.2. of this Regulation)



$a = 8 \text{ mm min}$

The above approval mark affixed to a vehicle shows that the vehicle type with regard to its EDR concerned has been approved in Germany (E 1) pursuant to UN Regulation No. 160. The first two digits of the approval number indicate that the approval was granted in accordance with the requirements of UN Regulation No. 160 in its original form.



The above Unique Identifier shows that the type concerned has been approved and that the relevant information on that type-approval can be accessed on the UN secure internet database by using 270650 as Unique Identifier. Any leading zeroes in the Unique Identifier may be omitted in the approval marking.

## Annex 4

### Data elements and format<sup>1</sup>

Table 1

| <i>Data element</i>                                    | <i>Condition for requirement<sup>2</sup></i>                                                                                                                     | <i>Recording interval/time<sup>3</sup> (relative to time zero)</i>      | <i>Data sample rate (samples per second)</i> | <i>Minimum range</i>                                                | <i>Accuracy<sup>4</sup></i> | <i>Resolution</i> | <i>Event(s) recorded for<sup>5</sup></i> |
|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|----------------------------------------------|---------------------------------------------------------------------|-----------------------------|-------------------|------------------------------------------|
| Delta-V, longitudinal                                  | Mandatory - not required if longitudinal acceleration recorded at $\geq 500$ Hz with sufficient range and resolution to calculate delta-v with required accuracy | 0 to 250 ms or 0 to End of Event Time plus 30 ms, whichever is shorter. | 100                                          | -100 km/h to + 100 km/h.                                            | $\pm 10\%$                  | 1 km/h.           | Planar                                   |
| Maximum delta-V, longitudinal                          | Mandatory - not required if longitudinal acceleration recorded at $\geq 500$ Hz                                                                                  | 0–300 ms or 0 to End of Event Time plus 30 ms, whichever is shorter.    | N/A                                          | -100 km/h to + 100 km/h.                                            | $\pm 10\%$                  | 1 km/h.           | Planar                                   |
| Time, maximum delta-V, longitudinal                    | Mandatory - not required if longitudinal acceleration recorded at $\geq 500$ Hz                                                                                  | 0–300 ms or 0 to End of Event Time plus 30 ms, whichever is shorter.    | N/A                                          | 0–300 ms, or 0- End of Event Time plus 30 ms, whichever is shorter. | $\pm 3$ ms                  | 2.5 ms.           | Planar                                   |
| Speed, vehicle indicated                               | Mandatory                                                                                                                                                        | -5.0 to 0 sec                                                           | 2                                            | 0 km/h to 250 km/h                                                  | $\pm 1$ km/h                | 1 km/h.           | Planar<br>VRU<br>Rollover                |
| Engine throttle, % full (or accelerator pedal, % full) | Mandatory                                                                                                                                                        | -5.0 to 0 sec                                                           | 2                                            | 0 to 100%                                                           | $\pm 5\%$                   | 1%                | Planar<br>Rollover<br>VRU                |

<sup>1</sup> Format requirements specified below are minimum requirements and manufacturers can exceed them.

<sup>2</sup> "Mandatory" is subject to the conditions detailed in Section 1.

<sup>3</sup> Pre-crash data and crash data are asynchronous. The sample time accuracy requirement for pre-crash time is -0.1 to 1.0 sec (e.g., T = -1 would need to occur between -1.1 and 0 seconds.)

<sup>4</sup> Accuracy requirement only applies within the range of the physical sensor. If measurements captured by a sensor exceed the design range of the sensor, the reported element shall indicate when the measurement first exceeded the design range of the sensor.

<sup>5</sup> "Planar" includes triggered events in sections 5.3.1.1, 5.3.1.2, and 5.3.1.3 and "VRU" includes triggered events in section 5.3.1.4.



| <i>Data element</i>                                                                                                                                                          | <i>Condition for requirement<sup>2</sup></i> | <i>Recording interval/time<sup>3</sup> (relative to time zero)</i> | <i>Data sample rate (samples per second)</i> | <i>Minimum range</i>   | <i>Accuracy<sup>4</sup></i> | <i>Resolution</i>      | <i>Event(s) recorded for<sup>5</sup></i> |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|--------------------------------------------------------------------|----------------------------------------------|------------------------|-----------------------------|------------------------|------------------------------------------|
| Service brake, on/off                                                                                                                                                        | Mandatory                                    | -5.0 to 0 sec                                                      | 2                                            | On or Off              | N/A                         | On or Off.             | Planar<br>VRU<br>Rollover                |
| Ignition cycle, crash                                                                                                                                                        | Mandatory                                    | -1.0 sec                                                           | N/A                                          | 0 to 60,000            | ±1 cycle                    | 1 cycle.               | Planar<br>VRU<br>Rollover                |
| Ignition cycle, download                                                                                                                                                     | Mandatory                                    | At time of download <sup>6</sup>                                   | N/A                                          | 0 to 60,000            | ±1 cycle                    | 1 cycle.               | Planar<br>VRU<br>Rollover                |
| Safety belt status, driver                                                                                                                                                   | Mandatory                                    | -1.0 sec                                                           | N/A                                          | Fastened, not fastened | N/A                         | Fastened, not fastened | Planar<br>Rollover                       |
| Air bag warning lamp <sup>7</sup>                                                                                                                                            | Mandatory                                    | -1.0 sec                                                           | N/A                                          | On or Off              | N/A                         | On or Off.             | Planar<br>Rollover                       |
| Frontal air bag deployment, time to deploy, in the case of a single stage air bag, or time to first stage deployment, in the case of a multi-stage air bag, driver.          | Mandatory                                    | Event                                                              | N/A                                          | 0 to 250 ms            | ±2ms                        | 1 ms.                  | Planar                                   |
| Frontal air bag deployment, time to deploy, in the case of a single stage air bag, or time to first stage deployment, in the case of a multi-stage air bag, front passenger. | Mandatory                                    | Event                                                              | N/A                                          | 0 to 250 ms            | ±2 ms                       | 1 ms.                  | Planar                                   |

<sup>6</sup> The ignition cycle at the time of download is not required to be recorded at the time of the crash but shall be reported during the download process.

<sup>7</sup> The air bag warning lamp is the readiness indicator specified in national air bag requirements and may also illuminate to indicate a malfunction in another part of the deployable restraint system.

| <i>Data element</i>                    | <i>Condition for requirement<sup>2</sup></i>                                                                                                              | <i>Recording interval/time<sup>3</sup> (relative to time zero)</i>   | <i>Data sample rate (samples per second)</i> | <i>Minimum range</i>     | <i>Accuracy<sup>4</sup></i> | <i>Resolution</i> | <i>Event(s) recorded for<sup>5</sup></i> |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|----------------------------------------------|--------------------------|-----------------------------|-------------------|------------------------------------------|
| Multi-event crash, number of events    | If Recorded <sup>8</sup>                                                                                                                                  | Event                                                                | N/A                                          | 1 or more                | N/A                         | 1 or more.        | Planar<br>VRU<br>Rollover                |
| Time from event 1 to 2                 | Mandatory                                                                                                                                                 | As needed                                                            | N/A                                          | 0 to 5.0 sec             | ±0.1 sec                    | 0.1 sec.          | Planar<br>Rollover                       |
| Complete file recorded (yes, no)       | Mandatory                                                                                                                                                 | Following other data                                                 | N/A                                          | Yes or No                | N/A                         | Yes or No.        | Planar<br>VRU<br>Rollover                |
| Lateral acceleration (post-crash)      | If Recorded                                                                                                                                               | 0–250 ms or 0 to End of Event Time plus 30 ms, whichever is shorter. | 500                                          | -50 to +50g              | +/- 10%                     | 1 g               | Planar<br>Rollover                       |
| Longitudinal acceleration (post-crash) | If Recorded                                                                                                                                               | 0–250 ms or 0 to End of Event Time plus 30 ms, whichever is shorter. | 500                                          | -50 to +50g              | +/- 10%                     | 1 g               | Planar                                   |
| Normal acceleration (post-crash)       | If recorded                                                                                                                                               | -1.0 to 5.0 sec <sup>9</sup>                                         | 10 Hz                                        | -5 g to +5 g             | ±10%                        | 0.5 g             | Rollover                                 |
| Delta-V, lateral                       | Mandatory - not required if lateral acceleration recorded at ≥500 Hz and with sufficient range and resolution to calculate delta-v with required accuracy | 0–250 ms or 0 to End of Event Time plus 30 ms, whichever is shorter. | 100                                          | -100 km/h to + 100 km/h. | ±10%                        | 1 km/h.           | Planar                                   |

<sup>8</sup> "If recorded" means if the data is recorded in non-volatile memory for the purpose of subsequent downloading.

<sup>9</sup> May be recorded in any time duration; -1.0 to 5.0 sec is suggested



| <i>Data element</i>                  | <i>Condition for requirement<sup>2</sup></i>                                | <i>Recording interval/time<sup>3</sup> (relative to time zero)</i>   | <i>Data sample rate (samples per second)</i> | <i>Minimum range</i>                                                | <i>Accuracy<sup>4</sup></i> | <i>Resolution</i>                           | <i>Event(s) recorded for<sup>5</sup></i> |
|--------------------------------------|-----------------------------------------------------------------------------|----------------------------------------------------------------------|----------------------------------------------|---------------------------------------------------------------------|-----------------------------|---------------------------------------------|------------------------------------------|
| Maximum delta-V, lateral             | Mandatory - not required if lateral acceleration recorded at $\geq 500$ Hz  | 0–300 ms or 0 to End of Event Time plus 30 ms, whichever is shorter. | N/A                                          | -100 km/h to + 100 km/h.                                            | $\pm 10\%$                  | 1 km/h.                                     | Planar                                   |
| Time maximum delta-V, lateral        | Mandatory - not required if lateral acceleration recorded at $\geq 500$ Hz  | 0–300 ms or 0 to End of Event Time plus 30 ms, whichever is shorter. | N/A                                          | 0–300 ms, or 0- End of Event Time plus 30 ms, whichever is shorter. | $\pm 3$ ms                  | 2.5 ms.                                     | Planar                                   |
| Time for maximum delta-V, resultant. | Mandatory - not required if relevant acceleration recorded at $\geq 500$ Hz | 0–300 ms or 0 to End of Event Time plus 30 ms, whichever is shorter. | N/A                                          | 0–300 ms, or 0- End of Event Time plus 30 ms, whichever is shorter. | $\pm 3$ ms                  | 2.5 ms.                                     | Planar                                   |
| Engine rpm                           | Mandatory                                                                   | -5.0 to 0 sec                                                        | 2                                            | 0 to 10,000 rpm                                                     | $\pm 100$ rpm <sup>10</sup> | 100 rpm.                                    | Planar<br>Rollover                       |
| Vehicle roll angle                   | If recorded                                                                 | -1.0 up to 5.0 sec <sup>9</sup>                                      | 10                                           | -1080 deg to + 1080 deg.                                            | $\pm 10\%$                  | 10 deg.                                     | Rollover                                 |
| ABS activity                         | Mandatory                                                                   | -5.0 to 0 sec                                                        | 2                                            | Faulted, Active, Intervening <sup>11</sup>                          | N/A                         | Faulted, Active, Intervening <sup>12</sup>  | Planar<br>VRU<br>Rollover                |
| Stability control                    | Mandatory                                                                   | -5.0 to 0 sec                                                        | 2                                            | Faulted, On, Off, Intervening <sup>12</sup>                         | N/A                         | Faulted, On, Off, Intervening <sup>12</sup> | Planar<br>VRU<br>Rollover                |
| Steering input                       | Mandatory                                                                   | -5.0 to 0 sec                                                        | 2                                            | -250 deg CW to + 250 deg CCW.                                       | $\pm 5\%$                   | $\pm 1\%$ .                                 | Planar<br>Rollover<br>VRU                |
| Safety belt status, front passenger  | Mandatory                                                                   | -1.0 sec                                                             | N/A                                          | Fastened, not fastened                                              | N/A                         | Fastened, not fastened                      | Planar<br>Rollover                       |
| Passenger air bag suppression status | Mandatory                                                                   | -1.0 sec                                                             | N/A                                          | suppressed or not suppressed                                        | N/A                         | suppressed or not suppressed                | Planar<br>Rollover                       |

<sup>10</sup> These elements do not need to meet the accuracy and resolution requirements in specified crash tests.

<sup>11</sup> Manufacturers can include other system states



| <i>Data element</i>                                                            | <i>Condition for requirement<sup>2</sup></i>                                              | <i>Recording interval/time<sup>3</sup> (relative to time zero)</i> | <i>Data sample rate (samples per second)</i> | <i>Minimum range</i> | <i>Accuracy<sup>4</sup></i> | <i>Resolution</i> | <i>Event(s) recorded for<sup>5</sup></i> |
|--------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|--------------------------------------------------------------------|----------------------------------------------|----------------------|-----------------------------|-------------------|------------------------------------------|
| Frontal air bag deployment, time to nth stage, driver <sup>4</sup> .           | Mandatory if fitted with a frontal air bag with a multi-stage inflator.                   | Event                                                              | N/A                                          | 0 to 250 ms          | ±2 ms                       | 1 ms.             | Planar                                   |
| Frontal air bag deployment, time to nth stage, front passenger <sup>12</sup> . | Mandatory if fitted with a front passenger's frontal air bag with a multi-stage inflator. | Event                                                              | N/A                                          | 0 to 250 ms          | ±2 ms                       | 1 ms.             | Planar                                   |
| Side air bag deployment, time to deploy, driver.                               | Mandatory                                                                                 | Event                                                              | N/A                                          | 0 to 250 ms          | ±2 ms                       | 1 ms.             | Planar                                   |
| Side air bag deployment, time to deploy, front passenger.                      | Mandatory                                                                                 | Event                                                              | N/A                                          | 0 to 250 ms          | ±2 ms                       | 1 ms.             | Planar                                   |
| Side curtain/tube air bag deployment, time to deploy, driver side.             | Mandatory                                                                                 | Event                                                              | N/A                                          | 0 to 250 ms          | ±2 ms                       | 1 ms.             | Planar<br>Rollover                       |
| Side curtain/tube air bag deployment, time to deploy, passenger side.          | Mandatory                                                                                 | Event                                                              | N/A                                          | 0 to 250 ms          | ±2 ms                       | 1 ms.             | Planar<br>Rollover                       |
| Pretensioner deployment, time to fire, driver.                                 | Mandatory                                                                                 | Event                                                              | N/A                                          | 0 to 250 ms          | ±2 ms                       | 1 ms.             | Planar<br>Rollover                       |
| Pretensioner deployment, time to fire, front passenger.                        | Mandatory                                                                                 | Event                                                              | N/A                                          | 0 to 250 ms          | ±2 ms                       | 1 ms.             | Planar<br>Rollover                       |

<sup>12</sup> List this element n - 1 times, once for each stage of a multi-stage air bag system.



| <i>Data element</i>                                            | <i>Condition for requirement<sup>2</sup></i>         | <i>Recording interval/time<sup>3</sup> (relative to time zero)</i> | <i>Data sample rate (samples per second)</i> | <i>Minimum range</i>                     | <i>Accuracy<sup>4</sup></i> | <i>Resolution</i> | <i>Event(s) recorded for<sup>5</sup></i> |
|----------------------------------------------------------------|------------------------------------------------------|--------------------------------------------------------------------|----------------------------------------------|------------------------------------------|-----------------------------|-------------------|------------------------------------------|
| Seat track position switch, foremost, status, driver.          | Mandatory if fitted and used for deployment decision | -1.0 sec                                                           | N/A                                          | Yes or No                                | N/A                         | Yes or No.        | Planar<br>Rollover                       |
| Seat track position switch, foremost, status, front passenger. | Mandatory if fitted and used for deployment decision | -1.0 sec                                                           | N/A                                          | Yes or No                                | N/A                         | Yes or No.        | Planar<br>Rollover                       |
| Occupant size classification, driver                           | If recorded                                          | -1.0 sec                                                           | N/A                                          | 5th percentile female or larger.         | N/A                         | Yes or No.        | Planar<br>Rollover                       |
| Occupant size classification, front passenger                  | If recorded                                          | -1.0 sec                                                           | N/A                                          | 6yr old HIII US ATD or Q6 ATD or smaller | N/A                         | Yes or No.        | Planar<br>Rollover                       |



TOP STORIES

## NEWS

## Germany's military-run transport fleet hacked

Germany's state-owned vehicle fleet, which provides chauffeurs for parliamentarians and is run by the Bundeswehr military, has been hacked. Federal cyber experts have begun a probe, reports the Bild am Sonntag newspaper.



Germany's Bundestag administration and federal parliamentarians were told Friday that unknown hackers had infiltrated the FuhrparkService (BWFU) transport fleet, reported the Sunday newspaper BamS (*Bild am Sonntag*).

"Last week, there was an attack on the company's IT network by an as yet unidentified external party," Germany's defense ministry added on Saturday.

Headquartered at Troisdorf, near Bonn, the BWFU is run by Germany's Bundeswehr military and comprises 33,500 vehicles, including trucks, and chauffeur-driven cars assigned to parliamentarians, including those in Berlin.

*Read more:* [Germany: Third of small and mid-sized companies have been hacked](#)

Last year, it provided 142,000 such chauffeur services for the Bundestag parliament and BaMs said it was possible the hackers could have obtained politicians' private addresses and other sensitive details such as times booked and locations.

Parliament's own information technology system was hacked in 2015. Last May, Chancellor Angela Merkel told the Bundestag there was "hard evidence" that Russian intelligence had been behind that infiltration.

The BWFU fleet and driver service, established in 2002 as a state-owned company, operates from 160 locations across Germany and recruits its own certified drivers.

The Bundeswehr military has a three-quarter majority holding in the fleet service; German Rail (Deutsche Bundesbahn) a one quarter stake.

*Read more:* [Germany proposes first-ever use of EU cyber sanctions over Russia hacking](#)

# Cyberattack against Germany's government 'ongoing'

## A 'serious' incident

The German defense ministry on Saturday said the hacking incident notified on Thursday resulted immediately in all electronic links to clients, including the ministry itself, the military and the federal parliament, being capped.

"In addition, the (BWFU) management has called in a company specialized in the analysis and rectification of damage caused by such incidents," it was reported.

*Read more:* [German hacker behind massive political data leak identified](#)

Also involved was another Cyber Emergency Response Team (CERT) of Germany's Federal Office for Information Security (BSI) based in Bonn.

Initial checks of the Bundeswehr military's own dedicated electronic network had shown no damage.

The administration of the federal Bundestag parliament had written to governing and opposition parliamentary groups, reported BamS, telling them: "The attacker and the concrete targets of his attack are not known."

"At present, it is not known when the data center was compromised for the first time, whether data was manipulated or whether data was siphoned off," the letter stated.

One of parliament's five vice-presidents, Thomas Oppermann of the center-left Social Democrats (SPD), described the cyber incident as "serious," saying it must be solved quickly.

*Read more:* [German cyber defense body defends itself over massive breach](#)

ipj/shs (dpa, AFP)

Sign up for DW's newsletters:

NEWS      SPECIAL INTEREST      TV      LEARNING GERMAN

Daily Bulletin

The best of DW news, analysis and opinions, delivered daily at 18:30 UTC.

Berlin Briefing

A weekly roundup of German politics and society.

DW Asia Newsletter

Your weekly rundown of news, background and analysis from DW's Asia Desk.

German News Service

The latest content from German News Service once a week.

Order

|                  |                                                                                                                    |
|------------------|--------------------------------------------------------------------------------------------------------------------|
| Date             | 16.08.2020                                                                                                         |
| Related Subjects | <a href="#">Bundeswehr</a> , <a href="#">Germany</a>                                                               |
| Keywords         | <a href="#">Germany</a> , <a href="#">Bundeswehr</a> , <a href="#">hacking</a> , <a href="#">German parliament</a> |
| Feedback:        | <a href="#">Send us your feedback</a> .                                                                            |
| Print            | <a href="#">Print this page</a>                                                                                    |
| Permalink        | <a href="https://p.dw.com/p/3h1qx">https://p.dw.com/p/3h1qx</a>                                                    |



# **Casos reales de ciberataques a flotas y sistemas de transporte**



## **INFORME "SISTEMAS DE GESTIÓN DE FLOTAS"**



# INTRODUCCIÓN

## ¿QUÉ ES UN SISTEMA DE GESTIÓN DE FLOTAS?

En primer lugar, una flota es el conjunto de vehículos de los que dispone una empresa. Estos pueden ser por ejemplo de tipo industrial destinados para gestiones de logística, de tipo comercial, de transporte o incluso los coches de uso diario de los trabajadores. Todo conjunto de vehículos al servicio de una empresa es una flota de vehículos.

Muchas empresas toman la decisión de contratar un proveedor único que les preste el servicio que mejor se ajuste a sus necesidades. Un sistema de gestión de flotas (SGF) es la administración y logística de un conjunto de vehículos a disposición de una empresa u organización. El objetivo principal de los sistemas de gestión de flotas es, como indica su nombre, la monitorización y control en tiempo real de una flota de vehículos. Lo que permite a la empresa optimizar al máximo los recursos.

Los sistemas de gestión de flotas identifican, entre otras cosas, el estado de los vehículos, su posición, los recorridos realizados, parámetros técnicos del vehículo, estado de la mercancía... y permite a la central de control visualizar dichos parámetros en tiempo real.

### ¿Cómo funciona un sistema de gestión de flotas?

Para poder implementar un SGF es necesario contar tanto con un software como con un hardware específico:

**Hardware:** para poder realizar la monitorización de los distintos parámetros es necesario que se instalen dispositivos hardware especiales en el vehículo que se encarguen de recopilar la información que va a mandarse al centro de control. Normalmente las empresas ofrecen un sistema que integra todas las funcionalidades necesarias para el control de los vehículos. Generalmente, las funciones integradas en dichos dispositivos son:

- Sistema GPS: resulta indispensable para controlar la posición de los vehículos y, de esta manera, optimizar las rutas a seguir por los conductores en función, por ejemplo, del tráfico o para controlar el estado de las entregas.
- Tacógrafo: un tacógrafo registra datos acerca la marcha del vehículo y determinadas actividades del conductor: los kilómetros recorridos, la velocidad, la hora, las pausas o los periodos de descanso.
- Termógrafo: registra la temperatura del vehículo, algo indispensable para compañías de transporte de mercancías como alimentos, los cuales tienen que ir constantemente con unas condiciones controladas de temperatura.
- Parámetros técnicos de la conducción: como las revoluciones del motor, la temperatura del aceite, el consumo de combustible, el sistema de frenado, los sistemas TPMS que monitorizan la presión de los neumáticos, cuando se encienden las luces de emergencia, si se salta la alarma antirrobo, etc.

**Software:** se encuentra instalado en el propio hardware y es el que permite la gestión de diferentes funciones:

- Gestión de los tiempos de conducción: descarga remota del tacógrafo, descarga remota de las tarjetas de los conductores, control de la jornada de trabajo, simulación de los tiempos de conducción, gestión de infracciones, conducción eficiente, etc.
- Gestión de la documentación en ruta: con la recepción, impresión, escaneo, archivo y envío de la documentación, lector de código de barras, integración con la firma electrónica y un sistema de mensajería profesional.
- Navegación profesional para ayuda a la conducción.
- Elementos de configuración y control de acceso y de versiones.
- Comunicaciones con los sistemas de control de la central.

Además, en la mayoría de los casos, las compañías ponen a disposición de sus trabajadores aplicaciones que permiten, por ejemplo, gestionar y planificar los viajes con la oficina de tráfico, el intercambio de mensajes en tiempo real con la central, la planificación de actividades, la gestión de repostajes, las dietas, el control de la lista de tareas, la gestión documental, la navegación profesional o la recogida de firmas. Todas estas funciones, lógicamente, varían dependiendo de las necesidades de la empresa, por lo que no serán iguales para una compañía de transporte de mercancías que para una de alquiler de vehículos.

Toda la información recopilada se envía a la central de control, donde se recoge y se administra. Las comunicaciones se realizan principalmente a través de redes GPRS, 3G o 4G, generalmente gracias al servicio de las operadoras tradicionales de telefonía. Dicha central de control se suele implementar en las oficinas de la empresa contratante. Muchos de estos sistemas de control son de modalidad SaaS (Software as a Service), que básicamente es un modelo de distribución de software en el que tanto el programa como los datos manejados se centralizan y alojan en un servidor externo a la empresa. Es decir, el software que la empresa utiliza no se encuentra en la misma, sino que un proveedor externo se ocupa de su hospedaje en la nube, así como de su mantenimiento y de su soporte. Esto parece complicado de entender, pero es algo muy sencillo y utilizado prácticamente por todo el mundo: cualquier servicio de correo electrónico es básicamente esto, ya que el software está alojado en los servidores de Yahoo o de Google por ejemplo, con todos los correos que tenemos en la bandeja de entrada y nosotros podemos acceder a él desde cualquier dispositivo que tenga conexión a internet.

Una cosa muy importante de los sistemas de gestión de flotas es que, a pesar de contar con unas características generales y comunes para prácticamente todos sus clientes, al estar destinados al sector profesional y este contar con infinidad de posibilidades y necesidades técnicas, han de adaptarse a las características únicas de cada compañía, siendo indispensable la versatilidad de la gestión.

A parte de recopilar datos y de ponerlos a disposición del usuario en una interfaz administrativa, los sistemas de gestión de flotas suelen incluir entre sus servicios la organización de esos datos y de la creación de informes y estadísticas que ayuden a interpretar y utilizar mejor la información obtenida, agilizando la toma de decisiones a la hora de establecer estrategias laborales.

## Vulnerabilidades que pueden sufrir los SGF

Como prácticamente todo lo que funciona electrónicamente, los sistemas de gestión de flotas son vulnerables frente a atacantes maliciosos. Vamos a dividir las vulnerabilidades que pueden sufrir dichos sistemas en tres categorías: las que pueden afectar a los sistemas que se han de instalar en los vehículos, los sistemas de almacenamiento y monitorización del centro de control y las aplicaciones.

### Sistemas instalados en el vehículo

El mayor riesgo en este caso sería la capacidad de manipular los datos que envía el vehículo al centro de control:

- Si se manipulan los datos sobre la temperatura que envía un camión refrigerado podría significar que toda la mercancía que transporta se pierda sin que nadie sea consciente de ello.
- Un dispositivo vulnerable permitiría a un cracker falsificar por ejemplo las rutas, los datos del estado del vehículo, la información del conductor, alarmas, estado de los sistemas de seguridad...

Todo ello podría suponer grandes costes económicos e incluso poner en grave riesgo la vida del conductor del vehículo:

Si se pretende asaltar un camión que dispone de un sistema de gestión de flotas vulnerable y el cracker es capaz de impedir que dicho camión envíe cualquier señal de alarma, o que en el centro de control perciban que el camión se ha salido de la ruta preestablecida, los atacantes podrían completar su propósito sin que nada pudiese impedirlo.

Además, no debemos olvidar la información personal que almacena. Un cracker podría tener acceso a los datos del conductor, del estado del vehículo y de las rutas que debe efectuar éste.

Los casos en los que se puede aprovechar un SGF vulnerable son enormes y ponen en peligro tanto los datos que almacena el sistema como la vida del conductor y, evidentemente, pueden suponer un coste económico muy elevado para la empresa.

Pero esto no es todo, si el sistema instalado en el vehículo tiene la capacidad de realizar acciones sobre el mismo, como abrir las puertas o apagar el motor, y no es completamente seguro, un cracker podría forzar dichas acciones pudiendo provocar un accidente y comprometer las vidas de los que viajasen en él y a su alrededor.

### Centro de control:

Si los servidores que utiliza de soporte el sistema de gestión de flotas son vulnerables, al igual que con los sistemas instalados en el vehículo, las posibilidades son críticas:

Que los servidores de un SGF fuesen vulnerables podrían suponer a un cracker conocer la posición de un vehículo o, incluso, la de toda la flota en tiempo real.

A la vez podría obtener información personal de todos los conductores que trabajan para la empresa, así como sus rutas establecidas y la frecuencia en que son realizadas.

Además, se podrían modificar los datos que almacenan dichos servidores, haciendo inútiles los informes y estadísticas que generados por los SGF para el estudio y mejora de la empresa.

De igual manera que en el caso anterior, si desde el centro de control es posible mandar información a los conductores, modificar sus rutas o, incluso, apagar y encender el motor de

los vehículos, un fallo en el sistema podría permitir al cracker realizar todas estas acciones de forma remota y sin dejar rastro.

### Aplicaciones:

Existen SGF que ofrecen, por ejemplo, aplicaciones a los conductores de los vehículos, con las que los conductores pueden comunicarse con la central, generar actividades, gestionar la estrategia de repostaje, planificar las rutas, gestionar los documentos, etc. Una aplicación vulnerable podría permitir al cracker acceder y modificar todos los servicios ofrecidos por dicha aplicación.

Una cosa muy importante dentro del mundo de la ciberseguridad y que nunca hay que olvidar es que el usuario es el punto más débil de la cadena, por ello las aplicaciones, al estar en contacto directo con las personas que los utilizan, siempre tienen un plus de peligrosidad.

Dependiendo de lo vulnerable que sea el sistema y de lo que se vea afectado, podrán realizarse unos ataques más o menos críticos. Esto se podría traducir en los siguientes ejemplos:

- Si se tratase de un camión que transporta medicamentos y se modifica la lectura del sensor de temperatura se podría echar a perder toda la carga.
- Si es posible abrir y arrancar el vehículo es posible robar decenas de coches de una flota.
- Si se puede controlar la posición de toda una flota y modificar la información que recibe el centro de control, sería factible asaltar la mercancía que transporta, por ejemplo un camión, sin que nadie se dé cuenta.

### ¿Qué características ha de tener un sistema de gestión de flotas?

Es muy difícil determinar qué características han de ser comunes en todos los SGF, ya que cada empresa contará con unas necesidades propias y únicas para su modelo de negocio. Pero a continuación hemos recogido una serie de ellas que se cumplen en la mayoría de casos:

1. **Sencillez.** Cuanta mayor sea la sencillez de la interfaz, mejor. Obviamente la comodidad a la hora de utilizar cualquier sistema no es una cuestión baladí. Un sistema excesivamente complicado o bien termina dejándose de usar o necesita un tiempo demasiado grande para aprender a usarlo, entrando en contradicción con una de las finalidades de los SGF: ahorrar tiempo.
2. **Ubicuidad.** Tener la capacidad de hacer frente a cualquier imprevisto que pueda surgir sin importar el lugar en el que ocurra gracias a las tecnologías móviles es un aspecto muy importante, algo que aporta tranquilidad y mejora la eficiencia en situaciones no planeadas.
3. **Big Data.** Contar con una gran cantidad es muy positivo, siempre que se tengan las herramientas idóneas para manejarlos. Información como el estado del vehículo o la localización es fundamental, pero ampliarla por ejemplo con datos sobre el estilo de conducción, el consumo o el rendimiento en función del clima ayudarán significativamente a mejorar la toma de decisiones.
4. **Informes.** Todos los datos recogidos no sirven de nada si no se plasman en informes que ayuden a entender mejor la situación y sirvan de apoyo a la hora de tomar decisiones lógicas. Estos informes han de poder visualizarse de una manera sencilla, práctica y han de ser adaptables a los requisitos de cada compañía.

5. **Información en tiempo real.** La localización en tiempo real es, con toda seguridad, la característica más importante de los gestores de flotas ya que habilita múltiples ventajas.
6. **Comunicación bidireccional.** Algunos gestores es cierto que cuentan con una comunicación unidireccional, que en la mayoría de los casos es únicamente de envío de datos del vehículo al servidor; pero que exista una comunicación en dos direcciones permite que tanto si se detecta un problema en el centro de control como si lo detecta el conductor durante su servicio, se pueda actuar de la mejor manera.
7. **Integración con sistemas de terceros.** Hoy en día cada vez están más ligados unos departamentos con otros dentro de las empresas. Y cada departamento tiene sus propios sistemas tecnológicos, cuya integración con la solución de gestión de flotas pueden suponer enormes ventajas. Por ejemplo, para la administración de activos, para la facturación, nóminas, etc.
8. **Robustez.** Porque de nada sirve tener un buen sistema tecnológico en la oficina, si los dispositivos instalados en los camiones se deterioran fácilmente o presentan problemas técnicos cada dos por tres.
9. **Navegación específica según el tipo de vehículo.** Hace poco se viralizó una imagen de un tráiler encajado en un estrecho camino sin posibilidad de dar la vuelta. Fue necesario llamar a la grúa y la factura no fue pequeña. Este tipo de situaciones se puede evitar con un navegador que tenga en cuenta la tipología, dimensiones y peso del vehículo, de forma que pueda indicar la ruta más adecuada y evitar situaciones comprometidas.
10. **Información de tráfico.** Los atascos son una de las causas que más estrés generan en los conductores profesionales. Un navegador que ofrezca información real sobre la situación del tráfico y que avise de los retrasos y de posibles rutas alternativas puede suponer la diferencia entre llegar a tiempo a destino o no, con la tranquilidad que esto conlleva.

# SITUACIÓN ACTUAL DE LOS SISTEMAS DE GESTIÓN DE FLOTAS

## Principales actores

Según el estudio “Fleet management in Europe. Growing importance in a world of changing mobility” realizado por la consultora Deloitte, el 50% del mercado europeo total de los gestores de flotas está controlado por cinco actores, y son los siguientes:

- ALD Automotive
- Athlon
- Arval
- Lease Plan
- Alphabet

De acuerdo a los resultados obtenidos de la investigación realizada por la firma británica, el mercado se está consolidando: en los últimos 15 años se lleva produciendo una fuerte consolidación en el mercado europeo de flotas. Esto ha provocado que tras más de 50

adquisiciones, el 50% haya quedado controlado por tan solo cinco grandes compañías. Existen tres razones que expliquen esta tendencia:

- La oferta de servicios transfronterizos: las estrategias de crecimiento y expansión de las empresas son la razón principal de este proceso. Los clientes multinacionales exigen una cobertura a nivel europeo que cubra las necesidades de sus filiales y empleados a través de un servicio uniforme. La adquisición de compañías existentes con sus flotas propias hizo aumentar considerable y rápidamente los tamaños de las carteras, las ofertas de productos y la cobertura geográfica.
- En segundo lugar, las economías de escala: las compañías de gestión de flotas estipularon que el tamaño era un requisito indispensable para poder obtener beneficio de las economías de escala, reduciendo sus costes operativos por contrato. Tener un alto volumen de negocio se traduce en un gran poder adquisitivo, algo que puede ser empleado para obtener beneficios de proveedores como los OEM o las empresas de combustible al poder realizar grandes desembolsos de dinero sin problema.
- Oportunidades de inversión con bajo riesgo: los bancos y los fondos de inversión se dieron cuenta de los altos márgenes de beneficio a bajo riesgo que ofrecía el negocio de las flotas de vehículos, lo que hizo que comenzasen a adquirir empresas de este tipo.

El resultado de eso ha sido la desaparición de los actores de mediano tamaño independientes. El mercado europeo de las compañías de gestión de flotas ha quedado reducido a cinco grandes proveedores y muchas empresas a nivel nacional fragmentadas que rara vez tienen un volumen superior a los 30.000 vehículos.

## Formas de obtener beneficio

Las formas de obtener beneficio de las compañías de gestión de flotas son muy variadas. Como ejemplo, la financiación y el arrendamiento solo significan entre un 30 y un 35% de los beneficios totales y ni siquiera son el generador de ingresos.

Una de las claves a la hora de conseguir maximizar los beneficios es saber pronosticar el valor residual de un vehículo. Esto permite ajustar los pagos mensuales de la mejor manera y poder comercializar de nuevo el vehículo al finalizar el contrato.

Detrás de la financiación en volumen de beneficios para la empresa encontramos el remarketing de productos, que constituye alrededor de un 20% de las ganancias. Esto está directamente relacionado con lo que hemos señalado de saber pronosticar correctamente el valor residual del vehículo, ya al venderlo por encima de ese valor se incrementan los beneficios de manera limpia.

Por otro lado, los contratos que las compañías de gestión de flotas redactan para sus clientes están repletos de cláusulas que se traducen en pequeñas multas o sanciones por incumplimiento del contrato, como puede ser el sobrepasar el kilometraje permitido o algunas relacionadas con desperfectos en el vehículo.

Otra de las fuentes de ingresos importantes en este tipo de negocios son los descuentos obtenidos a la hora de realizar grandes compras que realizan, por ejemplo a la hora de adquirir equipos originales, en donde a menudo suelen obtener descuentos de entre un 15 y un 25%. Si bien es cierto que estos descuentos muchas veces se aplican directamente en los clientes, para

poder ofrecer tarifas más y más competitivas, siempre quedan descuentos restantes que al final, en el balance, se traducen en ingresos positivos.

Para finalizar, vamos a hablar de lo que aporta el mayor porcentaje de beneficio, alrededor de un 40-50% del total: los servicios. Normalmente, las compañías de gestión de flotas subcontratan algunos de sus servicios ofrecidos a terceros especializados. En estos casos, cobran una tarifa de gestión mientras gestionan el contacto con el cliente.

## Servicios ofrecidos

Como hemos visto, las empresas dedicadas a la gestión de flotas obtienen gran parte de sus beneficios de los servicios que ofrecen más allá del propio vehículo.

- Gestión de licencias, títulos y registros: destinadas a gestionar los cada vez más complejos procesos burocráticos.
- Gestión del combustible: es común que al vehículo en cuestión le acompañe una tarjeta de combustible que ofrezca descuentos en determinados distribuidores y que detecten el abuso desmesurado de su uso.
- Mantenimiento: ponen a disposición del cliente una red de tiendas, asesores técnicos y servicios certificados 24/7.
- Talleres de reparación: a la hora de gestionar accidentes y problemas con los vehículos.
- Gestión tareas administrativas y de sanciones: ayuda y reducción de las tareas administrativas siempre que garantice el cumplimiento del contrato.
- Cambio de neumáticos: sobretodo en países del norte de Europa, en donde es necesario alternar los neumáticos en función de la temporada (verano e invierno).
- Vehículo de sustitución: en caso de accidente o de avería se le asegura al cliente un vehículo para poder seguir realizando su vida normal.
- Programas de capacitación y de evaluación de riesgos.
- Servicios telemáticos: destinados a mejorar la eficiencia de la flota, aumentando la productividad del conductor y reduciendo los costes operativos.
- Gestión del uso personal: seguimiento del kilometraje personal en línea y obtención de informes en tiempo real.

Si realizamos un análisis de los servicios ofrecidos por las cinco grandes compañías de gestión de flotas, comprobamos que ofrecen lo siguiente:

### **ALD Automotive:**

Servicios ofrecidos:

- ALD Net: portal web para administrar la flota 24/7. Proporciona alertas personalizadas sobre desviación en el kilometraje, renovaciones, consumo de combustible. Prepara informes automáticos en más de 14 idiomas, que cubren todas las áreas, como nuevos pedidos, nuevas entregas, contratos rescindidos, costes de funcionamiento, etc.
- Mi ALD: diseñado para que la administración sea más fácil, más rápida y eficiente. Así, se puede concentrar el trabajo en las actividades principales. Se puede: ver detalles sobre contratos y vehículos, solicitar asistencia para conductores, configurar y seleccionar un auto, actualizar el kilometraje del vehículo, buscar proveedores de servicios localizados, acceder a documentos útiles, subir documentos para conductores, enviar notificaciones...
- Selector de coche: esta herramienta facilita la selección de un automóvil comercial, configurarlo con opciones y accesorios y comparar hasta tres opciones diferentes:

acceder a la información reciente del vehículo 24/7, buscar vehículos mediante diferentes criterios, solicitar cotización basada en selecciones individuales...

- Cotizador web: herramienta para que los conductores puedan elegir sus automóviles en consecuencia de los parámetros establecidos por la empresa.
- Brinda autonomía e independencia a los conductores y ahorra tiempo a los gerentes.
- Telemática: Permite a los gerentes vigilar atentamente los vehículos de la compañía y ofrece una serie de beneficios: registro del viaje preciso y contado del kilometraje, mejor cumplimiento legislativo y control de costes, incremento de la productividad, disminución de los incidentes reportados debido a una mejor conducción, mayor posibilidad de recuperación en caso de robo de automóviles, notificación proactiva de servicios, reducción de costes operativos a través del mantenimiento oportuno y mejor comportamiento del conductor, datos para una gestión ambiental más eficiente.
- Servicios de valor agregado: contacto con el servicio ALD, tarjeta de combustible para realizar un seguimiento del consumo y seguro de prevención.

#### **ATHLON:**

- Renting con todos los servicios
- Gestión de los conductores desde el principio a fin de contrato
- Acceso de forma fácil al estado de su flota
- Informes mensuales con información de su flota y asesoramiento para alcanzar los objetivos
- Beneficios del servicio de gestión de flotas:
  - o Mayor enfoque en el objetivo de negocio de su empresa
  - o Menor tiempo dedicado a gestiones administrativas y que aportan poco valor
  - o Acceso rápido y completo al estado de su flota
  - o Toma de decisiones estratégicas que permitan alcanzar sus objetivos de movilidad

#### **ARVAL**

- Account Team: un equipo especializado, dedicado y centrado en las necesidades del cliente.
- Herramientas de autogestión: plataforma My Arval, que permite agilidad, cercanía e interacción entre la empresa y los conductores.
- Enfoque consultivo: asesoramiento experto durante toda la vida del contrato de tu vehículo, por un equipo comercial y de consultoría especializado.
- Servicios incluidos:
  - o Servicios de neumáticos
  - o Asistencia en carretera
  - o Mantenimiento y reparaciones en caso de accidente
  - o Atención 24/7
  - o Vehículo de Sustitución

#### **ALPHABET**

- Tareas administrativas y contables
- Gestión de mantenimiento y reparación en centros de servicio en todo el país
- Liquidación de servicios de automóviles en la red de talleres de reparación
- Informes mensuales con un análisis de costes
- Amortizaciones de depreciación que deben realizar las empresas



- Cambio gradual a otras soluciones de financiación
- Reducción de costes en los servicios de reparación y mantenimiento
- Control total sobre el presupuesto
- Servicios:
  - o Seguro
  - o Asistencia
  - o Tarjetas de combustible
  - o Informes
  - o Telemática: Gracias a la transmisión actual de datos desde dispositivos GPS instalados en automóviles, obtiene acceso a datos detallados de todos los vehículos de su flota. Incluyen la ubicación del vehículo, su velocidad, dirección de movimiento o lugar de paradas.
  - o Servicio de neumáticos
  - o Ajuste de reclamaciones en caso de accidente
  - o Coche de sustitución
  - o Alquiler a corto plazo
  - o Logística de vehículos
  - o Movilidad complementaria

#### **LEASE PLAN:**

- Gestor de flota online
- Servicios:
  - o Tarjeta de combustible
  - o Reserva online de taller de preferencia
  - o Servicio de cobertura
  - o Gestión de sanciones Plus
  - o Vehículo de sustitución
  - o Consultoría
  - o Plan renove
  - o Green plan

## **Cambio de mentalidad**

En general, la cuota del segmento del mercado privado está disminuyendo. En 2010, los segmentos del mercado privado y corporativo fueron casi igual de grandes en Europa Occidental: 7,3 millones de las matriculaciones privadas frente a los 7,2 millones de matriculaciones corporativas de automóviles.

Desde entonces ha habido un cambio en la tendencia del mercado hacia un automóvil corporativo inscripciones En 2016 ya había una diferencia significativa: 6,3 millones de privados (42% del total registros) frente a los 8,7 millones de empresas (58% del total de registros).

Este aumento puede explicarse principalmente con el recuperación económica y crecimiento de Europa Occidental. Además, las actuales tarifas disponibles permiten incentivos financieros atractivos (p. ej., leasing) para que las empresas amplíen sus flotas.

Para 2021, Deloitte pronostica una parte de nuevas matriculaciones de automóviles del 37% para particulares y del 63% para el canal corporativo.

Según el estudio de Deloitte, se esperan más de 10 millones de nuevas matriculaciones corporativas de automóviles en Europa Occidental en un año por primera vez. Esto equivale a

un aumento de la tasa de crecimiento (CAGR) del 3.5% entre 2016 y 2020 o casi el doble de la tasa de crecimiento del mercado global de ventas de automóviles en Europa.

Este aumento adicional en los registros corporativos implica un número creciente de flotas y de automóviles de empresa que necesita ser administrado y, por lo tanto, proporcionar una gran oportunidad de negocio para las empresas de gestión de flotas.

Por otro lado está la creciente importancia de los vehículos ecológicos. La Unión Europea llegó a un acuerdo para reducir las emisiones globales de CO2 en un 80% hasta 2050, en comparación con el año base de 1990.

Para lograr este ambicioso objetivo, la Comisión Europea define, además de muchas otras reglas, valores límite vinculantes para las emisiones de CO2 de vehículos nuevos. Actualmente la configuración está en 95 gramos / CO2 por kilómetro para 2020. Dicho límite Deloitte espera que disminuya a 84 gramos / CO2 por kilómetro para 2030 y 56 gramos / CO2 por kilómetro para 2040.

Los vehículos que no cumplan con los límites definidos se verán afectados por las prohibiciones y por impuestos más altos. Como resultado Deloitte espera que el volumen de vehículos de bajas emisiones en flotas corporativas aumente bruscamente dentro de los próximos años.

Por todo esto se plantean cuatro futuros estados posibles para la movilidad en los próximos años, los cuales es posible que coexistan en algún momento:

#### **Estado futuro 1: Cambio en el incremento de la tecnología**

Un mundo donde la propiedad privada permanece ya que los consumidores optan por mantener las formas de privacidad, flexibilidad, seguridad y conveniencia que han tenido hasta ahora, sin plantearse una conducción que no sea realizada por un humano. Al incorporar tecnologías de asistencia al conductor, este estado futuro asume que los vehículos autónomos no van a conseguir desplazar a los vehículos tradicionales.

#### **Estado futuro 2: Un mundo de coches compartidos**

El estado futuro 2 imagina cómo continúan creciendo los viajes compartidos, algo que afecta tanto a empresas como a usuarios individuales. La escala económica y el aumento de la competencia podría impulsar la expansión del vehículo compartido como servicio en nuevos territorios geográficos y segmentos de clientes más especializados. Como la movilidad compartida cubre una mayor proporción de las necesidades de transporte local, podría reducir la necesidad de vehículos personales, particularmente en hogares que tienen varios.

#### **Estado futuro 3: La revolución sin conductor**

El tercer estado futuro ve la adopción generalizada de vehículos autónomos, pero privados, lo que hace indicar que la propiedad sigue siendo algo dominante a la hora de tomar una decisión. Los conductores todavía prefieren tener sus propios vehículos, pero buscan la funcionalidad sin conductor por su seguridad y conveniencia.

#### **Estado futuro 4: Una nueva era de autonomía accesible**

El estado futuro 4 anticipa una convergencia tanto del coche autónomo como del vehículo compartido. Las empresas de gestión de flotas y los operadores de estos servicios ofrecen una variedad de experiencias a pasajeros para satisfacer una amplia variedad necesidades a precios

diferenciados y competente. Inicialmente se expandirá por zonas urbanas, pero se extenderá rápidamente a comunidades suburbanas.

Pasar de la propiedad a compartir supondrá aumentar la relevancia de las compañías de gestión de flotas.

El emergente patrón de movilidad de los adultos jóvenes ha cambiado gracias a una industria en la que proveedores de servicios como Uber, DriveNow y Car2go han experimentado, y todavía están experimentando, un crecimiento significativo y son sin lugar a dudas fenómenos definitorios de nuestra movilidad en un futuro.

Estos proveedores están cambiando la forma en que las personas se mueven. Las generaciones más jóvenes están liderando el camino hacia la movilidad de pago por uso en lugar de poseer un automóvil: casi el 50% de la nueva generación de adultos jóvenes les gusta usar una aplicación de teléfono inteligente para el transporte.

El coche compartido extiende los beneficios de la movilidad para las personas sin que tengan asumir el coste y el esfuerzo de pagar el precio de un automóvil. Europa representa alrededor del 50% del mercado mundial de automóviles compartidos y se espera que crezca más, llegando casi a los 16 millones de usuarios.

## Desde el transporte tradicional de pasajeros hasta los taxis robot: las flotas son el futuro

### **Transporte de pasajeros**

Uber se ha convertido en el mayor proveedor de transporte de pasajeros del mundo, pero no ha conseguido consolidar una huella significativa en suelo europeo. Con Londres o París como excepciones, en muchos países del continente Uber se ha encontrado con obstáculos legislativos. Se ha topado con una serie de competidores locales de transporte que han sabido aprovechar mejor su conocimiento de las dinámicas del mercado para construir negocios exitosos. La empresa myTaxi de Daimler se ha convertido, por ejemplo, en el proveedor de taxis más grande de Europa con más de 6 millones de clientes en 2016. El crecimiento fue de 2 millones con respecto a los datos de 2015. Por otro lado, otros servicios han sabido especializarse en servicios exclusivos de transporte, como limusinas, furgonetas o autobuses.

A esto se le han sumado los primeros intentos de integrar tecnología de conducción autónoma con la perspectiva de proporcionar independiente se han traducido en la aparición de "taxis robóticos".

### **Taxis robot**

Especialmente en el negocio de transporte donde un alto porcentaje de los costes van asociado al conductor, la aparición de vehículos sin conductor podría disminuir drásticamente estos costes.

Un estudio reciente de Deloitte ("DUP: Future of Movilidad ") muestra que alrededor del 50% del coste de los taxis está relacionado con el conductor.

Este desarrollo implica un crecimiento del número de vehículos que pertenezcan a una flota en lugar de los que lo hagan a particulares. El estudio de Deloitte "El Futuro de la movilidad: ¿qué sigue?" predice un Porcentaje del 70% de vehículos de flota de conducción autónoma en un entorno urbano para 2035. En un entorno de ese tipo, urbano y conectado, el atractivo de poseer un automóvil disminuye rápidamente si uno tiene acceso a un grupo de coches cuando lo necesite

Para garantizar un funcionamiento perfecto de estos taxis totalmente autónomos algunas cuestiones técnicas han de ser respondidas. El pago es una parte crucial de eso. Hoy, las compañías de transporte ofrecen pagos sin necesidad de tener efectivo, directamente a través de sus aplicaciones de teléfonos inteligentes, pero la próxima revolución está a la vuelta de la esquina.

La tecnología blockchain podría permitir que los autos envíen y reciban dinero, por ejemplo para pagar el mantenimiento y la reparación en caso de accidente. Blockchain podría suponer que el coche también fuese autónomo financieramente hablando.

### **Las flotas del futuro**

Varias compañías automotrices están reaccionando y aumentando su actividad en el sector de la gestión de flotas, tratando de evitar quedar reducidos a un rol de simples proveedores de hardware. Al final, los ganadores serán las empresas que brinden una experiencia perfecta al cliente con un coste limitado.

La creciente demanda de servicios de arrendamiento y de gestión de flotas ha impulsado significativamente el crecimiento y la rentabilidad de las empresas de este tipo de negocios en los últimos años. Este crecimiento ha provocado que se hayan interesado por este tipo de negocios nuevos actores como compañías automotrices o bancos, que están ingresando en este mercado utilizando sus productos propios. Por otro lado, las compañías y plataformas de tecnología ven esta industria como el punto de entrada para su modelo de negocio centrándose en el cliente.

Hoy en día, las compañías de gestión de flotas mantienen la delantera en este negocio tan complejo, pero la competencia es cada vez mayor. Para mantener esa ventaja, las empresas no deben descansar basándose en sus méritos ni en sus sólidos resultados financieros, sino que deben posicionarse estratégicamente de cara al futuro.

Hay diversos factores que han sido clave en el éxito de los sistemas de gestión de flotas. Una de ellas es la capacidad de crear una huella global que les permita proporcionar ofertas de servicios sin interrupciones más allá de las fronteras.

Por otro lado, soluciones innovadoras de movilidad como compartir vehículos corporativos también pueden suponer la posibilidad de generar ingresos basándose en las flotas. Centrándose en el conductor y no tanto en el automóvil, los servicios serán cada vez más importantes en un futuro cercano.

En base a esto, es lógico pensar que las empresas de gestión de flotas comiencen a ampliar su cartera de clientes y traten de dirigir sus operaciones hacia el canal privado, preparándose para un futuro de la movilidad donde, debido a la tendencia de compartir coches autónomos, las diferencias entre el vehículo privado y las flotas corporativas se volverán más grandes.

# CASOS REALES

## **EXEMPLEADO APAGA REMOTAMENTE 100 AUTOMÓVILES (2010)**

Un empleado descontento con el concesionario donde trabajaba -en Austin, Texas-, deshabilita de forma remota más de 100 automóviles de esa tienda, del tal forma que no se podían arrancar y el claxon comenzaba a sonar. El atacante hackeó Webtech Plus, un sistema de inmovilización remota de vehículos basado en la aplicación web que se utiliza para alertar a los clientes sobre pagos atrasados -y, en situaciones puntuales, bloquear el coche-.

## **DIVERSAS VULNERABILIDADES DESCUBIERTAS EN EL SOFTWARE DE AGILE FLEET (2013)**

Una auditoría demuestra que un atacante no autenticado puede obtener, de manera remota: información confidencial, denegar el servicio y ejecutar código arbitrario debido a diversas vulnerabilidades encontradas tanto en el software de gestión de flotas Agile FleetCommander como en el módulo de control, denominado FleetCommander Kiosk.

## **DATOS DE 850.000 CLIENTES DE UN SERVICIO DE LIMUSINAS, CRACKEADOS (2013)**

Crackers aprovechan vulnerabilidades en el sitio web de CorporateCarOnline -servicio de limusinas- para robar los registros de 850.000 personas, incluyendo nombres, direcciones, números de tarjeta de crédito y fechas de vencimiento de las mismas -información que un delincuente puede utilizar para llevar a cabo compras online-.

## **UN DONGLE OBD OFRECIDO POR UNA COMPAÑÍA DE SEGUROS ESTÁ REPLETO DE FALLOS (2015)**

Un investigador descubre fallos de seguridad en un Dongle OBD, ofrecido por una compañía de seguros usado en más de dos millones de vehículos estadounidenses, que podrían usarse para controlar el coche de forma remota.

## **ATACAN A UBER Y LE ROBAN DATOS DE 50.000 CONDUCTORES (2015)**

La compañía Uber -una VTC de vehículos de transporte con conductor- sufre una vulneración que afecta a los datos de 50.000 de sus empleados en todo Estados Unidos. Según la compañía, la información robada solo contiene nombres y licencias de conducir. Eso sí, la vulnerabilidad no es descubierta hasta cinco meses después de que se produce. Para evitar posibles problemas a los conductores, Uber lleva a cabo el seguimiento durante un año de los datos bancarios de los afectados, para comprobar que ningún intruso accede a sus cuentas.

## **LA APLICACIÓN DE TAXIS OLA TIENE ERRORES DE PROGRAMACIÓN (2015)**

Un investigador descubre que la aplicación de taxis Ola -la startup más grande de la India y una rival directa de Uber en aquel país- cuenta con diversos errores de programación, como que su API -o interfaz de programación de aplicaciones- se comunica con el servidor en texto plano -sin ningún tipo de encriptación-, lo que le permitió recargar la "billetera Ola" -el medio de pago de la app- de forma gratuita para solicitar taxis sin coste alguno.

## **SE VENDEN CUENTAS DE UBER EN LA DARK WEB (2015)**

Se están vendiendo cuentas activas de Uber en la dark web por solo 1€ y no se ha descubierto de donde provienen. El comprador obtiene datos personales de la víctima además de poder solicitar vehículos de forma gratuita.

## **EL SERVICIO DE TAXIS INDIO, OLA, CRACKEADO (2015)**

Un grupo de hackers llamados TeamUnknown publican que han sido capaces de piratear el sitio web de Ola -lo hacen público en la propia página-, servicio de taxis indio que opera en más de

100 ciudades de aquel país y con más de 150.000 vehículos, de tal manera que han obtenido información personal de los clientes como datos de la tarjeta de crédito, nombre de los usuarios, historial de transacciones, etc.

### **UNA INVESTIGACIÓN DEMUESTRA QUE SE PUEDEN HACKEAR LOS COCHES DE LA POLICÍA (2015)**

Una investigación demuestra cómo se puede tomar el control de dos vehículos de la flota de policía de Virginia, Estados Unidos. Concretamente, los modelos afectados son un Chevrolet Impala 2012 y un Ford Taurus 2013. Los hackers han demostrado que es posible controlar el vehículo; por ejemplo, se puede conseguir que el cambio automático se quede bloqueado en la posición 'P' de parking, que el motor se revolucione sin que nadie esté pisando el acelerador o se pare... Para llevar a cabo el experimento, los hackers tuvieron que acceder físicamente al coche, para reprogramar alguna de las características de los vehículos. Posteriormente, la manipulación a distancia se llevó a cabo desde dispositivos móviles.

### **LA EMPRESA YIDAO YONGCHE HA SIDO HACKEADA (2016)**

Crackean cuentas de usuario de la empresa de transporte de automóviles Yidao Yongche y consiguen robar dinero de los saldos de quienes utilizaban sus servicios, sea vía web o mediante la app.

### **APP OFICIAL TESLA (2016)**

Sustraen dos Tesla ModelS y bloquean la señal GPS para que no puedan ser rastreados.

### **MÁS DE 100 VEHÍCULOS PODRÍAN HABER SIDO CRACKEADOS (2016)**

La policía de Houston cree que más de 100 vehículos de Fiat-Chrysler han sido crackeados y robados para ser vendidos en México. Según el grupo automovilístico, los atacantes -Michael Armando Arce y Jesse Irvin Zelaya- podrían haber conseguido credenciales de trabajadores de concesionarios con las que lograron obtener acceso a bases de datos que emparejaban códigos de apertura con vehículos vendidos.

### **CLOUDFLARE, QUE PRESTA SERVICIO A UBER ENTRE OTROS, VULNERABLE (2017)**

El investigador Tavis Ormandy, del 'Proyecto Cero' de Google, descubre una vulnerabilidad en el servicio de infraestructura de Internet Cloudflare. Las solicitudes web a sitios respaldados por Cloudflare recibían respuestas con información confidencial de distintos servicios, entre los que se encuentra los que ofrece Uber. De esta manera, mensajes privados, correos, información de identificación personal, credenciales... entre otro tipo de datos quedaron expuestos.

### **UNOS MOTEROS ROBAN 150 JEEP WRANGLER FALSIFICANDO SUS LLAVES (2017)**

Una pandilla de moteros denominados 'Hooligans Motorcycle Club', con sede en Tijuana, roba 150 vehículos Jeep Wrangler mediante ciberataques. Los ladrones usaron una base de datos para conseguir, a partir de los números VIN de los vehículos, códigos que utilizaban para reprogramar llaves falsas. Una vez hecho, les basta unos pocos minutos para acceder al coche, abrir el capó con el fin de desactivar la alarma y llevarse el vehículo.

### **ROBADA LA INFORMACIÓN DE 57 MILLONES DE CUENTAS DE UBER (2017)**

Unos hackers se infiltraron en los servidores de Uber y robaron la información privada de 50 millones de clientes y siete millones de conductores de esta empresa de VTC. Los datos incluían información de licencia de conducir, nombres, direcciones de correo electrónico y números de

teléfono. La violación se produjo cuando los piratas informáticos descubrieron que los desarrolladores de la compañía habían publicado un código que incluía sus nombres de usuario y contraseñas en una cuenta privada del repositorio de software Github. Uber ha despedido al jefe de seguridad de la compañía y un ayudante por mantener el caso en secreto casi un año y por pagar cerca de 90.000 euros a los atacantes.

#### **UN INFORME MUESTRA QUE LAS COMPAÑÍAS DE ALQUILER NO PROTEGEN LOS DATOS (2017)**

Un informe de Privacy International muestra cómo las compañías de alquiler de automóviles no protegen la información personal de los clientes que conducen sus coches. Los investigadores alquilieron una serie de automóviles conectados a Internet y examinaron la información que se recopiló y retuvo en el sistema de información y entretenimiento de los vehículos analizados - por ejemplo, un Nissan Qashqai-. Cada automóvil alquilado contenía información personal fácilmente accesible sobre conductores anteriores.

#### **ROBAN DATOS DE 28.700 CLIENTES DE PORSCHE EN JAPÓN (2018)**

La filial de Porsche en Japón denuncia que se han producido múltiples ataques contra los servidores de datos de uno de sus contratistas, de tal forma que quedó expuesta toda información de unas 28.700 personas que habían tenido contacto con la compañía. Entre los datos se encuentran nombres, direcciones, correos electrónicos, números de teléfono, salarios, la cantidad y tipo de vehículos que disponen los clientes de la marca.

#### **UN HACKER ROBA LA INFORMACIÓN DE RUTA DE LOS VEHÍCULOS DE TRANSPORTE DE MARIHUANA EN EEUU (2018)**

Un cracker se infiltra en el sistema de la Junta de Licores y Cannabis de Estados Unidos en donde pudo robar datos e información vital para el seguimiento de sustancias ilegales. Hay información valiosa sobre los vehículos de entrega, las rutas, los tiempos de viaje, números VIN de los vehículos, matrículas, etc. La incidencia ha sido descubierta por MJ Freeway, una compañía que proporciona el servicio de datos y el software para el seguimiento de las plantas de droga.

#### **OBTIENEN LOS DATOS DE 14 MILLONES DE USUARIOS DE TAXI CAREEM (2018)**

Los cibercriminales logran piratear las cuentas de los usuarios de la aplicación mediante el acceso no autorizado al sistema que se utilizaba para almacenar datos. Los delincuentes consiguen acceder a los nombres, direcciones de correo electrónico, números de teléfono y datos de viajes de los usuarios de la app. Aunque, en principio, lo logran tener acceso a datos bancarios, de la tarjeta de crédito y de números de cuenta, desde Taxi Careem aconsejan a los usuarios que revisen periódicamente los extractos de sus cuentas bancarias, por si notan algún movimiento extraño.

#### **DETECTADA VULNERABILIDAD EN UN SERVIDOR DE CALAMP (2018)**

Calamp es una empresa proveedora de servicios telemáticos -TSP- para otras aplicaciones. Con la vulnerabilidad encontrada se puede proporcionar a los piratas informáticos lo necesario para rastrear la ubicación del vehículo, robar información del usuario e, incluso, apagar el motor de forma remota.

#### **DESCUBIERTA UNA VULNERABILIDAD EN EL SISTEMA DE RASTREO DE GPS TRACCAR (2018)**

El equipo de seguridad de la empresa AppCheck descubre lo que se conoce como una vulnerabilidad de Ejecución Remota de Código -RCE-. En concreto, la encuentra en el sistema de rastreo de vehículos GPS Traccar -versión <= 4.0-. Esto permite a un atacante comprometer el host del servidor a través de una cuenta de usuario autorregistrada que resulta en la ejecución remota de comandos. De esta manera se puede sintetizar el estado del motor de los vehículos.

#### **UBER ESPIÓ A SU COMPETIDOR GOCATCH EN AUSTRALIA (2019)**

Uber implementó un software espía para rastrear los automóviles y capturar información como el nombre del conductor y los detalles del automóvil, según reconoció un ex-empleado de Uber. El propósito era acercarse a los conductores rivales para atraerles hacia su plataforma y así ahogar a GoGatch dejándoles sin trabajadores.

#### **SUSTRAEN MÁS DE 100 COCHES DE CAR2GO (2019)**

El suceso se lleva a cabo a través de la aplicación, la cual presenta una vulnerabilidad significativa y puede utilizarse como un punto de entrada para acceder a los vehículos o incluso a los servidores de la telemática o del servicio de automóviles. Según esta conocida empresa de coches compartidos perteneciente al Grupo Daimler, el robo se trata de un fraude y no un hackeo. La mayoría de los coches sustraídos pertenecen, precisamente, a la marca Mercedes.

#### **UN HACKER HACKEA DOS APLICACIONES DE RASTREO GPS Y APAGA LOS MOTORES DE ALGUNOS VEHÍCULOS (2019)**

Un hacker, que se hace llamar L&M, accedió a las aplicaciones iTrack y ProTrack y consiguió monitorizar flotas de vehículos por todo el mundo, consiguiendo incluso detener algunos que viajaban a menos de 20 kilómetros por hora. La contraseña que los usuarios recibían de manera predeterminada era 123456, haciendo ingeniería inversa sobre esto accedió a la API de las aplicaciones y pudo entrar en miles de cuentas para extraer datos de ellas .

#### **UNA APLICACIÓN DE RASTREO DE VEHÍCULOS PERMITE QUE UN DELINCUENTE LOS CONTROLE (2019)**

El Instituto de Ingeniería de Software de la Universidad Carnegie Mellon ha descubierto que la aplicación MyCar, un servicio de pago creado para que los usuarios conecten periféricos a su coche y los controlen desde el móvil, así como para permitirles arrancar el vehículo, abrir o cerrar las puertas, conocer su posición... tiene una vulnerabilidad que posibilita que un atacante pueda extraer credenciales del código fuente y comunicarse con el servidor y, de esta manera, comprometer los vehículos -controlando todas las mencionadas funciones-.

#### **SUSTRAEN 28 FURGONETAS DE MERCEDES EN REINO UNIDO (2019)**

La policía de Sufflok, en Reino Unido, ha indicado que 28 Mercedes Sprinter han sido robados mediante crackeos, concretamente mediante la utilización de un sistema de amplificación y repetición de señal de la llave remota. Por ello han avisado a los propietarios de este modelo de furgoneta de que estén atentos y que tomen medidas de seguridad adicionales.

#### **PARALIZAN TODOS LOS COCHES DE POLICÍA DEL ESTADO DE GEORGIA (2019)**

Los ordenadores instalados en los coches patrulla del estado de Georgia -EE.UU.- se paralizan debido a un ciberataque. Dichos dispositivos han sido infectados por un ransomware, un tipo de ataque que secuestra -de forma virtual- el ordenador y lo paraliza hasta que se paga un



rescate económico. Los sistemas equipados en los vehículos son vitales para el desempeño de la labor de la Policía, al permitir que el coche reciba información crucial para los agentes.

#### **CONDUCTORES DE SERVICIOS VTC CRACKEAN LAS APLICACIONES EN SU BENEFICIO (2019)**

Se descubre que hay conductores de plataformas de coches de alquiler con conductor -VTC- que están utilizando aplicaciones modificadas de empresas de transporte como Grab y Gojek para engañar al sistema y así poder conseguir mayores beneficios por el trabajo que llevan a cabo. Las versiones de arranque de estas aplicaciones permiten a los conductores omitir la verificación, falsificar su ubicación, cancelar trabajos sin ser penalizados -pero cobrando por los mismos- y, en algunos casos, ver información privada del cliente.

#### **MERCEDES UTILIZA RASTREADORES PARA RECUPERAR VEHÍCULOS DE USUARIOS QUE SE RETRASAN EN LOS PAGOS (2019)**

Los sensores de ubicación que están instalados en todos los motores nuevos y usados vendidos por los distribuidores de la empresa en el Reino Unido pueden determinar la ubicación exacta del vehículo. La firma admite compartir información del propietario del automóvil y detalles de la ubicación del vehículo con agentes judiciales de terceros y firmas de recuperación que recuperan los automóviles.

#### **DESCUBREN FALLOS EN APLICACIONES DE RASTREO DE VEHÍCULOS (2019)**

Los investigadores conocidos en la red social Twitter como Vangelis tix Stykas, Yekki y Ken Munro, de Pen Test Partners, llevan a cabo la prueba de tres aplicaciones desarrolladas para la localización de vehículos: Tracker, TrackStar y SmarTrackd. Tras examinarlas descubren fallos en las API -Interfaz de Programación de Aplicaciones, que se utiliza para la comunicación entre servicios y productos- que permitirían a un hacker hacerse cargo de la cuenta, rastrear los automóviles en tiempo real, suprimir alertas de robo y extraer datos personales.

#### **UNA SERIE DE TROYANOS PUEDEN AFECTAR A LAS APLICACIONES DE TAXI Y COCHE COMPARTIDO (2019)**

Los investigadores de la compañía internacional Group-IB -especializados en la prevención de ataques cibernéticos- descubrieron una nueva campaña de troyanos del tipo Flexnet para Android llamada FANTA, que afecta a clientes de la Federación de Rusia y la CEI -Comunidad de Estados Independientes-. Los desarrolladores de FANTA pueden piratear los dispositivos de los usuarios de unos 30 servicios de Internet diferentes, como los servicios de taxi y coche compartido. Sin embargo, parece que los más afectados son los usuarios que suben anuncios de compra y venta de productos al sitio web 'Avito'.

#### **LOS DATOS DE 26.000 PROPIETARIOS DE HONDA QUEDAN EXPUESTOS (2019)**

Una vulnerabilidad en la nube que utiliza la compañía japonesa propicia que la base de datos Elasticsearch de American Honda Motor quede expuesta durante más de una semana, incluyendo datos personales de los clientes como direcciones de correo electrónico y físicas, teléfonos, marcas, modelos y VIN de vehículos o, incluso, los ID de los acuerdos comerciales. Este fallo es descubierto por Bob Diachenko el 11 de diciembre, siendo notificado a Honda el día 12, que procede al cierre del servidor el 13. Diachenko estima que hay un total de 976 millones de registros, con cerca de 26.000 datos relacionados directamente con el consumidor.

#### **DESCUBREN QUE LA APLICACIÓN GURUKUL DE ALQUILER DE COCHES ES VULNERABLE (2020)**

Concretamente, se descubre que la app sufre una vulnerabilidad 'de ejecución remota de archivos', de tal manera que es vulnerable a la carga de archivos maliciosos. Eso significa que un administrador puede cambiar la imagen de un producto, ya que en ese caso el código PHP no valida ni quién hace la subida ni qué tipo de archivo se está subiendo, lo que hace que un ataque tenga la capacidad de ejecutar comandos arbitrarios en el servidor.

#### **DESCUBREN QUE LA BASE DE DATOS DE LA EMPRESA BUCHBINDER NO TIENE SEGURIDAD EN INTERNET (2020)**

La base de datos de la empresa alemana Buchbinder -dedicada al alquiler de vehículos- cuenta con cerca de diez terabytes de datos almacenados y contiene información de más de 3,1 millones de clientes de la compañía en Alemania, Australia, Italia, Eslovaquia y Hungría. Pues bien, la violación de dicha base ha expuesto la información personal de todos esos clientes, como su dirección, números de teléfono y números de licencia. La fuga es descubierta durante la realización de un análisis rutinario llevado a cabo por Matthias Nehls, director ejecutivo de la Sociedad Alemana para la Seguridad Cibernética -Deutsche Gesellschaft für Cybersicherheit-.

#### **TRACKER, COMPAÑÍA DE RECUPERACIÓN DE COCHES, HACKEADA (2020)**

La compañía de recuperación y monitorización de vehículos, Tracker, ha comunicado que ha sido víctima de un delito cibernético en forma de ataque de ransomware. Rápidamente apagaron sus sistemas para evitar la propagación del virus, e iniciaron la investigación para esclarecer los hechos. Además de reconocer la vulneración, han informado de que no se han visto desprotegidos los datos personales de ningún cliente. Todo indica que el ataque ha sido obra de un grupo organizado de delincuentes.

#### **LOS DATOS DE BUBBLE DAN EXPUESTOS (2020)**

Todos los datos del servicio de ride sharing de Israel Bubble Dan han estado expuestos siempre, sin ningún tipo de seguridad. Después de publicar la vulnerabilidad, la compañía afirmó que ya estaba solucionado.

#### **LOS CRACKERS PUEDEN CLONAR MILLONES DE LLAVES DE TOYOTA, HYUNDAI Y KIA (2020)**

Investigadores de KU Leuven en Bélgica y de la Universidad de Birmingham en Reino Unido alertaron de que habían encontrado nuevas vulnerabilidades en los sistemas de encriptación de los inmovilizadores del vehículo., dejando la puerta abierta para que un cracker robe el coche usando un dispositivo Proxmark, que se hace pasar por la llave real del automóvil.

#### **TOTAL QUALITY LOGISTICS, CRACKEADO (2020)**

Total Quality Logistics (TQL) fue atacado cibernéticamente el domingo que comprometiendo su portal de operadores, abriendo potencialmente el acceso a las "cuentas de operadores, incluidos, en muchos casos, números de identificación fiscal y números de cuentas bancarias", según el sitio web de la compañía.

#### **MÚLTIPLES VULNERABILIDADES EN EL PROJECT WORLDS OFFICIAL CAR RENTAL SYSTEM (2020)**

El Sistema 1 de Project Worlds Official Car Rental es vulnerable a múltiples problemas de inyección SQL, como lo demuestran el correo electrónico y los parámetros (account.php), uname y pass parámetros (login.php), y el parámetro id (book\_car.php) Esto permite a un

usuario malicioso volcar la base de datos MySQL y omitir la solicitud de autenticación de inicio de sesión.

## VULNERABILIDADES QUE PUEDEN SUFRIR LOS SISTEMAS DE GESTIÓN DE FLOTAS

Las vulnerabilidades las voy a dividir en tres partes: las que pueden afectar a los sistemas necesarios para el SGF que instala el vehículo, los sistemas de almacenamiento y monitorización del centro de control y las aplicaciones.

### Sistemas instalados en el vehículo:

El mayor riesgo en este caso sería la capacidad de manipular los datos que envía el vehículo al centro de control:

- Manipular la temperatura que envía al centro de control un camión refrigerado podría significar que toda la mercancía que se transporta se pierda sin que nadie sea consciente de ello.
- Y esto puede extrapolarse a cualquier otra lectura, un dispositivo vulnerable permitiría a un cracker falsificar por ejemplo las rutas, los datos del estado del vehículo, la información del conductor, alarmas, estado de los sistemas de seguridad...

Todo ello podría ser catastrófico en función del objetivo del cracker:

Si se pretende asaltar un camión que dispone de un sistema de gestión de flotas vulnerable y el cracker es capaz de impedir que el camión envíe cualquier señal de alarma, o que el centro de control no perciba que dicho camión ha salido de la ruta preestablecida se le facilita muchísimo el llevar a cabo el asalto.

Además, no debemos olvidar la información personal que almacena, el cracker podría tener acceso a datos del conductor, del estado del vehículo y de las rutas que debe efectuar éste.

Los casos en los que se puede aprovechar un SGF vulnerable son enormes y ponen en peligro tanto los datos que almacena el sistema como la vida del conductor, y evidentemente, pueden suponer un coste económico muy elevado para la empresa.

Pero esto no es todo, si el sistema instalado en el vehículo tiene la capacidad de realizar acciones sobre el mismo, como abrir las puertas o apagar el motor, y es vulnerable, un cracker podría forzar dichas acciones sin que el conductor pueda hacer nada.

### Centro de control:

Si los servidores que utiliza de soporte el sistema de gestión de flotas son vulnerables, al igual que con los sistemas instalados en el vehículo, las posibilidades son críticas:

- Un SGF vulnerable en el lado de los servidores podría permitir a un cracker no solo conocer la posición de un vehículo sino de toda una flota en tiempo real.
- Al mismo tiempo podría obtener información personal de todos los conductores que trabajan para la empresa, así como sus rutas establecidas.
- Además, se podrían modificar los datos que almacenan dichos servidores lo que haría inútiles los informes y estadísticas que generan los SGF para el estudio y mejora de la empresa.
- De la misma forma que antes, si desde el centro de control es posible mandar información a los conductores, modificar sus rutas, o incluso apagar o encender el motor de los vehículos, un sistema vulnerable podría permitir al cracker realizar todas estas acciones.

Lo que debe dejarse claro aquí es que todo esto depende de lo vulnerable que sea el SGF. Como ya has puesto en otros informes, la ciberseguridad tiene en cuenta la disponibilidad, integridad y confidencialidad, normalmente no se rompen las tres de forma total, eso significaría que el sistema no sirve literalmente para nada...

Por lo tanto, podría ser que se afectara la disponibilidad y que un cracker consiguiera denegar el servicio en el centro de control, lo que podría impedir que los trabajadores realizaran ciertas acciones. O que afectará la confidencialidad y que el cracker pudiera obtener información confidencial (dependiendo de lo vulnerable que sea el atacante podría o no seleccionar a qué información accede), o podría afectar la integridad y que el cracker pudiera realizar modificaciones de esa información (nuevamente, dependiendo de lo vulnerable que sea podrá seleccionar o no que información modificar o introducir).

## Aplicaciones

Existen SGF que ofrecen, por ejemplo, aplicaciones a los conductores de los vehículos. En el caso del SGF explicado en el anterior documento los conductores pueden comunicarse con la central, generar actividades, gestión de repostajes, planificación de viajes, gestión documental...

En este caso es, nuevamente, lo mismo que los anteriores. Una aplicación vulnerable podría permitir al cracker acceder a los documentos almacenados, modificar sus viajes planificados o simplemente acceder a ellos, observar las comunicaciones entre el conductor y la central o incluso modificarlas, modificar la información para la gestión del reportaje...

Básicamente, como he dicho, dependiendo de cuan vulnerable sea el sistema y de a qué afecta esa vulnerabilidad (confidencialidad, disponibilidad e integridad) podrán realizarse unos ataques más o menos críticos. Lo que hay que pensar en posibilidades llamativas:

- Si el camión transporta medicamentos y se modifica la lectura del sensor de temperatura se pueden echar a perder todos.
- Si es posible abrir y arrancar el vehículo es posible robar decenas de coches de una flota.
- Si es posible controlar la posición de toda una flota de vehículos y modificar la información que recibe el centro de control sería posible asaltar la mercancía que transporta, por ejemplo, un camión sin que nadie se dé cuenta.

Este tipo de casos son los que llaman la atención, aunque es posible que un SGF sea vulnerable y lo único que puedas hacer sea acceder a cierta información irrelevante que recoge el dispositivo del vehículo o que recopilan en el centro de control. Todo depende, como digo, de cuan vulnerable sea.

Pero puestos a realizar suposiciones para el informe lo más llamativo es ponerse en el peor de los casos, porque puede pasar y ha pasado.



# **Método para la gestión eficiente del combustible en flotas de vehículos con rutas fijas. Aplicación a una empresa de construcción**



UNIVERSIDAD  
DE SEVILLA

1505

**Método para la gestión eficiente del combustible  
en flotas de vehículos con rutas fijas. Aplicación a  
una empresa de construcción**



## **CAPÍTULO 2. GESTIÓN EFICIENTE DE FLOTAS.**

### **2.1 Introducción a la Gestión de Flotas.**

#### **2.1.1 Introducción**

Se denomina “flota de transporte” a un conjunto de vehículos destinados a transportar mercancías o personas y que dependen económicamente de la misma empresa. El transporte profesional por carretera, tanto de pasajeros como de mercancías, es esencial para garantizar un adecuado desarrollo social y económico en nuestro país, así como para el logro de una mayor cohesión del territorio.

En términos energéticos, el consumo asociado a este sector tiene una notable incidencia sobre el consumo de energía nacional, representando en torno al 15% del consumo de energía final en España. Además, la práctica totalidad de la energía primaria consumida en el transporte por carretera proviene del petróleo, lo que agrava el problema generado por la excesiva dependencia de los combustibles fósiles y por el aumento de las emisiones de CO<sub>2</sub>, que da lugar a los fenómenos del calentamiento global del planeta y del cambio climático.

En las flotas de transporte, el combustible tiene especial relevancia en su estructura de costes, y más aún con los actuales precios a los que se cotiza el crudo en el mercado. Por tanto, para el adecuado desarrollo de su actividad económica, se hace necesaria la realización de una gestión eficiente del combustible en las mismas.

Una gestión eficiente de flotas, es aquella que para los mismos objetivos es capaz de utilizar la menor cantidad de recursos posibles. Como hay muchos tipos de empresas de transportes, habrá diferentes formas de gestionar las flotas, pero todas ellas tienen ciertas características comunes que se analizarán en este proyecto.

La satisfacción del cliente es una condición fundamental y necesaria, aunque no suficiente para el éxito empresarial. Esta satisfacción va ligada directamente a la valoración que el cliente hace del servicio, basada en su propia percepción. La cuantificación de este aspecto da lugar a lo que hoy en día se entiende por calidad, y es en realidad la calidad percibida por el cliente.

La consecución de la calidad implica que el proveedor trabaje con efectividad. Esta se consigue actuando sobre dos aspectos de la actividad: eficacia y eficiencia.

Eficacia es hacer que lo planificado y lo realizado se aproximen al máximo, es decir, la sintonía entre lo que se planificó hacer para conseguir que los clientes perciban la calidad adecuada en los productos que reciben y en sus servicios acompañantes, y lo que realmente se ha hecho. Un trabajo realizado con eficacia contribuirá a una mejor valoración percibida por los clientes de producto y de beneficio.

Pero existe un segundo aspecto de efectividad que es especialmente bien percibido por el cliente de beneficio: la eficiencia. El beneficio será mayor si los recursos

(operativos y/o materiales) necesarios para conseguir productos y venderlos a los clientes de producto se utilizan más efectivamente, es decir, si se pueden satisfacer las expectativas del cliente de producto con una mínima utilización o aplicación de recursos. Podríamos definir la eficiencia como la efectividad en la aplicación de los recursos necesarios para satisfacer las necesidades de los clientes, es decir, para trabajar con calidad.

Tanto la eficacia como la eficiencia son expresión de la efectividad para trabajar con calidad, por lo tanto trabajar de una manera optima, es conseguir la calidad esperada por los clientes con la máxima eficacia y con la máxima eficiencia.

Por lo general, dependiendo sobre todo del tamaño las empresas de transporte disponen de un departamento de tráfico, que es el encargado de la gestión y organización de las personas y medios necesarios para llevar a cabo la actividad del transporte, comprendiendo entre sus tareas la elección de vehículos, la selección de rutas y gestión de cargas, así como la gestión del consumo de carburante.

En este capítulo se analizará cómo gestionar de forma eficiente diversos aspectos de una empresa de transportes relacionados con el ahorro energético y medioambiental. Se verá la relación existente entre transporte, energía y medioambiente, así como la estructura de costes de una empresa de transporte genérica. También se tratarán aspectos como el mantenimiento, las operaciones o la renovación de la flota. Este capítulo se completa con un análisis de los componentes hardware y software que pueden ayudar a la gestión eficiente de una flota.

### 2.1.2 Definiciones

Se pueden distinguir tres tipos de flotas de transporte según su tamaño:

- *Flotas pequeñas*: normalmente de carácter familiar con un propietario autónomo y algunos conductores familiares o asalariados. Suelen tener hasta 5 ó 6 vehículos y la mayor parte de su trabajo lo hacen para un cliente o una gran empresa. El departamento de tráfico es poco importante y suele ser el propietario de la empresa el responsable de su actividad. El consumo de carburante es muy variable y difícil de cuantificar.
- *Flotas medianas*: con un número de 6 a 30 vehículos. Suele tratarse de pequeñas empresas familiares que han crecido aprovechando una buena gestión y especializándose en nichos de mercado o mercados emergentes. Estas empresas suelen tener ya una amplia cartera de clientes en los ámbitos nacional e internacional. Cuentan con un departamento de tráfico de relieve, gestionado por una persona de confianza de la dirección. A medida que aumenta el número de vehículos, la estructura de la empresa puede crecer hasta tener talleres de reparación, almacenes y depósitos de carburante propios.
- *Flotas grandes*: son empresas que cuentan con un elevado número de vehículos. Los vehículos pueden ser propios o subcontratados a autónomos. Pueden llegar a tener delegaciones en diferentes lugares del país y actúan en muchas ocasiones como

operadores logísticos y de distribución de grandes marcas. Suelen tener vehículos de diferentes tipos para diferentes servicios de transporte.

Es habitual que las flotas de vehículos industriales, tanto de autobuses como de mercancías, se especialicen en un servicio de transporte. Ello les permite competir en su nicho de mercado con mayor eficiencia, como por ejemplo en servicios discrecionales o servicios regulares de larga o corta distancia en el caso de autobuses y servicios de transporte de mercancías peligrosas, frigoríficos, cajas basculantes, cisternas o pescado en el caso de camiones. Sin embargo, otros criterios empresariales pueden recomendar la diversificación o la disposición de vehículos específicos para requerimientos especiales.

Dependiendo del tipo de servicio que presten, diferenciamos entre transporte de mercancías y transporte de personas.

Los vehículos de una flota de transporte de mercancías se suelen clasificar según la forma de organizar las cargas en los siguientes tipos:

- Carga general, paletizada o no paletizada, cargas grandes y pesadas, cargas frigoríficas, etc.
- Cargas especiales, como góndolas y plataformas para vehículos de gran tonelaje.
- Cargas a granel con cajas abiertas, bañeras basculantes, hormigoneras, tolvas, silos o cisternas.

Los vehículos de las flotas de transporte de pasajeros, se pueden clasificar según su ámbito de utilización en:

- Urbanos: realizan la mayor parte del recorrido por ciudad.
- Extraurbanos: Pueden ser de:
  - Larga distancia: se caracterizan por recorridos interurbanos.
  - Corta distancia: se caracterizan por recorridos mixtos

### 2.1.3 El jefe de tráfico:

El departamento de tráfico de una empresa tipo estaría formado por:

- El jefe de tráfico.
- Los auxiliares de tráfico.
- Los conductores.

El máximo responsable del departamento es el jefe de tráfico. Sus tareas son bastante diversas y algunas podían ser:

- Responsable de la contratación directa de los servicios de transporte
- Comunicación directa con los clientes: reclamaciones, quejas,...
- Realización de ofertas de transporte
- Responsable de la distribución o asignación de los servicios contratados
- Encargado de la documentación del transporte: partes de accidentes, reclamaciones de daños sobre la mercancía,...
- Control del estado de la flota: ITV, revisiones periódicas, mantenimiento, renovación de la flota,...
- Seguimiento del servicio prestado: cumplimiento de horarios de carga y descarga, documentación, permisos,...
- Supervisar el trabajo de los subordinados: planificación diaria, vacaciones, bajas,...
- Control de gastos, dietas, consumos,...

## **2.2 Transporte, Energía y Medio Ambiente.**

### **2.2.1 Introducción**

Toda actividad desarrollada por el hombre necesita de un gasto de energía. La energía puede provenir del propio ser humano (energía física) o de una máquina que intercambia trabajo con el Medio Ambiente. En este epígrafe nos vamos a centrar en el segundo grupo, ya que además de lo que acabamos de mencionar, también tiene un factor negativo como es la emisión de contaminantes.

El incremento de la actividad en países en vía de desarrollo ha elevado el número de emisiones al medioambiente, principalmente las de CO<sub>2</sub>, responsable del llamado efecto invernadero. Para disminuir estos contaminantes se han dado pasos para llegar a acuerdos globales, aunque de momento no ha habido consenso, ya que países como EE.UU. parecen no ver el alcance real del problema.

Hasta hace relativamente poco tiempo, la sociedad vivía de espaldas a esta problemática. Si había que acometer algún proyecto o prever la demanda de energía, se hacía sin tener en cuenta las posibles emisiones contaminantes. Además de eso, no se consideraban las energías renovables como una alternativa y no se ponía empeño en su desarrollo. Dichas energías, además de ser más limpias, también son necesarias, ya que las reservas de combustible fósil de la Tierra no durarán eternamente. Aunque todavía

queda mucho camino por recorrer, parece que al menos en el campo de las energías renovables se están consiguiendo alcanzar bastantes objetivos.

Otro problema existente en España es la gran dependencia energética de otros países. Hoy en día se trata de buscar la autosuficiencia energética.

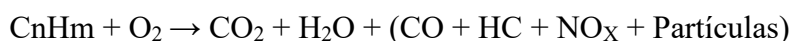
Volviendo al tema de las emisiones contaminantes hay que resaltar que en España el sector transporte emite alrededor de un 30-40% de las emisiones totales y dichas emisiones no se encuentran reflejadas por ejemplo en el protocolo de Kyoto que recoge sólo las emisiones provenientes de las empresas propiamente dichas, por eso resulta de mucho interés su disminución en un sector que hasta hace poco no estaba regulado. Ahora hay algunas leyes, como el impuesto de matriculación, que grava a los vehículos más contaminantes, que pretenden su disminución.

### 2.2.2 Cambio climático y contaminación local

Cuando hablamos de emisiones generadas por el transporte debemos diferenciar entre aquellas que contribuyen al cambio climático y aquellas que afectan de forma directa a la salud humana, o sea las que afectan a la calidad del aire.

Hay muchas razones para intentar ahorrar combustible, una de ellas es para **disminuir las emisiones de contaminantes** a la atmósfera.

La reacción de combustión de los hidrocarburos que se produce es del tipo:



Como se observa, en el proceso de combustión de un hidrocarburo siempre se producirá dióxido de carbono ( $\text{CO}_2$ ) y vapor de agua ( $\text{H}_2\text{O}$ ) y en las mismas cantidades estequiométricas (la combustión emite 2'6/2'35 Kg de  $\text{CO}_2$  por cada litro de gasóleo y gasolina respectivamente). Pero además, se emiten otros productos contaminantes debidos principalmente a una combustión incompleta.

Los productos de la combustión tienen dos tipos de efectos:

- 1) **Efecto local** (afecta a la calidad del aire):  $\text{CO}$ ,  $\text{HC}$ ,  $\text{NO}_x$  y Partículas en suspensión

El Monóxido de Carbono y los Hidrocarburos volátiles se producen por una combustión incompleta, mientras que los óxidos de nitrógeno se generan por un exceso de aire a alta temperatura.

- 2) **Efecto global** (cambio climático):  $\text{CO}_2$

El  $\text{CO}_2$  es esencialmente inofensivo en un entorno local, pero es acumulativamente perjudicial con un aumento de las concentraciones globales.

Las emisiones de CO<sub>2</sub> han aumentado debido a varios factores:

- a) Mejora de las características de seguridad de los vehículos.
- b) La adición de características de comodidad.
- c) La elección de modelos más grandes y más potentes.
- d) El aumento del número de vehículos en nuestras calles.

La evolución de las emisiones de contaminantes de efecto local ha ido disminuyendo en las dos últimas décadas a pesar del aumento de la movilidad. Esta disminución se debe fundamentalmente a las exigencias de emisiones máximas a los fabricantes de vehículos, de acuerdo a las directivas europeas de emisiones.

Sin embargo, las emisiones de CO<sub>2</sub> en España de 1990 a 2006 han crecido un 52,3% sujeto al incremento de movilidad y a la dependencia casi exclusiva del petróleo como fuente de energía. Son varias las medidas que se están llevando a cabo en los últimos años: incentivos al uso de combustibles y vehículos alternativos, impuestos sobre las emisiones de CO<sub>2</sub>, etiquetado energético, etc.

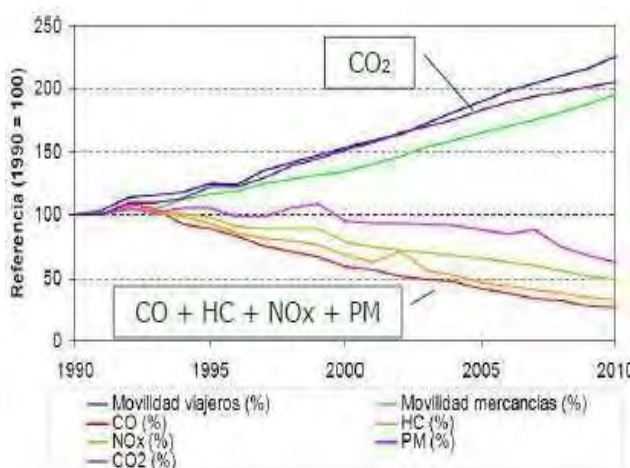


Ilustración 2.2.2

### 2.2.3 El problema medioambiental en España

De toda la energía que se consume en España, en torno al 30% es consumido por el sector transporte. Además, casi el 100% de la energía primaria consumida por dicho sector proviene de combustibles fósiles. Los grandes problemas asociados a la combustión de estos combustibles son dos:

- 1) La gran dependencia que tiene nuestro país de los yacimientos que se encuentran en el extranjero. El problema del autoabastecimiento es mayor aún en Andalucía.
- 2) La contaminación que provocan.

El desarrollo que ha experimentado nuestro país en los últimos años ha ocasionado, por ejemplo, que el número de vehículos de una familia media haya crecido. También que el transporte de mercancías haya aumentado. Todo eso se traduce en un aumento de las emisiones.

Algunas cifras que confirman estas afirmaciones son:

\*Autoabastecimiento: Energía producida/ Energía consumida

En 2007: España: 20,9%, Andalucía: 6,5%

\*Energía consumida en Andalucía en 2007:

Transporte: 37,1%, Industria: 35%, Resid+Prim+Serv: 28:0%

\*Fuentes de energía del sector transporte (Andalucía 2007)

Petróleo: 98,7 %, Biomasa: 0,8 %, Electricidad: 0,6 %

## 2.2.4 Medidas para la disminución de la contaminación

Hay diferentes medidas para intentar disminuir la contaminación. Algunas son:

- Real Decreto 837/2002: es obligatorio informar a los clientes del consumo de combustible del vehículo y emisiones de CO<sub>2</sub> de cada vehículo en venta.

Los vehículos tienen que llevar unas etiquetas obligatorias con la marca, el modelo, el tipo de carburante, emisiones de CO<sub>2</sub> (g/km) y consumo (L/100km) en ciudad, carretera y media. Otras etiquetas son de carácter voluntario y muestran por ejemplo la categoría en la que se engloba el vehículo (según su superficie) o una clasificación de cuánto consume con respecto a los de su categoría.

- Ley 34/2007: el impuesto de matriculación de vehículos se basará en las emisiones de CO<sub>2</sub> por km recorrido.

| Hasta 31 Diciembre 2007<br>Ley 38/1992 |                       |          | Desde 1 Enero 2008<br>Ley 34/2007  |                       |          |
|----------------------------------------|-----------------------|----------|------------------------------------|-----------------------|----------|
| Tipo                                   | Península/<br>Balears | Canarias | Tipo                               | Península/<br>Balears | Canarias |
| <1600 cc (gasolina)                    | 7%                    | 6%       | <120 g CO <sub>2</sub> /km         | 0%                    | 0%       |
| <2000 cc (diésel)                      | 12%                   | 11%      | >=120 y <160 g CO <sub>2</sub> /km | 4,75%                 | 3,75%    |
|                                        |                       |          | >=160 y <200 g CO <sub>2</sub> /km | 9,75%                 | 8,75%    |
|                                        |                       |          | >=200 g CO <sub>2</sub> /km        | 14,75%                | 13,75%   |

Ilustración 2.2.4



La aplicación de esta Ley ha tenido como consecuencia que los vehículos “greencar” (<120gr/km) incrementaron en 2008 su cuota de mercado hasta un 19%, un 8% más que en 2007. Además, los vehículos más contaminantes (>200gr/km) vieron caer sus ventas un 54,9%, y los vehículos de los tramos intermedios cayeron un 31,5% y un 37,9%.

### 2.2.5 Auditorías energéticas

La auditoria energética es un proceso sistemático por el cual la empresa obtiene información sobre su consumo energético, las variables que afectan de alguna forma a dicho consumo y las distintas maneras de incidir en ellas para poder reducir el consumo de energía. Una vez realizada la auditoría se redacta un plan de actuaciones, que se pone en marcha, comprobando luego si los objetivos se cumplen.

Los objetivos y las etapas se muestran a continuación:



Ilustración 2.2.5.1

- La toma de datos se suele hacer mediante: encuestas, aforos, entrevistas, observación directa, documentos, sistemas de información in situ.
- Para hacer el inventario de la flota se necesita conocer: las características de cada vehículo (consumos, emisiones, edad, potencia, plan de mantenimiento...), listado del personal implicado, instalaciones de uso, horario y frecuencias, tiempos y distancias, etc.
- De la situación actual necesitamos conocer: dimensionado de la flota, rutas de transporte, localización de puntos de recogida/entrega, tiempos, inventarios energéticos y ambientales (consumos y emisiones) y políticas de mantenimiento y renovación. Para realizar una diagnosis de la situación es necesario definir indicadores claves del rendimiento, que son valores de referencia para medir la eficiencia energética de las distintas actividades de la empresa.





Ilustración 2.2.5.2

Los indicadores que se suelen utilizar son: índices de estructura del personal, índices de estructura del parque vehicular, índices de costes, índices de consumo de combustible, índices de mantenimientos e índices de aprovechamiento de los vehículos.

- Para la diagnosis de la situación futura, es necesario hacer una estimación de la evolución del mercado (horizonte, demandas, crecimiento económico-social-demográfico). Con ello se hace un cálculo de los mismos indicadores en el futuro sin aplicar actuaciones de mejora y análisis comparativo con situación actual.
- Y como fase final de la auditoría energética, se proponen actuaciones de mejora. Para cada actuación (oportunidades de ahorro) se debe incluir: descripción de la actuación, viabilidad operativa, agentes involucrados, cuantificación energética (ahorro del consumo), cuantificación económica (costes e ingresos), cuantificación medioambiental (emisiones), impacto sobre calidad de servicio y plazos y presupuesto de implantación.

Entre las oportunidades de ahorro más habituales en un plan de actuaciones se tienen: fijar un plan de renovación de la flota con vehículos de menor consumo y emisiones, establecer un programa de gestión del combustible (desde la compra hasta el control de su uso), incorporar biocarburantes como fuente alternativa, establecer un programa de formación de personal en conducción eficiente y segura, usar herramientas para la planificación y la gestión eficiente de las operaciones, usar sistemas telemáticos para la localización y el seguimiento de los vehículos, desarrollar un plan de mantenimiento de la flota y analizar periódicamente los costes de gestión de la flota.

## 2.3 Gestión eficiente de costes

### 2.3.1 Introducción

Para llevar a cabo una gestión eficiente de flotas de transporte es necesario contar con un sistema de gestión de costes de la empresa, que pueda ayudar para la fijación de precios/tarifas.

Entre las funciones habituales de un sistema de gestión de costes destacan:

- Cuantificar los costes de los servicios prestados para la elaboración de las cuentas anuales.
- Proporcionar información útil a directivos y empleados respecto a la eficiencia de los procesos internos de la empresa.
- Buscar la rentabilidad de los servicios ofrecidos.
- Comparar mensualmente los gastos reales con los presupuestados.
- Implementar medidas oportunas para minimizar costes.

Ejemplo de costes en una empresa: un vehículo de 420 CV con una MMA (masa máxima autorizada) de 40 t y una carga útil de 25 t que recorre anualmente 120.000 km con un ratio de ocupación del 85% (circulando cargado el 85% de su recorrido), tiene aproximadamente el siguiente reparto medio porcentual de costes de operación:

| Concepto               | % DEL TOTAL |
|------------------------|-------------|
| Amortización           | 14,2 %      |
| Financiación           | 1,7 %       |
| Personal de conducción | 24,9 %      |
| Seguros                | 6,5 %       |
| Costes Fiscales        | 0,8 %       |
| Dietas                 | 12,3 %      |
| Combustible            | 29,4 %      |
| Neumáticos             | 5,5 %       |
| Mantenimiento          | 1,7 %       |
| Reparaciones           | 3,0 %       |
| TOTAL                  | 100 %       |

Ilustración

### 2.3.2 Tipos de Costes:

Los costes de los servicios de transporte pueden ser:

**Costes Directos:** Son los costes asociados de manera directa con un servicio de transporte. Pueden dividirse en:

- Costes Fijos: Son aquellos costes directos que se mantienen constantes con independencia del número de servicios que se realicen. Dentro de este grupo estarían:

- o Salarios de los conductores y seguros sociales a cargo de la empresa
- o Tributos (impuestos fiscales): sobre el vehículo (ITV, IVTM, inspecciones y revisiones) y sobre la actividad (IAE, tarjetas de transporte y visados)
- o Seguros: sobre los vehículos y sobre la carga o pasajeros.
- o Gatos financieros: por financiación propia (capital, reservas) o ajena (intereses de préstamos, gastos de leasing o renting)
- o Amortización: por pérdida de valor de los activos fijos
- Costes Variables: Son aquellos costes directos que varían en proporción al volumen de actividad (kilómetros recorridos, horas facturadas, servicios realizados). Los principales costes variables serían:
  - o Coste de combustible: tanto el consumido por el vehículo como por los equipos auxiliares.
  - o Neumáticos
  - o Lubricantes
  - o Costes de mantenimiento y reparaciones
  - o Dietas del conductor
  - o Peajes en autopistas

**Costes Indirectos:** Son los llamados costes de estructura, aquellos no especificados al mismo servicio de transporte (costes de administración, alquiler de oficinas,...). En este grupo nos encontramos entre otros con: gastos comerciales, gastos de administración, material de oficina, equipos informáticos, seguros de bienes inmuebles y amortización de bienes inmuebles.

El cálculo de cada uno de los costes anuales anteriores para toda la flota es sencillo tomando como referencia la contabilidad de la empresa. Sin embargo el cálculo individualizado de cada uno de los costes anuales para cada vehículo no es sencillo si no se lleva una contabilidad de costes adecuada. El cálculo de costes de cada vehículo por kilómetro recorrido es muy importante para ofrecer una tarifa competitiva al cliente por los servicios a realizar. Además permite calcular aquellos vehículos que suponen un mayor coste a la empresa y por tanto puede servir como referencia en el plan de renovación de la flota.

### **2.3.3 Indicadores de eficiencia en costes**

Los indicadores, como ya se ha comentado, permiten analizar la evolución del rendimiento de la empresa en diversos aspectos de la misma. En este caso, los indicadores de costes permiten analizar en cada momento el coste de operación de cada vehículo y de la flota en su conjunto.

Cada uno de los costes anuales anteriormente expuestos se puede considerar como un indicador. Sin embargo, para analizar la evolución de los costes se hace necesario

referenciar los costes variables al nivel de actividad. Por ello, los costes variables se deben calcular por kilómetro recorrido:

- Costes anuales de combustible por km anuales recorridos
- Costes anuales de mantenimiento por km anuales recorridos
- Costes anuales de reparaciones por km anuales recorridos
- Costes anuales de neumáticos por km anuales recorridos

En general los indicadores anteriores se pueden agrupar para cada vehículo, para que sirva como referencia para ofrecer tarifas de servicios a clientes:

- Costes variables por km
- Costes fijos e indirectos por hora
- Costes totales por km
- Costes totales por hora
- Costes totales por km y hora

## **2.4 Gestión eficiente del mantenimiento**

### **2.4.1 Introducción**

El mantenimiento es uno de los factores que más influye y contribuye al rendimiento final dentro de una empresa de transporte. El mantenimiento del parque vehicular consiste en proporcionar a los vehículos reparaciones, recambios y mano de obra por parte del personal de taller con el fin de que estén siempre a su nivel máximo de operación mecánica. El objetivo principal del mantenimiento es que los vehículos se encuentren en estado óptimo de funcionamiento y que asegure además la seguridad del conductor y los pasajeros/carga. El mantenimiento buscará por tanto la máxima disponibilidad a mínimo coste.

Del objetivo principal se desprenden varias líneas de trabajo:

- Planificación del mantenimiento.
- Control:
  - \*de las operaciones de mantenimiento.
  - \*de los costes de tales operaciones.

Una falta de mantenimiento prolongada en el tiempo provoca averías en los vehículos, lo que se traduce en la no disponibilidad del vehículo hasta que se repare dicha avería y en un coste adicional para la empresa. La mayoría de las veces la avería no se concentrará en una sola pieza, sino que la pieza afectada hará que las que están a su alrededor también sufran, por lo que el número de piezas a reparar se verá incrementado. En el peor de los casos habrá incluso que sustituir el vehículo por otro.

Para llevar a cabo las operaciones de mantenimiento es necesario definir:

- Métodos y organización de las operaciones de mantenimiento

- Recursos humanos necesarios
- Recursos materiales necesarios

El tamaño de la flota, el servicio al que se dedique nuestra empresa, así como otros factores determinan la organización del mantenimiento. Dependiendo de los recursos con los que cuente nuestra empresa, y de la partida económica que se pueda destinar al mantenimiento, puede haber dos tipos de mantenimiento, uno que se realice dentro del propio taller y otro en el que esas operaciones se encarguen fuera, a un taller externo.

Se recomienda un mantenimiento planificado, a intervalos definidos o al llegar a un nivel determinado, el cual recibe el nombre de mantenimiento preventivo. Su principal misión es la de reducir el número de fallos y la gravedad de los mismos detectándolos en una etapa temprana. Se pueden distinguir dos tipos de mantenimientos preventivos:

- *Mantenimiento basado en la condición, o mantenimiento sobre condición*, es el mantenimiento preventivo realizado en base a los resultados de la monitorización del funcionamiento del equipo.

Cuando este tipo de mantenimiento se ejecuta siguiendo una predicción consecuencia del análisis y la evaluación de los parámetros significativos de la degradación del elemento se denomina *mantenimiento predictivo*.

- *Mantenimiento sistemático*, es el mantenimiento preventivo realizado en base a unos intervalos de tiempo preestablecidos, o a un número de unidades de uso (por ejemplo cada 10000 km) pero sin investigación previa de la condición del elemento.

#### **2.4.2 Objetivos de un Plan de Mantenimiento**

Los objetivos de la gestión del mantenimiento son:

- a) Minimizar los costes de los servicios de mantenimiento lo máximo posible.
- b) Disponer de los vehículos en todo momento, es decir que estén disponibles el mayor tiempo posible.
- c) Llevar un control y programación de los mantenimientos de cada vehículo. Proveer de las facilidades necesarias para que los operadores no cualificados realicen el mantenimiento mínimo requerido en los equipos.

#### **2.4.3 Etapas de un Plan de Mantenimiento**

El establecimiento de un plan de mantenimiento en una empresa de transporte requiere de una serie de etapas a llevar a cabo:

1. Nombrar un responsable, que será la persona encargada de planificar y hacer cumplir el plan de mantenimiento.
2. Asegurar que el vehículo cumple obligaciones legales:

Primer paso más allá de un plan de mantenimiento. Actividades a realizar:

- o Chequeos diarios del conductor
- o Informes de defectos
- o Inspecciones periódicas de seguridad
- o Mantener informados a los conductores
- o Marcar los vehículos no disponibles

3. Revisar la frecuencia de mantenimiento

En base a la distancia recorrida y el tipo de operación que realiza el vehículo se puede estimar la frecuencia de mantenimiento.

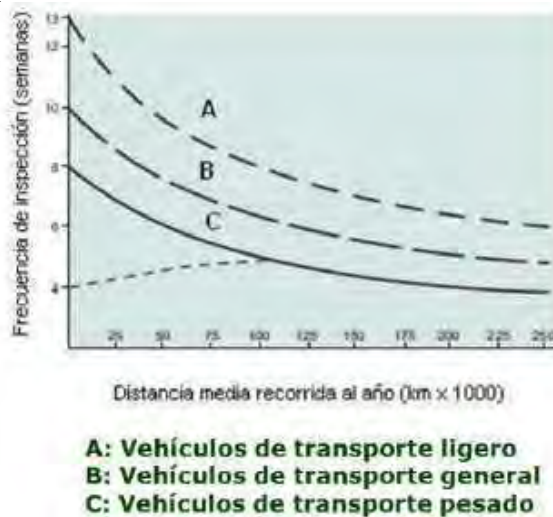


Ilustración - Frecuencia de inspección en diferentes vehículos

4. Revisar la flota

Ajustar la flota a las operaciones más adecuadas a cada vehículo: tipo de operación, terreno, equipo auxiliar, lubricante adecuado, etc.

5. Costes del ciclo de vida

Calcular costes anuales de mantenimiento. Dichos costes junto con el valor residual de cada vehículo, sirven como referencia para el cálculo de los periodos económicos a la hora de sustituir los vehículos de la flota. Es recomendable sustituir un vehículo cuando:

- o Valor residual bajo
- o Coste de mantenimiento alto

6. Cómo ejecutar el Mantenimiento

Existen varias formas de llevar a cabo el mantenimiento de una flota:

- o Subcontratar: Seleccionar Proveedores
- o Taller propio: Reglas de Mantenimiento
- o Contratar y usar taller propio.

Existen varios factores que afectan a la decisión de cómo hacer el mantenimiento:

- o Tamaño de la flota
- o Complejidad de equipos
- o Horarios de trabajo
- o Distancias a instalaciones
- o Disponibilidad de terrenos para mantenimiento propio
- o Disponibilidad de los vehículos de ser mantenidos

Las principales ventajas de poseer taller propio son:

- o Programación flexible de vehículos
- o Ahorro en desplazamientos (tiempo y combustible)
- o Si los vehículos son especiales, hay menos empresas subcontratistas
- o Dejar de ser uno más en cola

#### 7. Tener el apoyo de la empresa

Es fundamental para un mantenimiento eficiente, adquirir compromiso de la empresa, a través de la dirección, el personal de mantenimiento y los conductores.

#### 8. Controlar el rendimiento

Finalmente y como paso esencial para la mejora continua, hay que hacer uso de indicadores claves del rendimiento y de herramientas de apoyo (GMAO, localización de flotas)

La puesta en marcha de un plan de mantenimiento requiere del uso de soportes de información y planificación, como:

- Ordenes de trabajo
- Intervalos de mantenimiento
- Registro de operaciones

### 2.4.4 **Indicadores del Mantenimiento**



Se pueden usar los siguientes indicadores:

- *MTBF, (Mean time between failures)*: Tiempo Medio Entre Fallos, el objetivo básico es que el vehículo tenga un MTBF elevado y estable, porque eso querrá decir que los fallos están controlados, y por tanto se tiene la oportunidad de prevenirlos. Un MTBF que fluctúe indica que el vehículo no está en absoluto controlado.
- *MTTR, (Mean time to repair)*: Tiempo Medio Para Reparar, conocer exactamente el tiempo dedicado a las intervenciones, conocer porqué y cómo se está invirtiendo el tiempo para reparar, qué problemas adicionales tiene el personal de mantenimiento, etc.
- *% de Mto. Preventivo versus % de Mto. Correctivo*, del total de mantenimiento realizado a cada vehículo. Un buen Mantenimiento sería aquel en el que el 90% de las intervenciones fuesen planificadas, el esfuerzo debe orientarse hacia aquí.
- *Nº de Fallos*: El número de ellos y cuántos de cada categoría. Puede darse el caso que la gran mayoría de ellos sean Averías, por tanto el coste asociado será elevado tanto en mano de obra como en materiales, o puede que las Paradas hagan que el vehículo tenga una eficiencia muy pobre, por tanto también el coste se verá afectado.

## **2.5 Gestión eficiente de operaciones:**

### **2.5.1 Introducción**

La planificación y gestión de las operaciones en empresas con una flota de vehículos tiene como objetivo cumplir con los servicios ofertados al cliente a mínimo coste de operación. Es decir, hay que coordinar todos los recursos disponibles (humanos y materiales) para cumplir las relaciones contractuales de los servicios al cliente (fechas de entrega, productos, seguridad), todo ello con unos ciertos criterios económicos para la empresa.

Las decisiones se pueden agrupar en dos tipos:

- Decisiones estratégicas: a medio plazo, como pueden ser: el dimensionado de la flota para ajustar oferta y demanda, el diseño de las zonas o rutas fijas de reparto/recogida, el cálculo de horarios fijos de rutas, el dimensionado de la estructura de personal necesaria, etc.
- Decisiones tácticas u operativas: a corto plazo para organizar los recursos necesarios a los servicios, como pueden ser: el reparto de pedidos entre los vehículos disponibles, la distribución de la carga en cada vehículo, el diseño de la ruta dinámica de reparto/recogida, el cálculo de las jornadas diarias, la asignación de conductores a cada jornada de trabajo, etc.

### **2.5.2 Fases en la gestión operativa de flotas**



Cada tipo de empresa de transporte tiene sus propias características de operación, por lo que es habitual encontrarse estudios independientes por sectores (transporte de pasajeros) o por tipos de problemas (problemas de rutas de vehículos). Sin embargo, varias actividades son comunes a todas ellas, como el diseño de rutas o la asignación de conductores. A continuación proponemos algunas de las actividades comunes en cualquier empresa de transporte ordenadas por etapas:

– Etapa 1: Diseño o cálculo de rutas eficientes

Para realizar un mejor uso de los vehículos que componen la flota y de los conductores, mejorando la eficiencia operativa, se pueden diseñar rutas de transporte de mínimo recorrido, coste o tiempo.

– Etapa 2: Planificación de la oferta

Cálculo de los vehículos necesarios para satisfacer la demanda y los horarios. Se debe realizar una gestión eficiente de conductores y de reparto de las cargas de los vehículos.

– Etapa 3: Planificación de los servicios

Cálculo de las jornadas de trabajo (servicio) que debe realizar un único conductor, cumpliendo condiciones de convenio.

– Etapa 4: Planificación del personal

Asignación de cada conductor a cada jornada de trabajo, cumpliendo las condiciones contractuales.

– Etapa 5: Gestión de la operación

Actividades de administración y control sobre la actividad del transporte, las entregas y recogidas, seguimiento de la flota, de las incidencias, etc.

Otras consideraciones a tener en cuenta son las relacionadas con las Legislaciones vigentes en materia de transporte. Al diseñar un plan de gestión eficiente de flotas es imperativo considerar las legislaciones vigentes, ya que éstas pueden señalar restricciones importantes, tales como límites de velocidad de los vehículos, capacidad máxima en peso o volumen, horarios de circulación por determinadas zonas, tiempos máximos de circulación, entre otras.

### 2.5.3 **Tipos de rutas**

Como se acaba de comentar, una de las etapas comunes a todas las empresas de transporte consiste en el diseño de rutas eficientes. Los tipos de rutas marcan no obstante el periodo de cálculo de las mismas: rutas fijas suelen mantenerse en el tiempo, mientras que rutas dinámicas requieren nuevos diseños de forma continua.

- *Rutas fijas:*

Son rutas permanentes, no sujetas a cambios, con puntos de recogida y entregas fijos. La flota y el personal suelen ser estable. La planificación es sencilla y rutinaria. No se garantiza la ocupación completa de los vehículos.

- *Rutas periódicas:*

Son rutas fijas respecto a los puntos de recogida y entregas pero varían los días de recogida y entrega (estacionalidad).

- *Rutas dinámicas:*

Atiende a necesidades cambiantes del cliente. Existen frecuentes rotaciones de vehículos y personal. Necesita una planificación diaria desde el departamento de tráfico. Mayor aprovechamiento del vehículo y del personal.

#### 2.5.4 **Diseño eficiente de rutas**

Al realizar una optimización adecuada de las rutas, se pueden alcanzar beneficios en el área de transporte, reduciendo los costes totales de esta área entre un 10% y 20%. Adicionalmente a la reducción de costes, se pueden obtener diversos beneficios como la reducción de tiempos, reducción de distancias recorridas, aumento eficiente de la utilización de la flota, reducción del trabajo administrativo, mejora del servicio al cliente, mejor organización de los recursos: tiempo, vehículos disponibles, operadores.

El objetivo principal del diseño de rutas es distribuir a mínimo coste una serie de objetos o personas entre una serie de instalaciones a través de vehículos con capacidad limitada. En el transporte de mercancías, el problema es definir las rutas de envío de mercancías desde uno o varios centros de envío a uno o varios puntos de entrega, cumpliendo la cantidad demandada y las fechas de entrega, y con mínimo uso de recursos (mínimo coste). En el transporte de pasajeros se busca localizar las paradas de recogida de pasajeros y definir las rutas, cumpliendo una cierta calidad de servicio a mínimo coste.

Las empresas de transporte a la hora de acometer esta tarea de planificar sus rutas de recogida o reparto con los vehículos de su flota, se presentan con serios problemas en muchas ocasiones. Tienen que cumplir una serie de restricciones o limitaciones para realizar su servicio, como son:

- Una disponibilidad y una capacidad de sus vehículos limitada
- Unas condiciones estrictas para las fechas/horas de recogida o entrega
- Unas condiciones especiales de las rutas respecto a las características de sus vehículos

Se presenta pues un problema de gran complejidad, donde muchas veces no se dispone de una herramienta de ayuda y se toman soluciones intuitivas basadas en la experiencia y sin ninguna base cuantitativa. Esta tarea es crítica en las empresas de

transporte porque impacta directamente en los costes y en el servicio al cliente, y como resultado de una mala planificación se puede ver afectada la rentabilidad, se puede caer en incumplimientos o retrasos en las entregas y se pueden incurrir en excesivos costes de transporte e inventario.

Las decisiones manuales en base a la experiencia son poco precisas, no cuantificables y en la mayoría de los casos más costosas que usando herramientas automáticas de planificación de rutas.

Los principales beneficios de estas herramientas de ayuda a la toma de decisión son:

- Reducen los tiempos de búsqueda de soluciones
- Reducen los costes: menor uso de recursos y de tiempos de viaje
- Permiten realizar cambios de última hora

#### **2.5.4.1 Etapas en la planificación de rutas**

Se diferencian las etapas para el diseño y planificación de rutas de transporte según sea de pasajeros o de mercancías.

##### *– Transporte de mercancías:*

El transporte de mercancías por cuenta propia es el más habitual. Los conductores y vehículos pertenecen a una empresa. Existe habitualmente un centro común o base donde están las oficinas, talleres y almacenes. Desde este centro se envía la mercancía que solicitan los clientes en determinados puntos de entrega a determinadas horas.

Un primer paso será analizar los diversos puntos de entrega para agrupar las mercancías en cada vehículo sin superar la capacidad máxima.

Uno de los aspectos importantes de la planificación de rutas es la vuelta del vehículo a la base para seguir realizando servicios. La búsqueda de puntos de retorno con carga puede minimizar tiempos muertos y kilómetros en vacío, pero puede aumentar los costes por dietas o un repostaje fuera de la base. Hay pues que seleccionar el punto con mejores condiciones de carga de retorno.

Una vez se sepan los puntos de entrega y de retorno de cada vehículo, se pasa a calcular la ruta de mínimo coste (distancia, consumo, dietas, etc.) de cada vehículo.

A continuación se calculan los horarios que cumplan las fechas y horas de entrega con el mínimo retraso y mínimas esperas.

Con los horarios calculados y el orden de entrega, se calculan las rutas exactas a través del uso de navegadores o herramientas GIS. Con ello se comprobarían los kilómetros y costes exactos.

##### *– Transporte de pasajeros:*

En las empresas de transporte de pasajeros, la primera fase en el proceso de planificación del transporte consiste en el diseño de las rutas o líneas de transporte de forma que se consiga recoger al máximo número de pasajeros que desean desplazarse de una zona a otra, con el menor coste posible.

Para el diseño de las rutas es necesario conocer primero la demanda de viajeros, que vendrá reflejada por el número de viajes que desean realizar los habitantes de una zona

o ciudad. Por otro lado, se dispone de una oferta expresada como el viario urbano o interurbano y por último existirán criterios que se desean imponer al diseño. Los resultados obtenidos en esta fase serán nuevas líneas de transporte, mejoras de líneas existentes o estrategias de operación. Estas líneas de transporte quedan expresadas a través de la localización de las paradas y del diseño del recorrido.

Una vez conocidas las líneas de transporte, la segunda fase es la del **cálculo de frecuencias de paso y horarios**. Los datos de entradas para esta segunda fase son: la demanda de pasajeros desagregada por franjas horarias y por parada así como la política de servicio, algunos autores indican la necesidad de conocer los vehículos disponibles. Las salidas obtenidas en esta fase son las frecuencias de paso por parada y franja horaria y posteriormente, junto con procesos de sincronización, los horarios de salida y llegada de vehículos a las paradas.

#### 2.5.4.2 Métodos de cálculo de rutas eficientes:

A continuación se revisan diferentes métodos de cálculo de rutas eficientes, de menor a mayor complejidad, tal y como han ido perfeccionándose la modelización de la realidad del problema del transporte de flotas de vehículos.

##### – Problema TSP

El problema más común que se presenta en el diseño de rutas es el problema de viajero de negocios o TSP (Travelling Salesman Problem). Este problema se define como aquel en el que un viajero sale de un punto de partida y tiene que recorrer varios destinos, tocando una sola vez cada uno, y al final tiene que regresar a su lugar de origen, minimizando la distancia a recorrer.

Se puede decir que el clásico TSP es un problema sin restricciones, sin embargo en la realidad la gran variedad de situaciones que se pueden presentar en un TSP dan lugar a que se estudien muchas variantes de este problema, algunas de estas pueden ser debido al número de vehículos, a la cantidad de puntos de origen, en restricciones en la carga o capacidad de los vehículos, entre muchos otros.

El problema m-TSP es una de estas variantes, supone un solo punto de origen, pero con varios vehículos (o el recurso que se utilice) para el recorrido de todos los destinos, al igual que en el TSP, los destinos solamente deben ser visitados una vez cada uno.

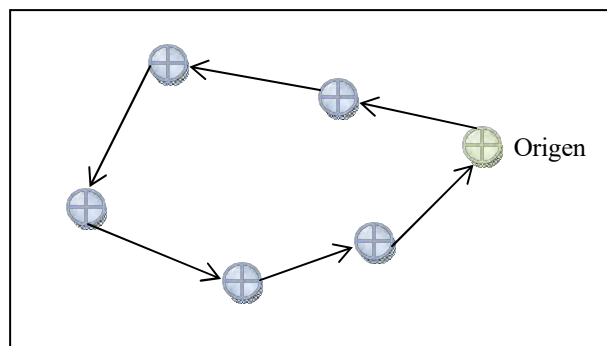


Ilustración. Representación gráfica del problema TSP.

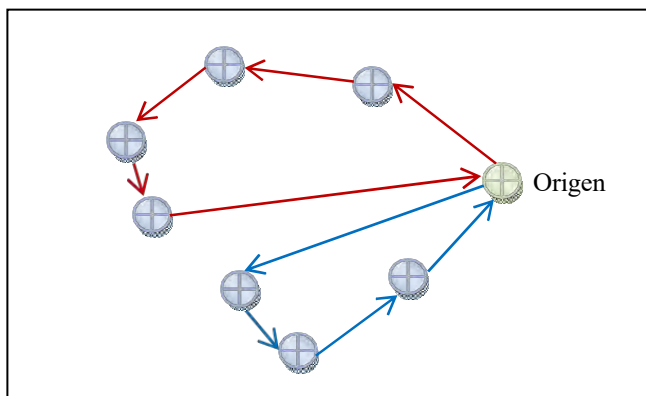


Ilustración. Representación gráfica del problema m-TSP

### – Problema VRP

Una evolución a los problemas TSP son los problemas de diseño de rutas de reparto, VRP (Vehicle Routing Problem). En este tipo de problemas se plantea que un conjunto de rutas visite determinado número de destinos, a partir de uno o varios orígenes, considerando restricciones de capacidad y/o tiempo. El objetivo del diseño de las rutas es que se obtenga la mínima distancia recorrida, cumpliendo con las restricciones especificadas.

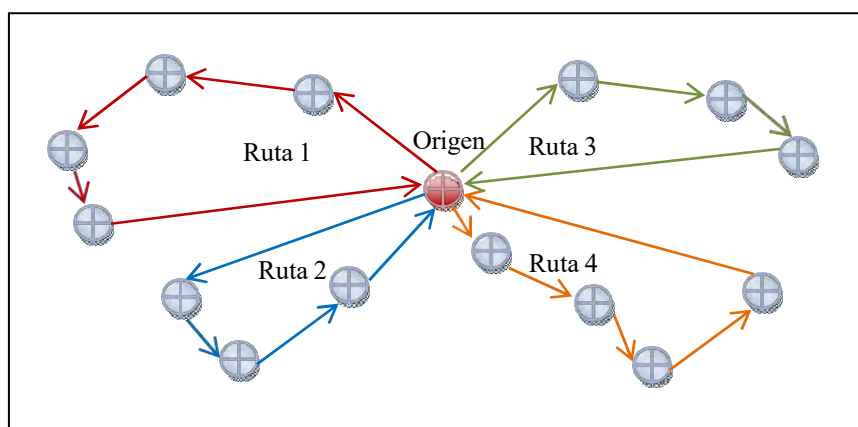


Ilustración. Representación gráfica del problema VRP.

A continuación se muestra una clasificación de los problemas más frecuentes en el diseño de rutas.

| Problema                   | Características                                                                                                                                                      | Optimizar                         |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| TSP (clásico)              | Diseñar una ruta para un único vehículo que tiene que pasar por "n" ciudades (o clientes) a partir de un único origen (o almacén).                                   | Distancia recorrida.              |
| m-TSP                      | Diseñar las rutas de "m" vehículos que tienen que pasar, entre todos, por "n" nodos a partir de un único origen.                                                     | Distancia total de las "m" rutas. |
| VRP con un único depósito  | Diseñar las rutas de "m" vehículos que visitan, entre todos, cada uno de los "n" nodos a partir de un único origen y cumpliendo con las "restricciones" del sistema. | Función de coste del sistema.     |
| VRP con más de un depósito | Diseñar las rutas de "m" vehículos que visitan, entre todos, cada uno de los "n" nodos a partir de                                                                   | Función de coste del sistema.     |

|                              |                                                                                                                                                                                                  |                                                                                                                        |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
|                              | más de un origen y cumpliendo con las "restricciones" del sistema.                                                                                                                               |                                                                                                                        |
| CVRP<br>(Capacitated VRP)    | Diseñar las rutas de "m" vehículos que visitan, entre todos, cada uno de los "n" nodos a partir de un único origen y donde cada vehículo tiene una capacidad C y una ruta no puede sobrepasarla. | Función de coste del sistema teniendo en cuenta las capacidades.                                                       |
| VRPTW (VRP with time window) | Diseñar las rutas de "m" vehículos que visitan, entre todos, cada uno de los "n" nodos a partir de un único origen y donde cada cliente tiene una ventana de tiempo en la que desea ser servido. | Función de coste del sistema teniendo en cuenta las ventanas del tiempo.                                               |
| CVRPTW                       | CVRP + VRPTW                                                                                                                                                                                     | Función de coste del sistema teniendo en cuenta las ventanas de tiempo de los clientes y la capacidad de cada recurso. |

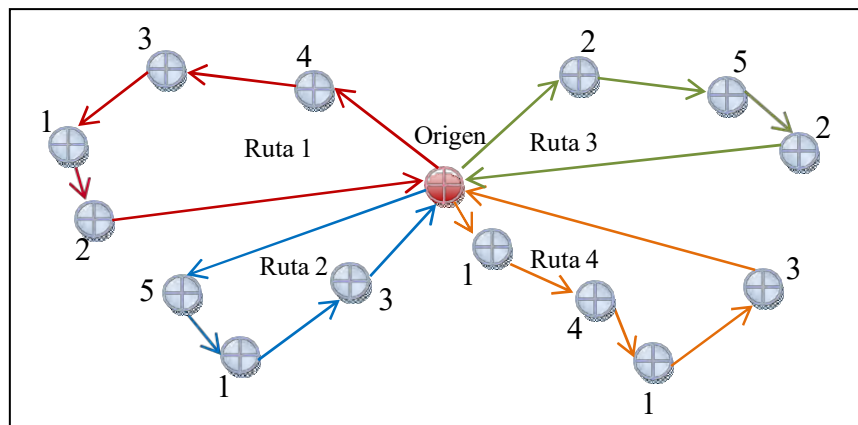


Ilustración. Representación gráfica del problema CVRP.

#### 2.5.4.3 Asignación eficiente de vehículos

Los vehículos de una flota se definen por un conjunto de atributos, como son: su capacidad de carga en peso, en volumen, sus costes asociados, etc. En la utilización de los vehículos se incurren en costos fijos por el uso y en costos variables que dependen de las distancias recorridas, el tiempo, entre otros parámetros. Uno de los retos más importantes en la gestión del transporte es la utilización de una flota idónea en términos de capacidad, flexibilidad, accesibilidad, seguridad y coste.

Al momento de elegir el vehículo ideal para el transporte de mercancías es necesario considerar algunos factores, tales como:

- Tipo de vehículo
- Capacidad en peso
- Capacidad en volumen
- Tipo de carrocería de acuerdo a la mercancía que se transporta
- Equipos adicionales requeridos
- Acondicionamiento del vehículo para el confort en la conducción

La selección del vehículo dependerá entonces de la mercancía que se vaya a transportar (tipo de mercancía, cantidad en peso y volumen), del tipo de ruta a seguir, de los requerimientos del cliente, así como de la que convenga más a la empresa en términos de costo y tiempo.

En el caso del transporte público de pasajeros los factores a considerar para la selección del vehículo ideal son:

- Tipo de ruta, si se trata de una local o foránea.
- Capacidad en número de personas que pueden transportar.
- Redes viarias.
- Red de carreteras.

#### **2.5.4.4 Asignación eficiente de conductores:**

Para optimizar la eficacia de los recursos humanos se pueden utilizar los mismos modelos matemáticos y las mismas técnicas de programación matemática aplicados a la organización y distribución de los recursos físicos. En empresas de transporte público de pasajeros es esencial una asignación óptima de conductores dado que el potencial humano constituye el factor de coste más relevante.

En etapas anteriores, se han ajustado los vehículos al nivel de demanda de los usuarios, tanto en itinerarios como en frecuencia de paso. En la asignación eficiente de conductores hay que coordinar estos itinerarios y frecuencias de paso con los calendarios laborales y condiciones contractuales de los conductores de la flota. Para ello, se plantean dos problemas a resolver:

- *Crew Scheduling*. Organización de las jornadas de trabajo. Esta fase comprende el proceso por el cual se elaboran las jornadas de trabajo y se determinan los puntos de relevo, es decir el conjunto de partes de trabajo efectuadas por un mismo conductor.
- *Rostering*. Una vez determinadas las jornadas de trabajo, el siguiente paso es asignar estas jornadas a trabajadores concretos, considerando una serie de factores como son: periodos de descanso, días libres, cambios de turno y número total de horas trabajadas.

## **2.6 Renovación de flotas**

### **2.6.1 Introducción**

Debido a los costes fijos por amortización y depreciación, el coste total de operación de un vehículo nuevo siempre es más elevado que el de una unidad antigua, pero a cambio de eso, obtenemos un vehículo que consume menos energía y tiene unas prestaciones operacionales mejores, lo que asegura su disponibilidad.



La renovación oportuna de los vehículos en las empresas transportistas se refleja en un conjunto de beneficios significativos, ya que además del ahorro en el consumo de combustible, se tienen importantes ventajas tales como los ahorros en el mantenimiento en los primeros años de operación de la unidad y una mayor disponibilidad del vehículo al reducirse los tiempos de inmovilización en el taller.

El factor considerado normalmente como más importante para una empresa de transporte, es mantener en operación cada vehículo el máximo tiempo posible, a pesar de que los costes de mantenimiento aumenten cada vez más, o que se tenga un sistema bien controlado en la operación de las unidades desde el punto de vista económico.

La falta de conocimientos sobre los costes de operación llevan a las empresas a prolongar indefinidamente la vida de sus flotas, por lo que es necesario dar seguimiento a los costes de operación, ya que éstos son básicos para determinar el periodo exacto para dar de baja el vehículo, y seleccionar el más adecuado para las operaciones de la compañía. Estos factores se vinculan directamente con la rentabilidad de una empresa de transporte.

Los vehículos antiguos ya han terminado de pagar los gastos financieros derivados de la amortización del crédito y tampoco tienen cargos por depreciación contable.

Al prolongar la vida útil de un vehículo, se llega a gastar en mantenimiento el equivalente al valor nuevo de la unidad cada 5 o 6 años; este gasto se reparte en el tiempo por lo que no lo percibe el transportista. Sin embargo, es conveniente preguntarse si no es mejor cambiar antes las unidades, aunque esto implica gastos financieros por amortización de préstamos, que resulta más costoso en los primeros años de uso de la unidad que el sobrecoste provocado por un mayor mantenimiento de una unidad antigua.

La mayoría de las empresas de transporte tienen una política de renovación, que puede estar definida en términos del kilometraje recorrido, por la edad del vehículo, o por ambas. Una vez que se haya comprado la nueva unidad es importante planificar su mantenimiento.

Los métodos para decidir el periodo óptimo de reposición se pueden clasificar en tres grandes categorías:

i Métodos contables:

En estos métodos se considera el vehículo de transporte como un activo contable que se deprecia en el tiempo. A medida que disminuye el valor de éste, se incorporan reformas no originales que aumentan el valor de rescate del vehículo. Se suele comparar el valor de rescate o comercial de la unidad cuando exista algún mercado de reventa de los vehículos usados, con el coste acumulado de mantenimiento del vehículo. Cada vez que el coste acumulado de mantenimiento supera el valor comercial de la unidad, se encuentra un periodo oportuno para renovarlo.

El criterio teórico para determinar el momento ideal para remplazar un vehículo, se puede considerar de acuerdo con la siguiente fórmula como aquel que proporciona el menor coste promedio anual, es decir:



$$CPA = \frac{(DA + MA)}{t}$$

donde: CPA= Coste promedio anual  
DA= Coste de Amortización acumulada  
MA= Coste de Mantenimiento acumulado  
t = Periodo en años

Sin embargo el momento exacto será cuando el coste total anual supere al coste promedio anual. La siguiente gráfica muestra el momento exacto de la renovación para un vehículo como ejemplo:

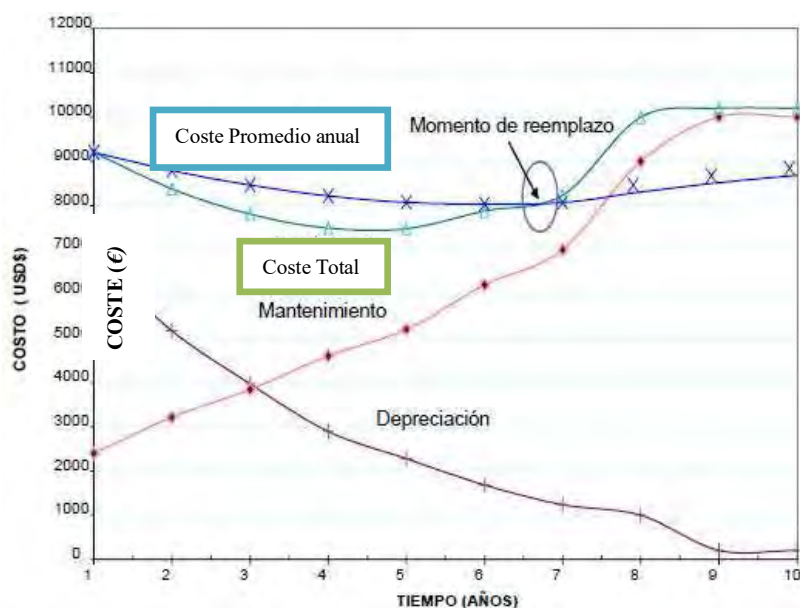


Ilustración – Momento de reemplazo de un vehículo

## ii Métodos extracontables

Se les denomina métodos extracontables a los métodos de contabilidad analítica que permiten calcular el coste total de transporte, a partir de una desagregación de las cuentas de la contabilidad general. Dentro de estos métodos extracontables, el más conocido es el método del coste unitario anual: Consiste en calcular a lo largo de la vida útil de las unidades, el conjunto de costes fijos y variables por familia de vehículos. Al dividir esta cantidad por el kilometraje anual o acumulado, se deduce un coste unitario de utilización para cada categoría de vehículos. Cada vez que se observa un valor mínimo de este coste, es oportuno cambiar las unidades involucradas. De no proceder así, la empresa tendría que soportar más adelante costes crecientes de utilización.

## iii Métodos de optimización

Los métodos referidos permiten determinar uno o varios periodos de renovación vehicular. Pero en ningún momento permiten decidir cómo reponer las unidades, porque no toman en consideración algunos puntos críticos tan importantes como son la disponibilidad financiera de la compañía o su capacidad crediticia, y su política de renovación si es que la empresa la tiene definida. Se han desarrollado

métodos de optimización desarrollados de los cuales los más utilizados por empresas de transporte de mercancías y pasajeros, son el método del margen de utilidad y el método del coste de posesión.

## **2.6.2 Consideraciones de empleo del vehículo**

A la hora de comprar el nuevo vehículo, lo primero es hacer un estudio de sus condiciones de empleo del para satisfacer la demanda. En dicho estudio hay que considerar entre otros factores:

- Tipo de itinerario
- Tasa prevista de retorno en vacío
- Peso máximo
- Factor tiempo de empleo
- Kilometraje a recorrer
- Condiciones externas de relieve y calidad de la carretera.

Se debe tener en cuenta que un vehículo de alto precio no es necesariamente el mejor para realizar el servicio, pues incurren en mayores costes de mantenimiento, consumo, emisiones, etc. Incluso vehículos de una misma clase, con precios similares, pueden pertenecer a tecnologías diferentes, y unos pueden ser adecuados y otros no.

## **2.6.3 Consideraciones económicas**

Una vez se disponga de un listado con los vehículos que mejor se ajustan a las condiciones de empleo, el paso siguiente consiste en realizar un estudio comparativo de costes y seleccionar el tipo de financiación más adecuada. Respecto al tipo de financiación para la adquisición de vehículos se tienen las siguientes posibilidades:

- Capital propio, que proceden de ahorro, beneficio, amortización, valor residual
- Capital ajeno (crédito a medio plazo)
- Arrendamiento (contrato y promesa unilateral de venta)

También hay que seleccionar una política de mantenimiento y otra de amortización o depreciación del vehículo, que puede ser lineal o no lineal (acelerada). En esta política hay que definir un periodo de amortización que depende de factores como: la evolución del coste de mantenimiento o el envejecimiento tecnológico del vehículo.

Finalmente, los costes de operación, los costes fijos junto con el precio real y el valor residual del vehículo se han de considerar para la elección del vehículo más adecuado.

En resumen, es claro que no sólo el precio de compra basta como parámetro determinante de una política de compra. Comprar a precio barato puede resultar engañoso si no se toman en cuenta los costes de operación del vehículo

## **2.7 Dispositivos de control y seguimiento**

### **2.7.1 Introducción**

Hay ingentes cantidades de tecnología encaminadas a ayudar a crear operaciones eficientes. Muchos de estos avances tecnológicos tienen una influencia directa en el consumo de combustible. Sin embargo, la más precisa tecnología no puede sustituir la eficiencia de una persona.

El principal beneficio de las aplicaciones telemáticas es que pueden ayudar en la gestión efectiva y eficiente de los recursos con un ahorro importante del consumo de combustible. Hay que asegurarse, por otra parte, de que los empleados han recibido una formación para su buen uso.

### **2.7.2 Información de sistemas de tráfico**

Son sistemas de trabajo en red que proporcionan datos en directo del estado del tráfico. Estos servicios pueden planear rutas en tiempo real, emiten recomendaciones basadas en predicciones, datos históricos e información sobre las incidencias del tráfico.

Además de la información que se pueda obtener por radio o televisión hay también sistemas de información gratuitos que se pueden descargar de internet. También existen servicios privados que cobran una tarifa anual a cambio de la información, la cual llega directamente al conductor del vehículo vía GPS. El principal beneficio de usar estos sistemas es que ayudan a evitar o minimizar las congestiones de tráfico.

### **2.7.3 Herramientas para la planificación de viajes**

Un planificador de viajes es un programa de software que contiene una red digital de carreteras, con las carreteras definidas por categorías y velocidades. Tiene la capacidad de calcular la mejor ruta entre dos puntos dados y también es capaz de calcular la mejor ruta cuando existen nodos intermedios. El principal propósito es calcular tiempo, distancias y costes de cada viaje.

Los planificadores de viajes pueden ayudarnos a encontrar una ruta eficiente en términos de consumo de combustible. Hay algunos que se pueden descargar de forma gratuita de internet.

### **2.7.4 Sistema de planificación de rutas computerizados**

Un sistema de planificación de rutas computerizado (CVRS), combina datos de localización del usuario con la entrega o recogida de productos (como pueden ser la cantidad y el peso) para crear una planificación más eficiente de una flota de vehículos y de conductores. Las principales ventajas son: el ahorro de tiempo a la hora de realizar la planificación si lo comparamos con los métodos tradicionales, el ahorro de combustible y la menor necesidad de vehículos y de conductores. También tienen la capacidad de tener en cuenta situaciones en las que dos productos no deben ser cargados en el mismo vehículo.

### **2.7.5 Sistemas de navegación por satélite**

Estos sistemas llevan un GPS y una pantalla para no tener la necesidad de consultar un mapa de carretera. Permiten a los conductores planificar su ruta y recibir instrucciones una vez que han emprendido ya el viaje. Incluyen mapas detallados que son expandibles para poder incluir ciudades y calles adicionales. El dispositivo calcula el tiempo del viaje una vez que son planeados y se actualizan cuando vas en ruta hacia el destino final.

Eliminan la necesidad de los conductores de llevar anotaciones de cómo llegar al destino, lo que les permite concentrar su atención en la carretera, permitiendo una conducción más eficiente y ahorro de combustible en carretera.

También reducen el tiempo de planificación, los recorridos innecesarios, así como disminuyen el tiempo medio del viaje. Algunos sistemas pueden ayudar también a los conductores advirtiéndoles de problemas de tráfico y con la posibilidad de rediseñar la ruta a seguir.

Aunque tiene muchas ventajas su utilización, los conductores no pueden confiar ciegamente en ellos, ya que no detectan algunos problemas que nos podemos encontrar, como puentes bajos, zonas en obras, etc.

## **2.8 Software de gestión de flotas**

### **2.8.1 Introducción**

Las empresas que desarrollan herramientas para la gestión de flotas, se centran en tres aspectos de forma independiente:

- **Herramientas de localización y seguimiento de flotas:** utilizan sistemas de información y dispositivos telemáticos a bordo de los vehículos para llevar un control en tiempo real de la flota y elaborar informes de las rutas y los servicios prestados día a día. Estas herramientas están integradas dentro de un Sistema de Información Geográfica (GIS) e incorporan la generación de rutas óptimas origen-destino. En general incorporan el envío de mensajes desde la central al vehículo y en algunas ocasiones se incorpora el envío bidireccional. Algunas de

estas herramientas incorporan funciones específicas como la gestión de alertas o la gestión del tacógrafo digital.

- **Herramientas de planificación y operación de rutas:** se encargan principalmente del cálculo y definición de las rutas de los vehículos, la asignación de los conductores, la distribución de la carga o el orden de visita de los clientes. Las decisiones más adecuadas se basan en modelos matemáticos debido a la dificultad en el cálculo de las funciones antes mencionadas. Estas herramientas se integran dentro de un GIS y tienen en cuenta los requisitos de las operaciones (horarios de entrega/recogida, capacidades de los vehículos, restricciones de
- **Herramientas de control del combustible y el mantenimiento:** son las de menor coste y las más utilizadas para la gestión de flotas de tamaño medio/bajo. Estas herramientas incorporan de forma integrada los módulos de abastecimiento de combustible, mantenimiento de neumáticos, reparaciones y revisiones de vehículos. En estas herramientas se lleva un control de los gastos en combustible, mano de obra, consumibles y repuestos, que supone una parte importante de los costes de una flota. Todas ellas incorporan informes mediante tablas y/o gráficos de los datos más importantes (consumos, kilómetros recorridos, costes en reparaciones,...). Algunas herramientas permiten el traspaso de la información de costes a las herramientas contables de la empresa, o bien la captura de información de otros dispositivos instalados como GPS.

## 2.8.2 Comparaciones entre las distintas herramientas:

En la siguiente tabla se muestran las herramientas comerciales más usadas en el ámbito de los procesos involucrados en la gestión de flotas de transporte, presentando para cada una de ellas una descripción básica y las limitaciones de uso que presentan:

| HERRAMIENTA         | EMPRESA                            | DESCRIPCIÓN                                                                                                                                                                                                | LIMITACIONES                                                                                                                                                                     | ENLACE                                                            |
|---------------------|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| MOVILOC             | GMV                                | Servicio para la gestión, localización y seguimiento de flotas de vehículos. Diseñado para proporcionar los datos de localización e informes de rutas y servicios para gestionar el día a día de la flota. | No incorpora aspectos relacionados con la gestión económica, energética o medioambiental.<br>No incluye la planificación de rutas.<br>No incorpora la gestión del mantenimiento. | <a href="http://www.moviloc.com/">http://www.moviloc.com/</a>     |
| Localizza Navigator | Localizza Sistemas de Localización | Servicios de localización de vehículos y de gestión de flotas en tiempo real a través de Internet.                                                                                                         | No incorpora aspectos relacionados con la gestión económica, energética o medioambiental.<br>No incluye la planificación de rutas.<br>No incorpora la gestión del                | <a href="http://www.localizza.com/">http://www.localizza.com/</a> |

|                               |             |                                                                                                                                              |                                                                                                                                                                                              |                                                                                                             |
|-------------------------------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
|                               |             |                                                                                                                                              | mantenimiento.                                                                                                                                                                               |                                                                                                             |
| TomTom WORK                   | TomTom      | Solución de navegación conectada para la gestión y el control de vehículos y conductores, con comunicación bidireccional.                    | No incorpora aspectos relacionados con la gestión económica, energética o medioambiental.<br>No incluye la planificación de rutas.<br>No incorpora la gestión del mantenimiento.             | <a href="http://www.tomtomwork.com/es/index.xml">http://www.tomtomwork.com/es/index.xml</a>                 |
| Micronav PROFESSIONAL EDITION | Micronav    | Sistemas software/hardware de control y gestión de flotas mediante las tecnologías GPS, GPRS e Internet.                                     | No incorpora aspectos relacionados con la gestión económica, energética o medioambiental.<br>No incluye la planificación de rutas.<br>No incorpora la gestión del mantenimiento.             | <a href="http://www.micronav.net">http://www.micronav.net</a>                                               |
| DataWeb 4                     | DATATRONICS | Solución para el Control y Gestión remota de Flotas en tiempo real a través de Internet/Intranet bajo un entorno 'full- web'.                | No incorpora aspectos relacionados con la gestión económica, energética o medioambiental.<br>No incluye la planificación de rutas.<br>No incorpora la gestión del mantenimiento.             | <a href="http://www.datatronics.es/">http://www.datatronics.es/</a>                                         |
| CRO                           | Involve GBI | Servicio para la optimización, cálculo y suministro de la planificación de visitas del equipo comercial.                                     | No incorpora aspectos relacionados con la gestión económica, energética o medioambiental.<br>No incluye el control y seguimiento de vehículos.<br>No incorpora la gestión del mantenimiento. | <a href="http://www.involvegb.es/OptimizacionRutas.html">http://www.involvegb.es/OptimizacionRutas.html</a> |
| fwLogistic                    | Eptisa SI   | Software en formato de framework, que permite integrar funcionalidades de optimización logística a los sistemas ya existentes en la empresa. | No incorpora aspectos relacionados con la gestión económica, energética o medioambiental.<br>No incluye el control y seguimiento de vehículos.<br>No incorpora la gestión del mantenimiento. | <a href="http://www.ti.eptisa.com">http://www.ti.eptisa.com</a>                                             |
| AXIODIS                       | Systeam     | - Herramienta de                                                                                                                             | No incorpora aspectos                                                                                                                                                                        | <a href="http://www.systeam.com">http://www.systeam.com</a>                                                 |

|                   |                             |                                                                                                                                                                                                                                                                   |                                                                                                                                                                                              |                                                                                                 |
|-------------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
|                   | Logística Empresaria        | planificación y optimización del transporte, que considera las restricciones operativas de la empresa. Permite importar datos cartográficos de distinto formato. Incorpora indicadores de gestión.                                                                | relacionados con la gestión energética o medioambiental.<br>No incluye el control y seguimiento de vehículos.<br>No incorpora la gestión del mantenimiento.                                  | om.ar/axiodis-index.htm                                                                         |
| Opti-Time Demand  | On OPTI-TIME, S.A.          | Software para planificar y optimizar los planes de trabajo de los equipos móviles en tiempo real, al tiempo que se adapta a las restricciones asociadas a los recursos y a las necesidades de los clientes.                                                       | No incorpora aspectos relacionados con la gestión económica, energética o medioambiental.<br>No incluye el control y seguimiento de vehículos.<br>No incorpora la gestión del mantenimiento. | <a href="http://www.opti-time.com">http://www.opti-time.com</a>                                 |
| ANAGO             | System Logística Empresaria | - Software de gestión del mantenimiento de flotas. Incluye: Reparaciones, Abastecimiento de Combustible, Neumáticos y Mantenimiento Preventivo.                                                                                                                   | No incorpora aspectos relacionados con la gestión medioambiental.<br>No incluye el control y seguimiento de vehículos.<br>No incluye la planificación de rutas.                              | <a href="http://www.system.com.ar/anago-index.htm">http://www.system.com.ar/anago-index.htm</a> |
| CIF-TRANS         | CIF Software                | Programa de gestión de empresas de transporte terrestre de mercancías por carretera, que permite gestionar pedidos, asignar cargas a vehículos y conductores, gestionar las comunicaciones entre la base y el camión, analizar y controlar los costes y facturar. | No incorpora aspectos relacionados con la gestión medioambiental.<br>No incluye el control y seguimiento de vehículos.<br>No incluye la planificación de rutas.                              | <a href="http://www.cif-trans.com">http://www.cif-trans.com</a>                                 |
| visualTrans FLOTA | Visual Trans                | Programa de gestión de empresas de transporte, que permite gestionar pedidos, asignar cargas a vehículos y conductores, gestionar el taller de mantenimiento, analizar y controlar                                                                                | No incorpora aspectos relacionados con la gestión medioambiental.<br>No incluye el control y seguimiento de vehículos.<br>No incluye la planificación de rutas.                              | <a href="http://www.visualtrans.es">http://www.visualtrans.es</a>                               |



|             |                                      | los costes y facturar.                                                                                                                                                    |                                                                                                                                                                 |                                                                         |
|-------------|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| phc FLOTA   | phc Software                         | Programa de gestión de empresas de transporte, para el control de la flota y conductores. Incluye gestión de costes, gestión del mantenimiento y gestión del combustible. | No incorpora aspectos relacionados con la gestión medioambiental.<br>No incluye el control y seguimiento de vehículos.<br>No incluye la planificación de rutas. | <a href="http://www.phcsoftware.es/">http://www.phcsoftware.es/</a>     |
| SOFTFLOT    | InteraSystem                         | Programa de gestión de flotas. Incluye control de costes y presupuestos, neumáticos, combustible, mantenimiento y logística.                                              | No incorpora aspectos relacionados con la gestión medioambiental.<br>No incluye el control y seguimiento de vehículos.<br>No incluye la planificación de rutas. | <a href="http://www.interasystem.com/">http://www.interasystem.com/</a> |
| FLEETMASTER | WST Servicios Web para el Transporte | Programa para la administración integral de su flota, en los aspectos más críticos como: Mantenimiento, Llantas, Combustibles, Compras e Inventarios.                     | No incorpora aspectos relacionados con la gestión medioambiental.<br>No incluye el control y seguimiento de vehículos.<br>No incluye la planificación de rutas. | <a href="http://www.wstgroup.net/">http://www.wstgroup.net/</a>         |

Tabla. Herramientas Comerciales usadas en los ámbitos de Control y Seguimiento de vehículos, Planificación de rutas y Gestión del Combustible y Mantenimiento de vehículos

Las conclusiones fundamentales del análisis de estas herramientas indican que:

- Las herramientas comerciales no integran aspectos energéticos y medioambientales. Las empresas de transporte no disponen de un sistema que evalúe el inventario medioambiental de su flota y por tanto no pueden calcular indicadores que midan la evolución de las emisiones de diversos agentes contaminantes.
- Las herramientas para las empresas de transporte pertenecen a 3 categorías: a) seguimiento de vehículos (*MOVILOC*, *Localizza Navigator*, *TomTom WORK*, *Micronav*, *DataWeb 4*), b) planificación de rutas (*CRO*, *fwLogistic*, *AXIODIS*, *Opti-Time*), y c) gestión del combustible y el mantenimiento (*ANAGO*, *CIF-TRANS*, *visualTrans*, *phc FLOTA*, *SOFTFLOT*, *FLEETMASTER*). Las herramientas comerciales se ofrecen por separado aunque ofrecen la posibilidad de integrar dos de ellos, normalmente el b) con el a) o bien el c) con el a). Esta posibilidad implica una mayor inversión y normalmente las empresas de transporte adquieren sólo una de las herramientas. No se ha encontrado una herramienta que integre las 3 categorías.
- Las herramientas comerciales se enfocan principalmente para el transporte terrestre de mercancías y no consideran en general otros sectores como el transporte de pasajeros o la recogida de residuos.





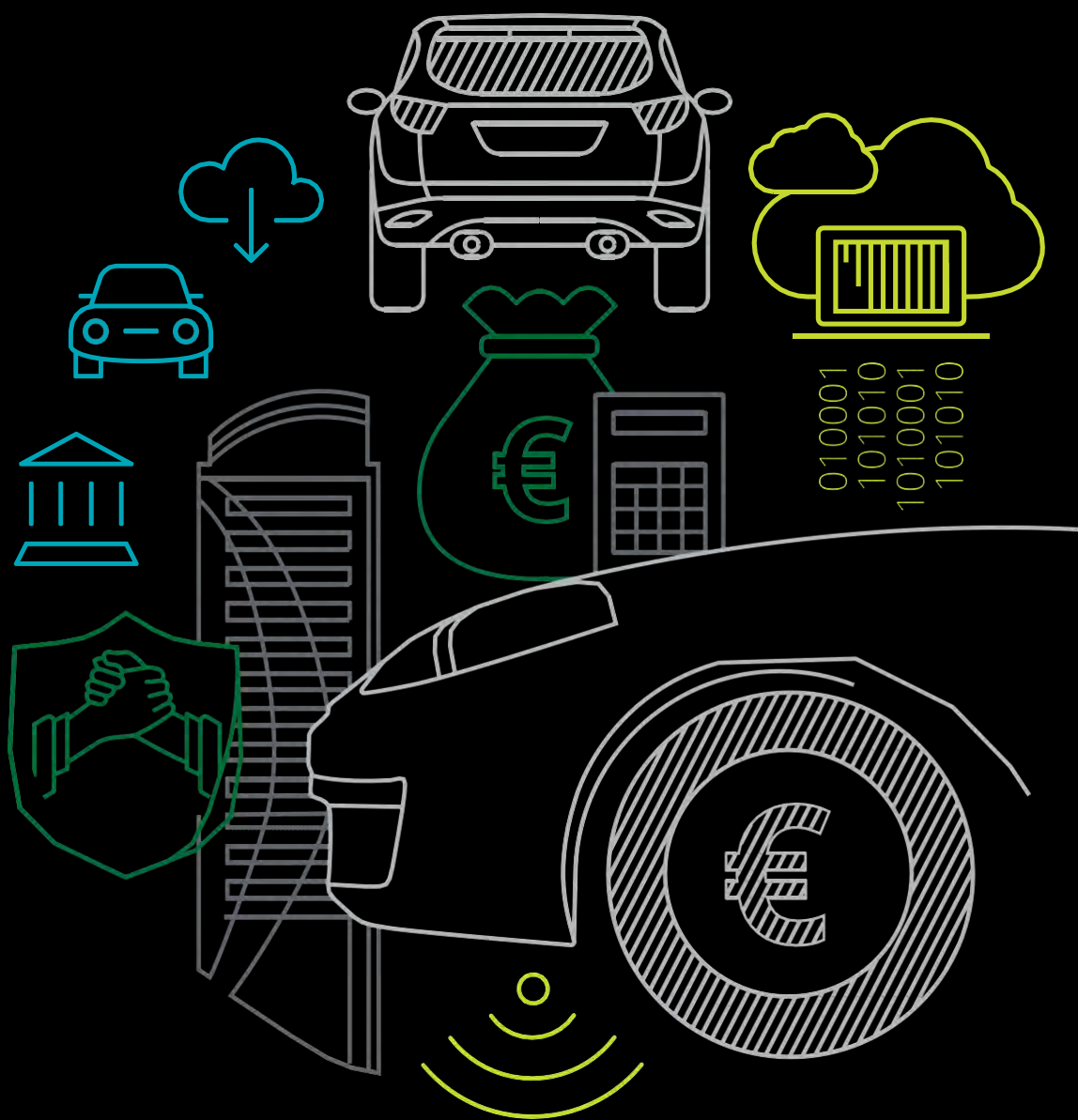
## Método para la gestión eficiente del combustible en flotas de vehículos con rutas fijas. Aplicación a una empresa de construcción



- Las herramientas de gestión del transporte no se integran con los sistemas de gestión de las empresas (ERP) para ayudar a la toma de decisiones estratégicas o tácticas. Estas herramientas permiten elaborar una amplia variedad de informes pero no explotan dichos resultados para confeccionar una lista de propuestas de actuaciones.



# **Gestión de flotas en Europa. Importancia creciente en un mundo de movilidad cambiante**

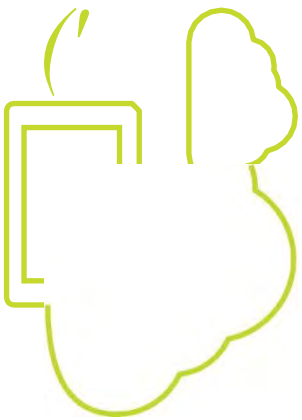
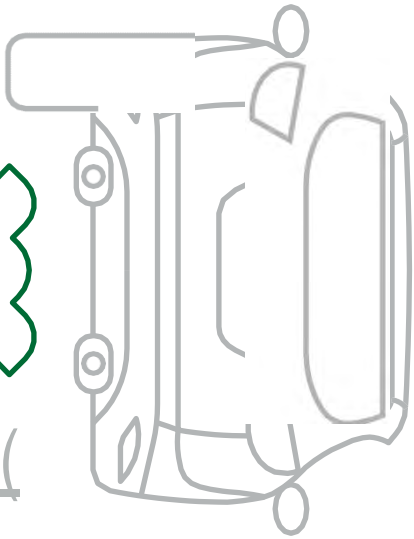
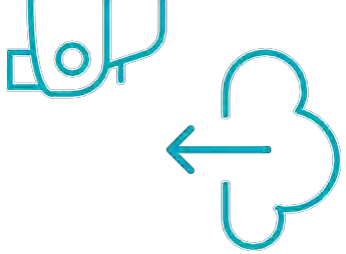


**Fleet management in Europe**  
Growing importance in a world  
of changing mobility

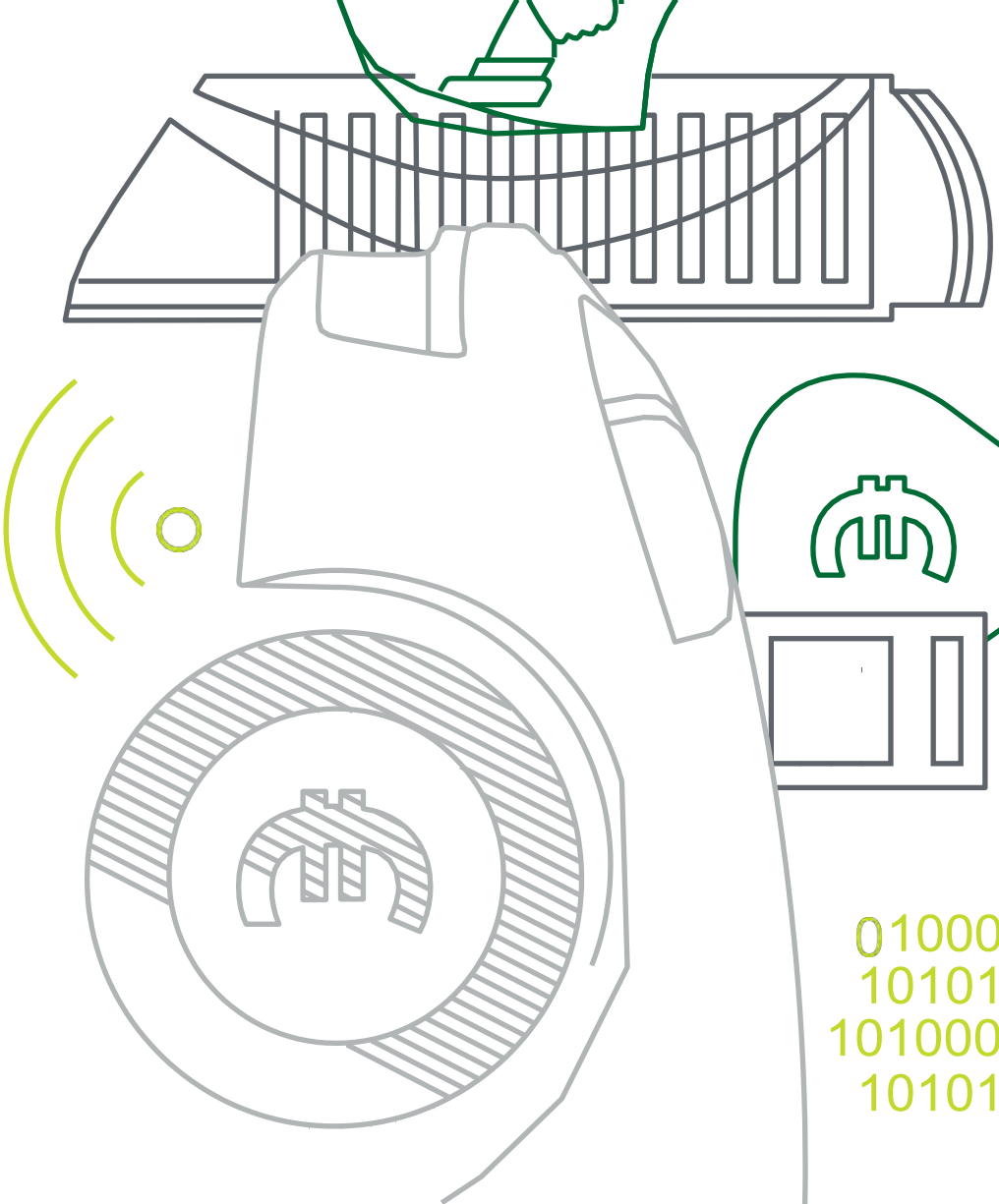
**Future** *of*  
**Mobility**



|                                                          |    |
|----------------------------------------------------------|----|
| Preface                                                  | 05 |
| Relevance of fleet management                            | 06 |
| Key players in the fleet management market               | 18 |
| Selected M&A activities of market leaders                | 24 |
| Business model analysis                                  | 30 |
| Future of Mobility and implications for fleet management | 40 |
| Strategic fields of action regarding fleet management    | 50 |
| Conclusion                                               | 52 |



010001  
101010  
1010001  
101010



# Preface

Fleet management has developed into a multi-billion-euro industry in Europe in recent years. More importantly, the fleet management business continues to grow and is gaining significant strategic importance in a world of changing mobility. Particularly when we think about two of the main trends which are most likely to substantially influence the future of the automotive industry: firstly the trend towards sharing instead of owning and secondly the trend towards self-driving vehicles. It comes as no surprise that more and more OEMs are actively pursuing opportunities in the multi-brand fleet management market.

Historically, the business was largely dominated by fleet management companies fully or partially owned by large banks. And today, several of the largest players still are. In recent years however, several OEMs have (re-)entered the multi-brand fleet management market, or substantially expanded their operations.

In this study we will explain in greater depth why the strategic relevance of fleet management will continue to grow, what the key characteristics of the business model

are, and what will be the future drivers of the corporate car market. Furthermore, the study names the key players in the industry, which main M&A activities have recently characterized consolidation in the industry, and what implications the main trends in the automotive industry with regard to the Future of Mobility will have for fleet management. Our study concludes with a summary of major strategic implications and respective fields of relevant actions required of the various players in the fleet management business.

Although fleet management is turning more and more into a global business and several of the largest players in the segment are now able to offer fleet management services globally (mostly through cooperation), we have chosen to focus this study exclusively on the European market. Europe is by far the largest market for fleet management globally and also in many regards the most advanced. Despite the fact that other fleet management markets such as North America, for example are characterized by distinct differences as compared to the European market, we believe that the major findings of our study will ultimately also have relevance on a global scale.

We hope you enjoy reading our insights and thoughts on this increasingly important segment of mobility.

**Sebastian Pfeifle**

Partner | Strategy & Operations

**Christopher Ley**

Senior Manager | Strategy & Operations

**Florian Tauschek**

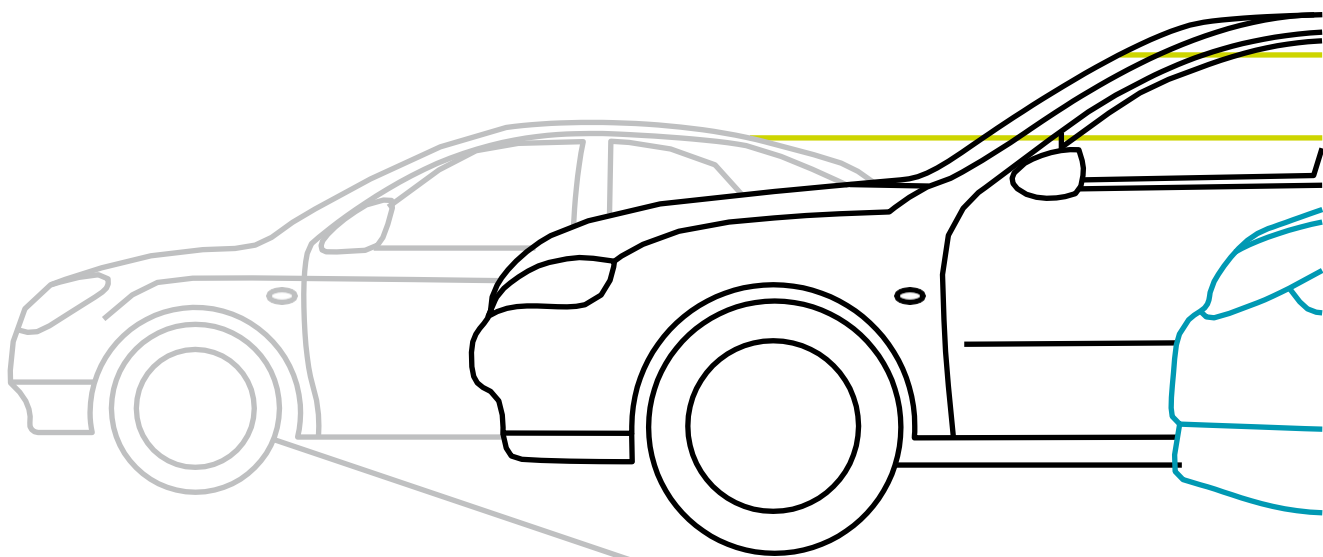
Senior Consultant | Strategy & Operations

**Philipp Enderle**

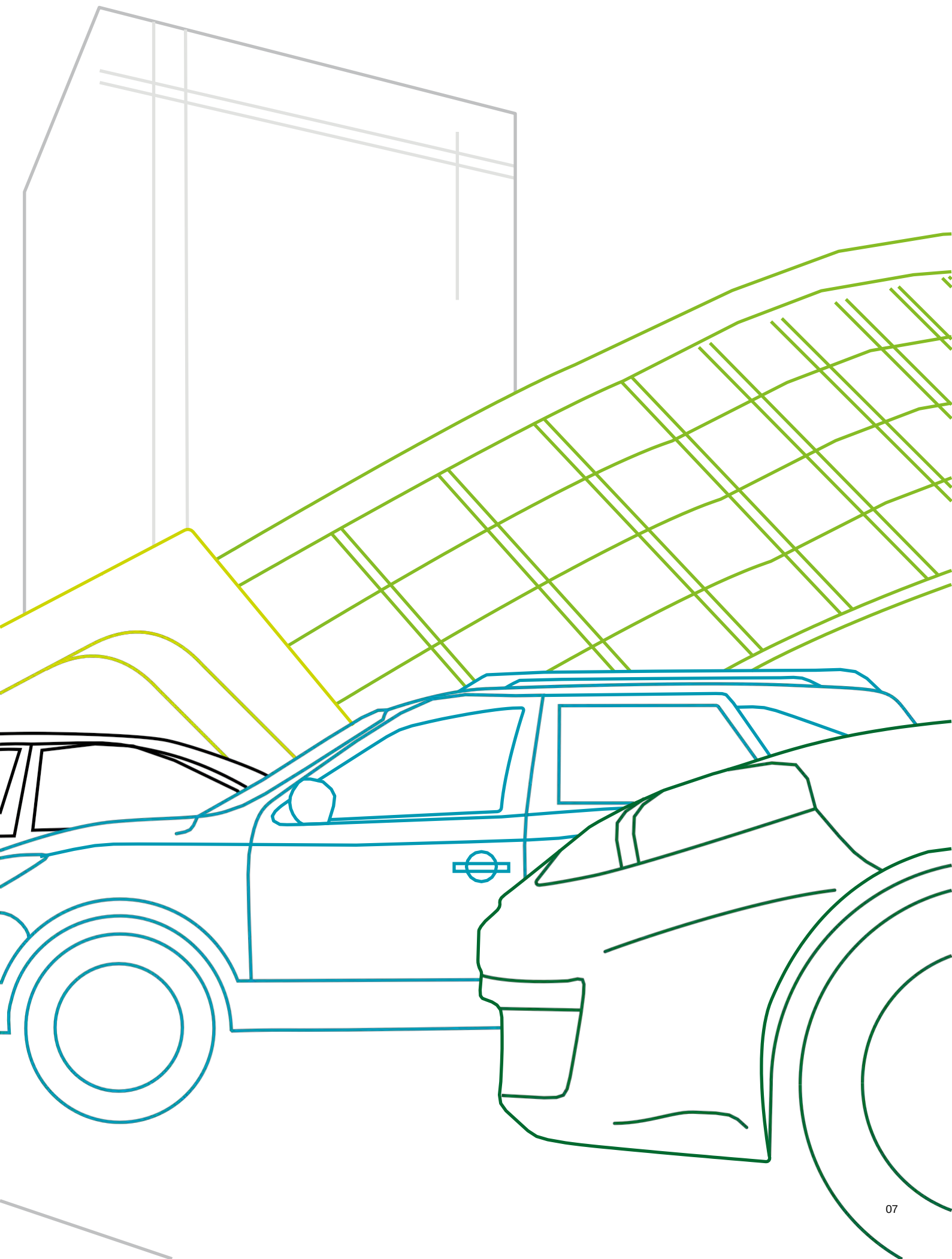
Consultant | Strategy & Operations

# Relevance of fleet management

Today, the ability to manage and operate fleets of multi-brand vehicles is a highly profitable business. Tomorrow, it will be a key capability to be successful in the Future of Mobility.







The automotive market in Europe is characterized by two major customer segments. Almost all new vehicles sales are either registered to private or to corporate customers (leaving a small number of registrations for e.g., governments). Both segments and their respective requirements have experienced continuous change in recent years.

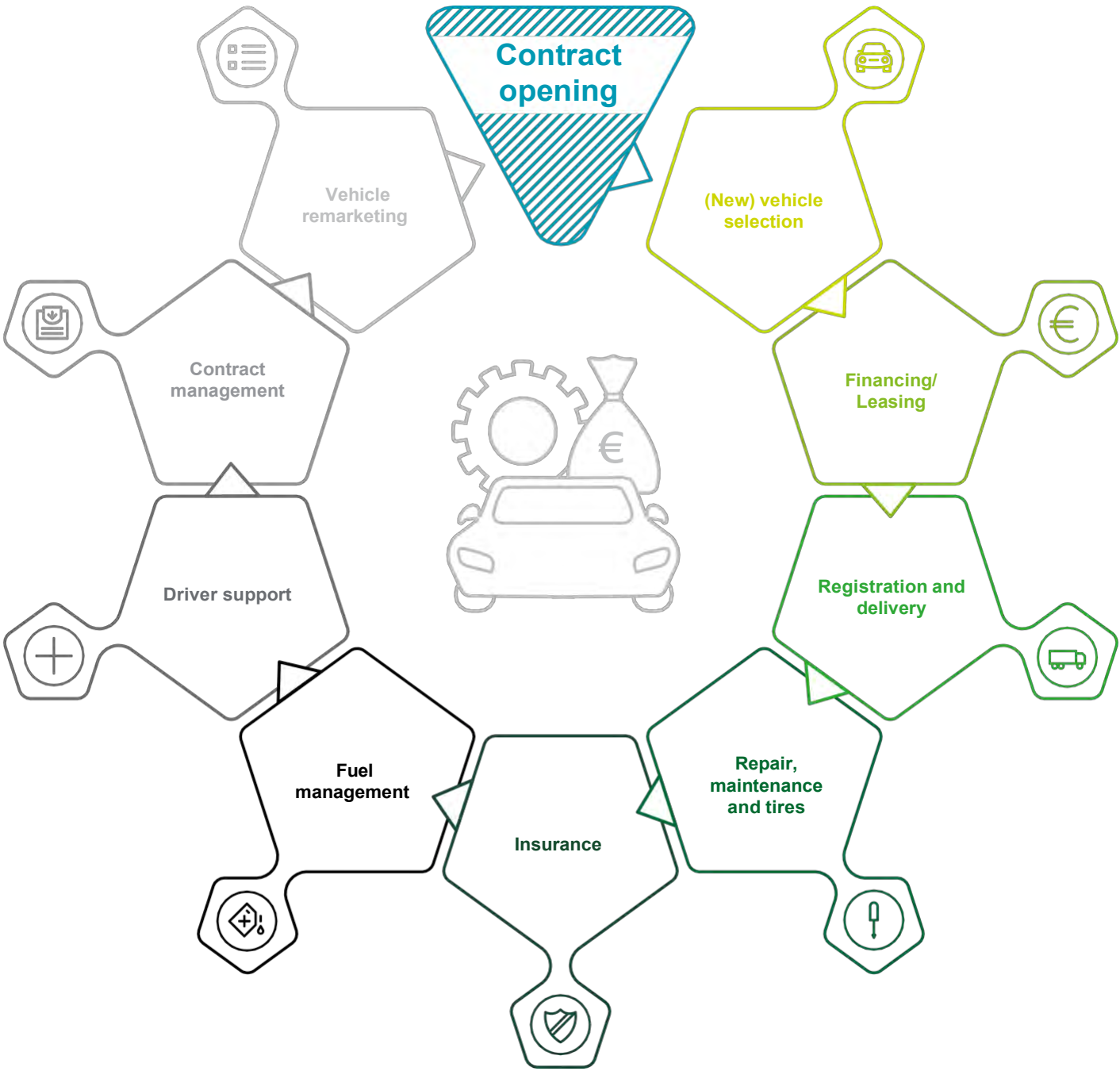
Today, nearly two out of three new cars are sold to the corporate channel. The majority of these vehicles are registered as company cars, i.e., as corporate car pools or corporate fleets and this segment is therefore called “true fleet”. Companies have vehicle fleets for various reasons, of which the most obvious is because they are needed for the business objective (e.g. service cars or sales cars). Another important factor in Europe is the high relevance of employee cars that are offered as a form of compensation (benefit in kind). This model is rather unique in a global perspective. The main motives may be found in the favorable treatment for tax purposes and also in behavioral motives (e.g., status thinking).

Historically, companies used to own their company cars and manage their fleets in-house. In recent years this has drastically changed, with more and more companies buying full-service leasing contracts instead of vehicles to reduce fixed assets and accordingly their total assets, while transferring the residual value risk of the vehicles to external parties. In addition, more and more companies outsource the management of their fleets to specialized companies with the aim of realizing further cost reductions.

A fleet management company (FMC) typically offers services over the entire life cycle of a vehicle, including purchasing, financing/leasing, and services, as well as reselling the vehicle on termination of the contract (see Figure 1).

## Typical fleet management service offerings cover the entire vehicle lifetime.

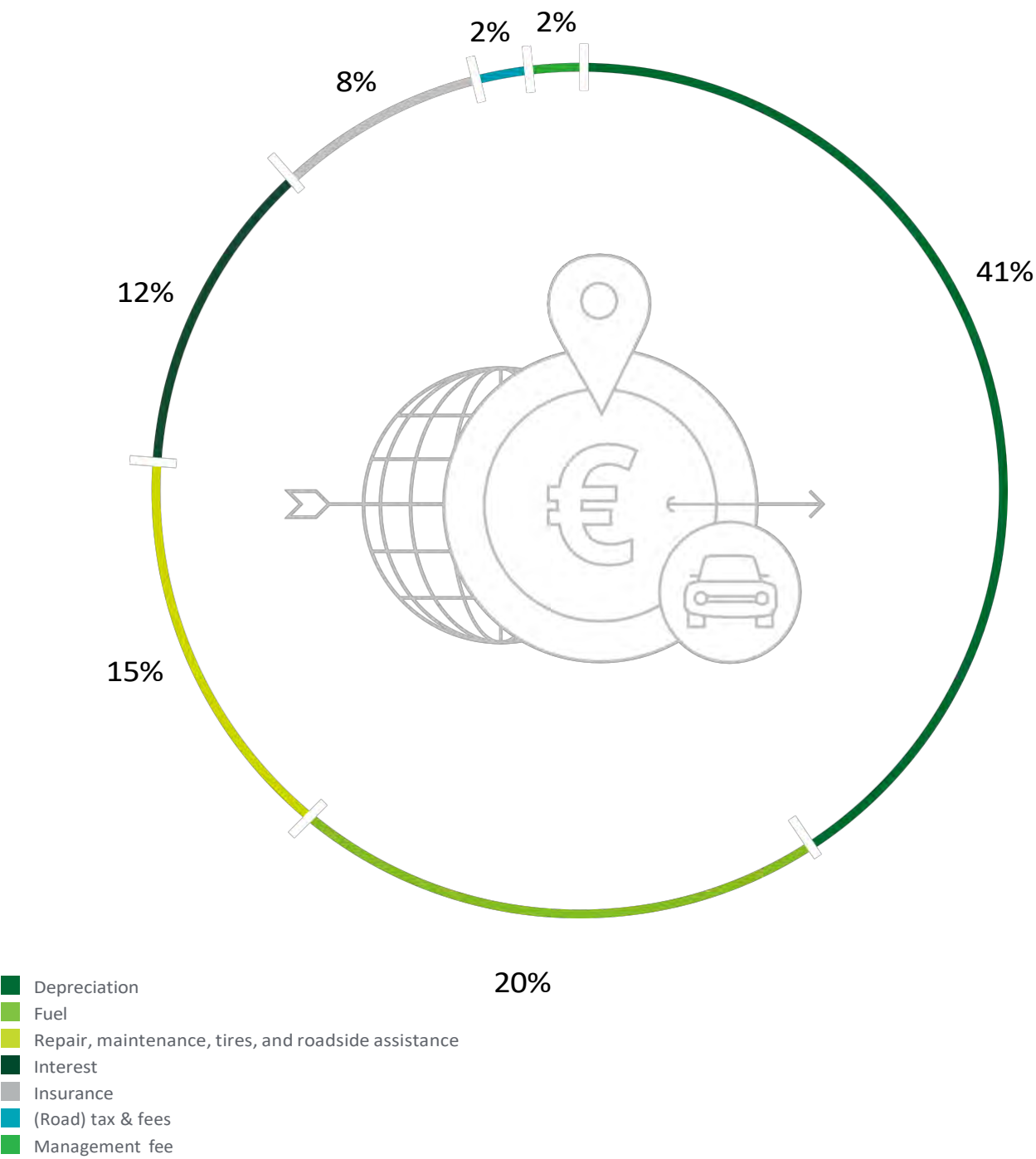
Fig. 1 – Typical fleet management service offering



Source: Deloitte analysis



Fig. 2 – Average total cost of ownership for company car in Europe



Source: Global Fleet (2015)



From a customer perspective the total cost of ownership (TCO) is the key to identifying cost saving potential and reducing operating expenses. Figure 2 shows a typical TCO split for a European fleet vehicle. Depreciation takes the largest slice over the lifetime of a company car. Fuel costs make up about 20% of the TCO while maintenance, tires, and repair management add up to an additional 15%. Interest expenses comprise 12% of total costs. The remaining costs can be attributed to additional services and management fees.

In total, only 40% of the TCO is related to the actual vehicle, 60% of the costs are incurred during the use of the vehicle itself.

Fleet management companies pursue a strategy of reducing these costs for their customers. To tackle the key cost drivers, FMCs follow different approaches. Their large purchasing volumes grant them a strong market power to negotiate high discounts with OEMs. Price reductions of 15–25% are quite standard. Profound knowledge about residual values and remarketing enables FMCs to achieve higher remarketing prices for their used cars. Part of these gains is passed on to customers, helping to reduce monthly charges and leading to a highly competitive

price environment. Furthermore, providing fuel cards can lower fuel expenses by a few percentage points. FMCs also leverage their service and maintenance network to offer better prices than authorized or OEM-affiliated repair shops, in order to reduce the TCO costs for FMC customers.

Today, more and more companies tend to analyze and optimize the total cost of mobility (TCM) rather than the TCO. While the TCO gives a cost calculation per vehicle, the TCM is calculated per mobility user (employee) and takes holistic multi-modality mobility models into account. The TCM calculation considers all costs ranging from the vehicle itself and its related costs to other mobility options such as taxis, flights, car sharing, or rental cars.

Most recent innovative products from fleet management companies focus on the TCM and offer comprehensive solutions for their customers to reduce their total cost of travel expenses and fleet-related costs rather than just TCO.

While doing so, fleet management companies are expanding their core competencies from vehicle management to total mobility management.





Europe is dominated by the corporate channel – new car sales are shifting from private to corporate.

In Europe, the corporate channel has overtaken the private channel as the most important one. While the overall number of new vehicle sales has steadily grown with only one small decline in 2013, the split between private and corporate sales has shifted in favor of the corporate channel.

Overall, the private market segment share is declining. In 2010 the private and corporate market segments were almost equally large in Western Europe (7.3 million private vs. 7.2 million corporate car registrations). Since then there has been an increasing market shift towards more corporate car registrations. In 2016 there was already a split of 6.3 million private (42% of total registrations) vs. 8.7 million corporate (58% of total registrations) registrations. This increase can be mainly explained with the economic recovery and growth of Western Europe. In addition current low interest rates permit attractive financial incentives (e.g., leasing) for companies to expand their fleets.

By 2021, Deloitte forecasts a share of new car registrations of 37% for the private and 63% for the corporate channel. With total registrations expected to exceed the 16 million mark, Deloitte expects more than 10 million new corporate car registrations in Western Europe in one year for the first time. This equals a compound annual growth rate (CAGR) of 3.5% between 2016 and 2020 or almost double the growth rate of the overall European car sales market. This further increase in corporate registrations implies an increasing number of corporate fleets and company cars which need to be managed and therefore provide a major business opportunity for fleet management companies.

Although the general market shift towards corporate is clear throughout Europe, there are strong regional differences between countries, resulting in different corporate penetration rates. The differences between the five largest European markets, Germany, France, UK, Italy and Spain are shown in Figure 4.

#### Sales to corporate channel:



##### OEM:

OEM self registrations (to employees)



##### Rental:

Rental cars (short, medium, and long-term rental)



##### True fleet:

Corporate fleets with or without full service leasing

Fig. 3 – New car registrations in Europe (EU16) in millions

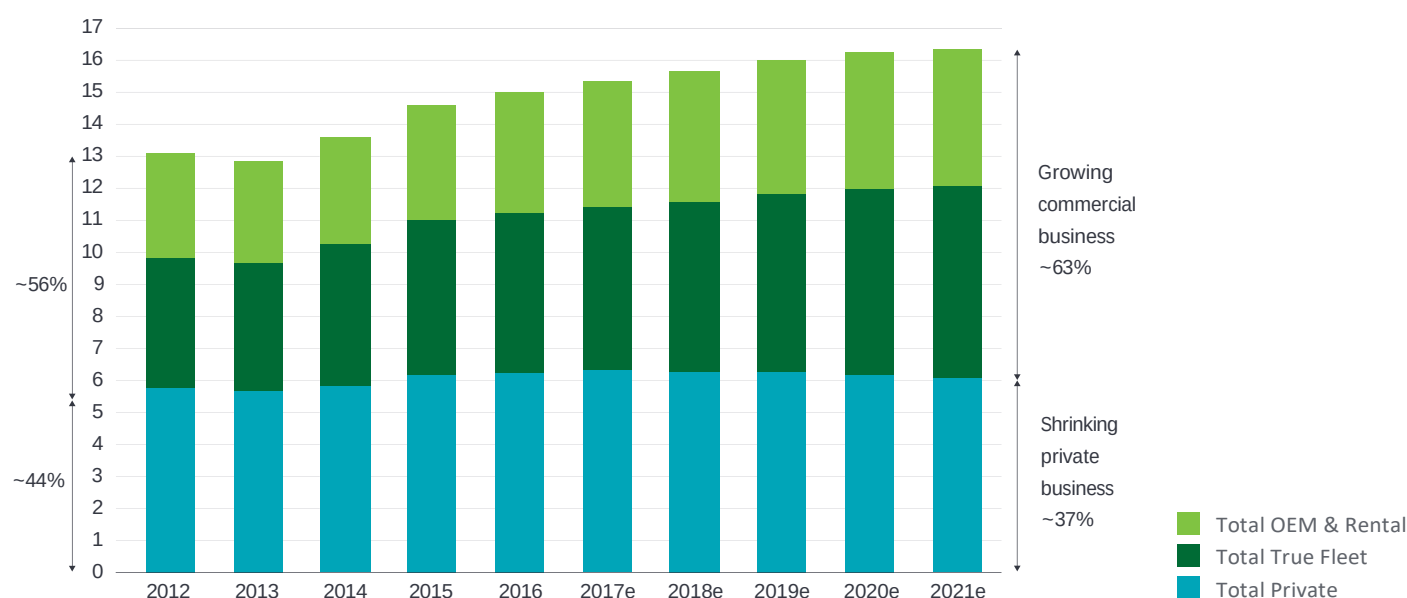
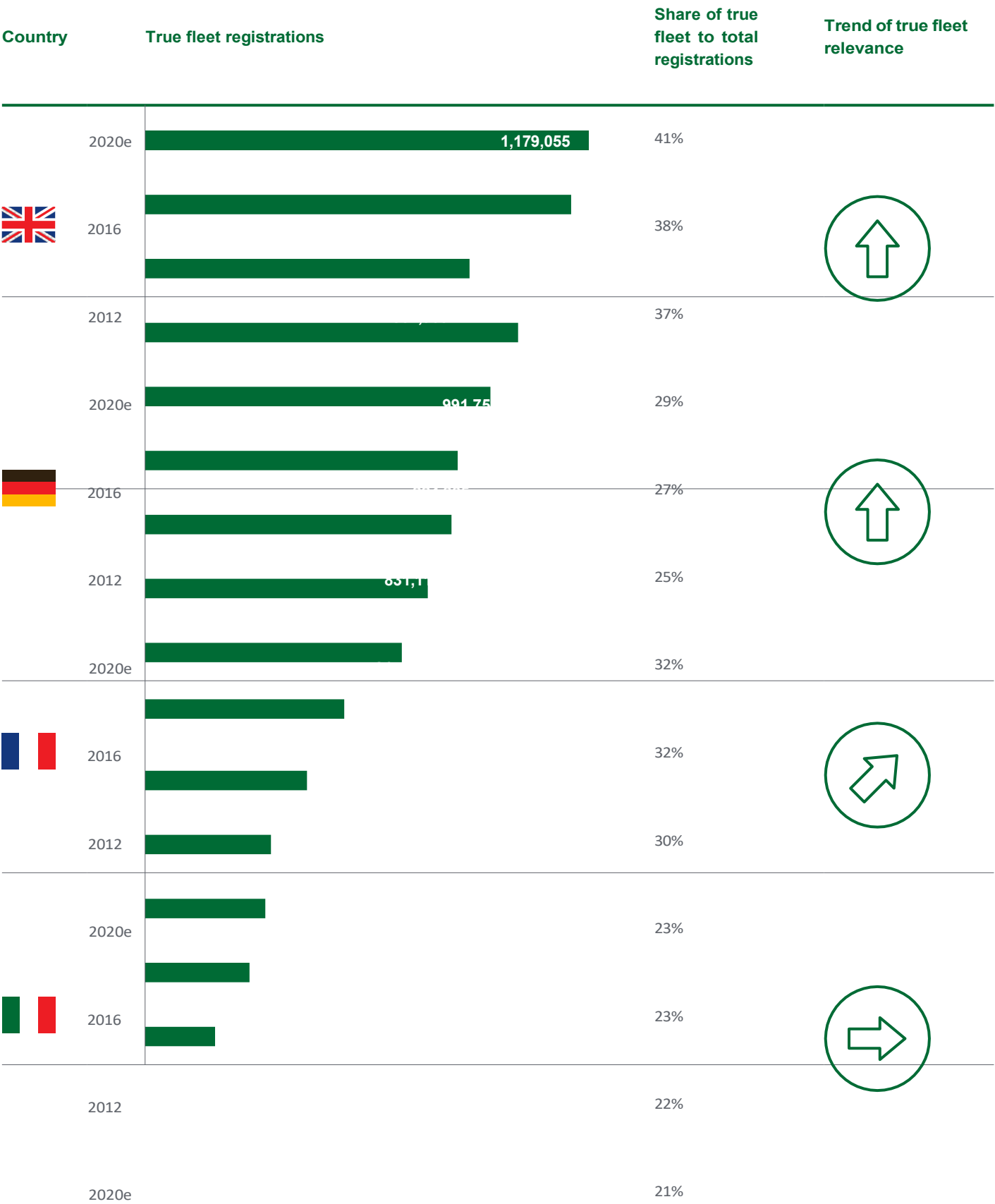


Fig. 4 – Overview of fleet management specifics in EU countries





2016

21%



2012

**183,574**

24%

Source: Deloitte analysis, Dataforce (2016), LMC (2016)

## Description

## Drivers

- Total number of new vehicle registrations is expected to increase to 2.9M by 2020
- Total corporate market segment (OEM & Rental + Fleet) is expected to increase from 59% (1.3M cars) in 2012 to 63% (1.8M cars) in 2020
- Historically leasing segment in Britain is very strong; relatively low share of OEM & rental segment

- **Growth in salary sacrifice models<sup>2</sup>**
- **Recent changes in “benefit in kinds” taxation might soften further corporate growth<sup>2,3,4</sup>**
- **Uncertainty of BREXIT negotiations might harm future growth in new car registrations**
- **Employment growth**

- Total number of new vehicle registrations in Germany expected to increase to 3.5M by 2020
- Corporate market segment expected to increase from 63% (2.1M cars) in 2012 to 69% (2.4M cars) in 2020
- Germany has a high number of short term OEM self registrations to sidestep recommended sales prices of OEMs and to give discounts to end customers

- **Economy and employment growth boosts further corporate demand**
- **High share (10–30%) of OEM self registrations<sup>5</sup>**
- **Company car as strong status symbol commonly used as extra incentive**
- **Company cars are tax beneficial under the one-percent-regulation**

- Total number of new vehicle registrations is expected to increase to 2.5M by 2020
- Corporate market segment is expected to increase from 51% (1.1M cars) in 2012 to 56% (1.4M cars) in 2020
- French market has a strong tradition of long-term rental (Location Longue Durée (LLD)) and short-term rental offerings and therefore a strong rental segment

- **Domestic market of large French full service leasing providers (Arval, ALD Automotive, PSA's “Free2Move”)**
- **Real disposable income expanding**
- **Employment growth**

- Total number of new vehicle registrations is expected to increase to 2.3M by 2020
- Only market within the Top 5 in which private market segment outweighs corporate segment
- Corporate market segment is expected to decrease from 41% (600k cars) in 2012 to 38% (900k cars) in 2020
- Italian market has a strong tradition in rental services (e.g. due to tourism)

- **Economic situation still worse than before the crisis**
- **Only gradual economic recovery**
- **Although Italy has the most companies (~4.3M) of the Top 5 markets, the majority of them (~4.1M) are below 10 FTEs and have therefore no significant company car fleets<sup>6</sup>**

- Spanish market is the smallest within EU Top 5
- Total number of new vehicle registrations is expected to increase to 1.5M by 2020
- Penetration of external fleet management services within fleet registrations is high with many small and medium-sized companies active in this segment
- Spanish market has a strong tradition in rental services (e.g. due to tourism in particular on the Spanish islands)

- **Political program (“PIVE”) to support the continued modernization of the nation's motor vehicle stock ongoing<sup>7,8</sup>**
- **Households are less wealthy than before recession**
- **Purchasing power of households is still recovering**



# Future drivers of the corporate car market

Apart from the economic, demographic, and political drivers outlined, which are mainly country-specific, Deloitte foresees two main drivers affecting the future development of the European corporate car market across Europe.

## Accounting standards

Beginning in January 2019 the International Accounting Standard Board (IASB) will require companies to disclose leased assets in their balance sheets and also to recognize liabilities for future rental payments. For company cars financed with operating leases, this is a major change. Up to now, these assets and liabilities could be kept off the balance sheet so as to disclose a low debt-to-equity ratio to enable easier access to funding. The change in accounting standards described considerable effects on corporate car markets.<sup>9</sup>

## Green

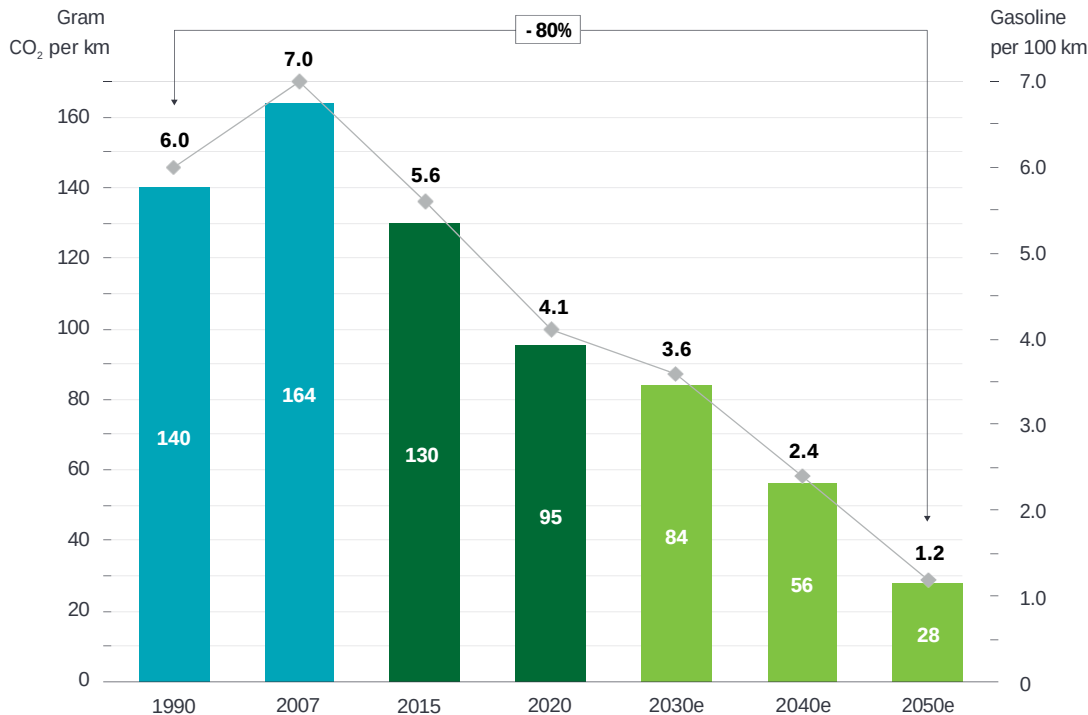
Apart from changes to accounting standards, there is a second major factor affecting the fleet market, driven by regulation. No matter which country is selected, green initiatives are ongoing everywhere, which will have a considerable impact on future corporate fleets.

The European Union came to an agreement to reduce the overall CO<sub>2</sub> emissions by 80% up to 2050, compared to the base year of 1990. To achieve this ambitious goal, the EU Commission defines, besides many other rules, also binding limit values for the CO<sub>2</sub> emissions of new cars. Currently they are set at 95 grams/ CO<sub>2</sub> per kilometer by 2020. A limit which Deloitte expects to decrease to ~84 grams/ CO<sub>2</sub> per kilometer by 2030 and ~56 grams/ CO<sub>2</sub> per kilometer by 2040.<sup>10</sup>

Furthermore, in September 2017 the new Worldwide Harmonized Light Duty Vehicles Test Procedure (WLTP) will be introduced.<sup>11,12</sup> This new testing regime was jointly developed by experts of the EU, Japan, and India to provide a more realistic picture of real vehicle emission and fuel consumption.

Vehicles which do not comply with the defined limits will be affected by driving bans and higher taxes. As a result Deloitte expects the share of low emission vehicles in corporate fleets to increase sharply within the next years.

The trend towards green is a ticking time bomb for FMCs and captives. For these companies it will be more and more complicated to find enough customers for used diesel-engined cars when their lease contracts expire – sending their residual values on a downward slide.

**Fig. 5 – Expected future development of CO<sub>2</sub> emission limits in Europe**Source: Deloitte analysis<sup>10,13</sup>

## Deep dive – Regional Regulatory Impacts

### United Kingdom:

Salary sacrifice is a strong driver for company cars/ fleet sales due to relatively high tax incentives. The UK is discussing the adjustment of Benefit in Kind (BIK) taxation, based on the new WLTP, threatening company car drivers with an increase of up to 30% in BIK. Deloitte expects that around 50% of the 970k British employees paying BIK on their car will be affected by these planned changes. The significance of this change for the whole corporate car sector in UK becomes obvious if this number is put into perspective with the total corporate registrations of 1.7M in 2016.

Only ultra-low emission vehicles with emissions <75grams CO<sub>2</sub> per km will be excluded from these changes and will

continue to enjoy the benefit of reduced taxation. Deloitte therefore expects a sharp increase in hybrid and battery-electric vehicles in UK's corporate fleets.<sup>14,15</sup>

### Germany:

Many German cities are currently discussing driving bans for certain inner-city areas for vehicles not meeting the latest Euro 6 emission standards, so as to achieve CO<sub>2</sub> and NOX emission standards defined by the EU. The city of Stuttgart recently went ahead and decided to put such a ban in place starting in January 2018. Only diesel vehicles meeting Euro 6 standards (with the exception of delivery vehicles and certain craftsmen) will be allowed to enter the city center. This ban affects ~68% (or 73k) of all registered diesel ve-

hicles in Stuttgart.<sup>16</sup> At the beginning of May the city of Hamburg also introduced bans for two main roads in the center.<sup>17</sup>

If other cities follow the role models of Stuttgart and Hamburg, this will have enormous consequences the German corporate vehicle park – currently ~80% of it is running on diesel. Shares of PHEVs and hybrids as well as BEVs are expected to rise significantly in Germany too.<sup>18</sup>

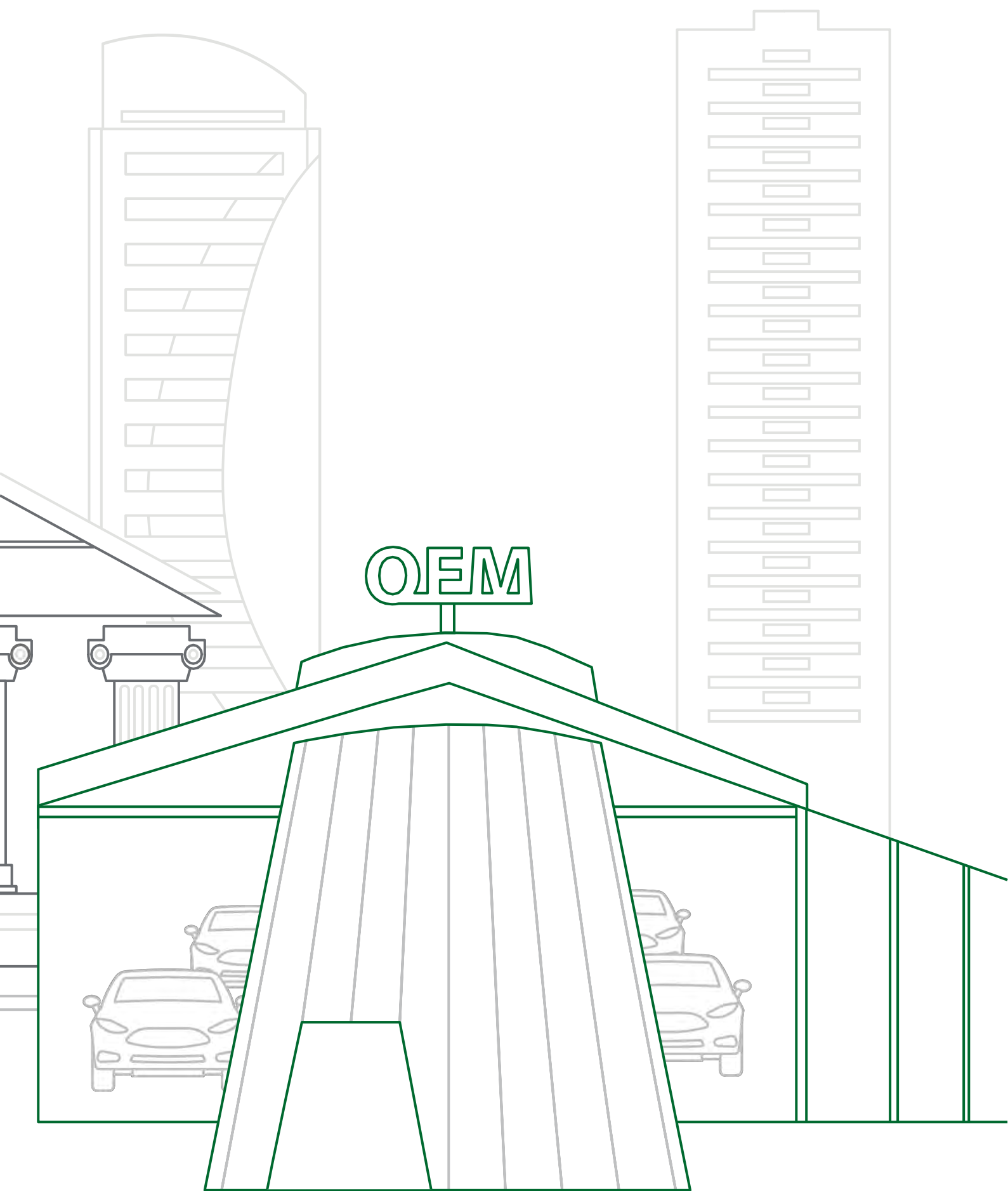




# Key players in the fleet management market

Fleet management has historically been dominated by banks, with OEMs now entering the market.





Historically, fleet management companies in Europe grew out of the banking industry. Banks identified vehicle leasing as an asset-based business model with profitable interest margins, the potential for additional recurring service revenue, and manageable risk. In addition to banks, some OEMs grew naturally into fleet management, evolving from retail leasing contracts to managing and financing large corporate fleets leveraging the financial power of their captives.

Leading European bank-backed fleet management companies are Arval (owned by BNP Paribas Group) and ALD Automotive (owned by Société Générale). Leading captive related multi-brand FMCs are Alphabet (BMW FS) and Athlon (Daimler FS) and most recently PSA's "Free2Move". Volkswagen Leasing (VWFS) is a major player in that field but is, despite having recently acquired CarMobility!, currently rather focused on its own group brands and is therefore not analyzed in further detail in this study.

The structure of many fleet management companies has changed in recent years. The European market leader LeasePlan, for example, was founded as a subsidiary of ABN Amro banking group but later became owned in an equal joint venture between the German Metzler Bank and the Volkswagen Group. In 2016, the previous owners sold LeasePlan to a consortium of institutional investors led by a Dutch pension fund.<sup>19</sup>

In a highly consolidating market today, the Top 5 players in Europe own more than 50% of the market. Figure 6 compares the key players in Europe.

Fig. 6 – Top 5 fleet management companies in Europe



|                       | Units in operation<br>(as of 2016)                        | HQ                         | Shareholder                                                  | Recent transactions                                                           |
|-----------------------|-----------------------------------------------------------|----------------------------|--------------------------------------------------------------|-------------------------------------------------------------------------------|
| <b>LeasePlan</b>      | >1,600,000<br>(~70% in EU)                                | Amsterdam,<br>Netherlands  | LP Group B.V.,<br>consortium of institu-<br>tional investors | LP Group BV's<br>acquisition of<br>LeasePlan Corp NV for<br>€3.7 billion      |
| <b>ALD Automotive</b> | >1,400,000<br>(~90% in EU)                                | Clichy,<br>France          | 100% subsidiary of<br>Société Générale<br>Group              | May 2016, ALD<br>Automotive acquired<br>Parcours SAS for € 300<br>million     |
| <b>Arval</b>          | >1,000,000<br>(>3 million with global<br>partner Element) | Rueil-Malmaison,<br>France | 100% subsidiary of<br>BNP Paribas Group                      | June 2015, Arval<br>acquired General<br>Electric's European<br>fleet business |



|                 | Units in operation<br>(as of 2016) | HQ                           | Shareholder                                            | Recent Transactions                                                                                    |
|-----------------|------------------------------------|------------------------------|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| <b>Alphabet</b> | >650,000<br>(~90% in EU)           | Unterschleißheim,<br>Germany | 100% subsidiary of<br>BMW Group                        | September 2011, Alpha-<br>bet acquired ING Car<br>Lease, a subsidiary of ING<br>Group for €637 million |
| <b>Athlon</b>   | >340,000<br>(all EU)               | Machelen,<br>Belgium         | 100% subsidiary of<br>Daimler Financial<br>Services AG | July 2016, Daimler FS<br>acquired Athlon for<br>€1.1 billion                                           |

Source: Deloitte Analysis, mergermarket.com, Annual Reports, Company Websites

# Strong consolidation in last years led to 5 major players having >50% market share

## **Market is consolidating**

In the past 15 years a strong consolidation has started within the European fleet market which is still ongoing. More than 50 acquisitions formed a concentrated market where the Top 5 companies own more than 50% of the total European market.

Three main reasons in particular are driving this trend:

## **Cross-border service offering matters**

The main reason for the consolidation process can be seen in the companies' growth strategies. Multinational customers demand a pan-European service coverage to serve their European subsidiaries and employees with a seamless service level even across borders. Strong competition to become the European leader in fleet management started a race which can hardly be won by pure organic growth. The acquisition of existing companies and their fleets became a lever to quickly increase portfolio size, product offering and geographic coverage.

## **Economies of scale**

Secondly, scaling effects can be seen. FMCs identified size as a prerequisite to benefiting from economies of scale and to reducing their operating costs per contract. In addition, high volumes lead to strong purchasing power over suppliers (such as OEMs and fuel providers).

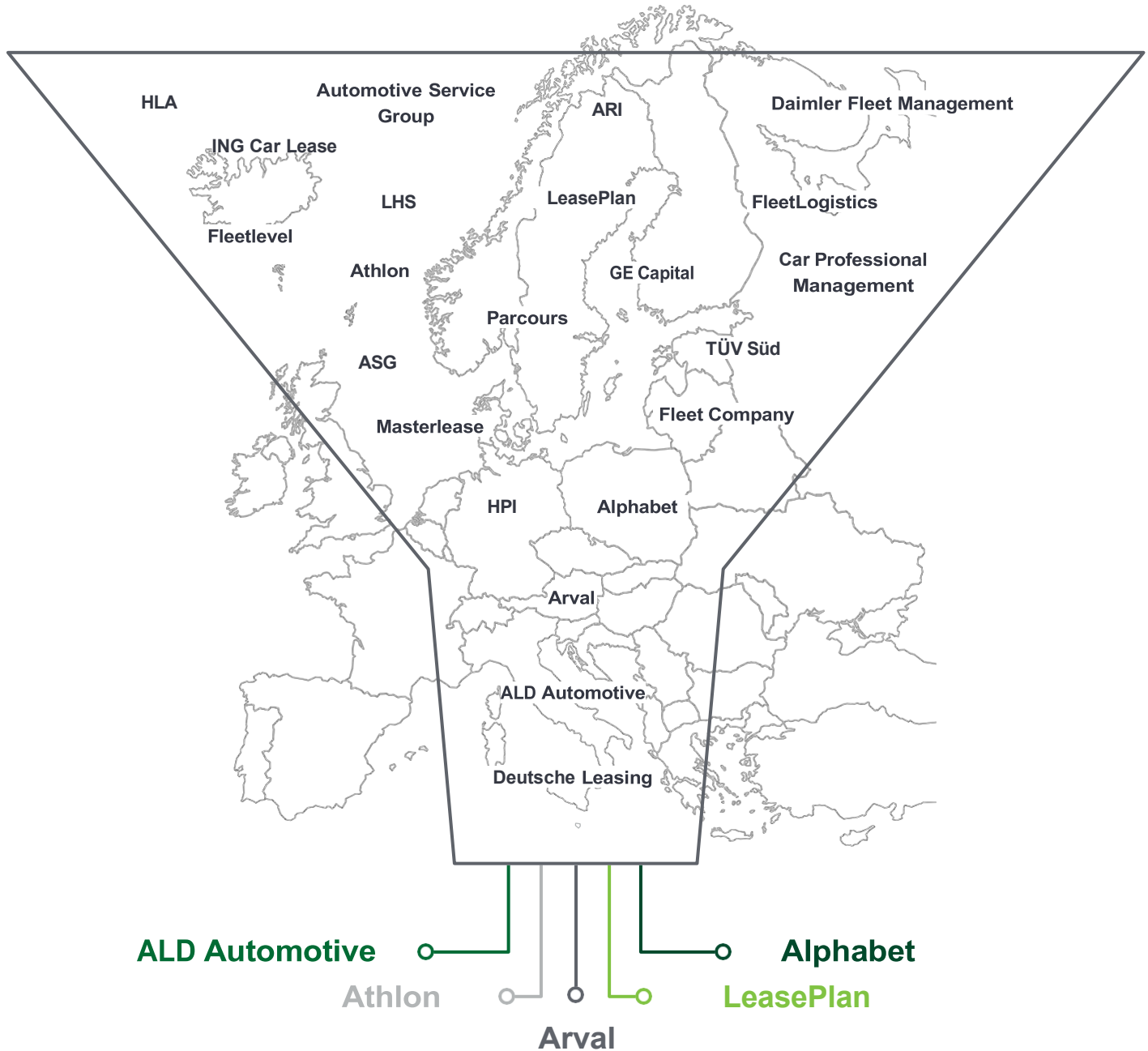
## **Investment case**

Banks and private equity funds appreciated the high profit margins and relatively low risks of fleet management business and started to acquire FMCs as strategic investment cases in times of low interest rates.

## **Ongoing consolidation**

As a result the independent medium-sized pan-European players like Athlon or Parcoures have all been acquired and this sub-segment has effectively vanished. The European FMC market today can be separated into a group of five large pan-European providers and a large number of fragmented domestic companies rarely having more than 30,000 cars under management.

Fig. 7 – Strong consolidation in European fleet management market



>50% of total European fleet market  
managed by Top 5 players



# Selected M&A activities of market leaders

Driven by the three factors outlined all large fleet management providers have conducted significant M&A deals in Europe during the last decade.

Whereas the motivation of the captive-backed FMCs was mainly to leapfrog a long period of organic growth by instantly acquiring a large portfolio, the independent providers selectively bought companies across Europe to increase their size and geographic coverage in the respective markets.

These ongoing M&A activities and the decreasing availability of suitable targets resulted in an sharp increase in respective transaction prices. The average price paid per contract has doubled during the last decade.

This price increase becomes very obvious when comparing the recent acquisitions made by OEM-affiliated FMCs. Although

Daimler Financial Services acquired a similar portfolio size as Alphabet did five years earlier, the price per contract was approximately 50% higher. Alphabet paid roughly € 2,917 per contract whereas Daimler had to pay approximately € 4,400 per contract.\*

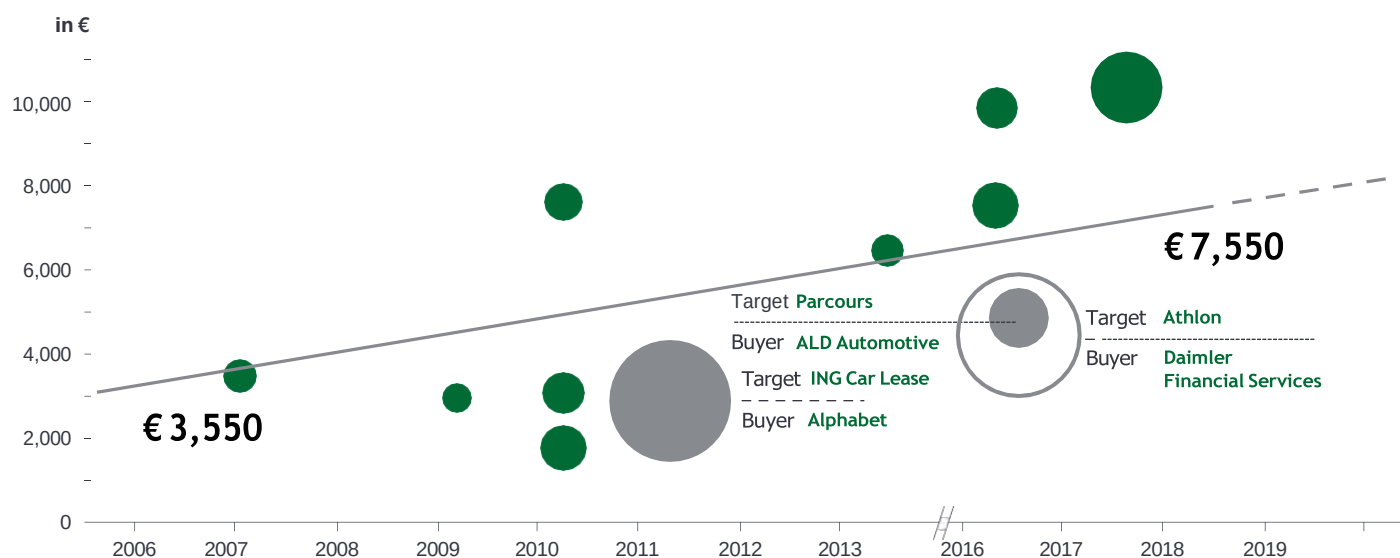
Another example is the case of LeasePlan. Volkswagen acquired LeasePlan jointly with other investors in 2004. VW paid approximately € 1 billion for its 50% share. In 2015 VW and Bankhaus Metzler sold off LeasePlan to LP Group B.V. for a total of € 3.7 billion. VW is expected to have received up to € 2.2 billion or nearly double the amount that the group paid for its stake roughly ten years earlier.<sup>19</sup>

Most recent examples show that this trend is continuing. In early 2017, Zenith was bought by Bridgepoint Advisers Ltd. for roughly € 10,300 per contract.<sup>19</sup>

Fig. 8 – Selected transactions of Top 5 players in recent years

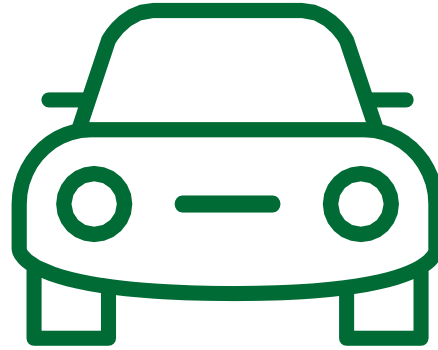
|                      | 2011                 | 2015                               | 2016                              | 2016                  |
|----------------------|----------------------|------------------------------------|-----------------------------------|-----------------------|
| <b>Target</b>        | <b>ING Car Lease</b> | <b>GE Capital Fleet Service</b>    | <b>Athlon</b>                     | <b>Parcours</b>       |
| <b>Buyer</b>         | <b>Alphabet</b>      | <b>Arval<br/>BNP Paribas Group</b> | <b>Daimler Financial Services</b> | <b>ALD Automotive</b> |
| <b>Vehicles</b>      | 240,000              | 164,000                            | 250,000                           | 61,500                |
| <b>Price</b>         | ~ € 700M             | n/a                                | ~ € 1.1B                          | ~ € 300M              |
| <b>Ø per vehicle</b> | € 2,917              | n/a                                | € 4,400                           | € 4,878               |

Fig. 9 – Average amount paid per vehicle based on historical transactions



Size of bubble represents the volume of vehicles (UiO) involved in the transaction

Source: Deloitte analysis, mergermarket.com



## Case Study: The acquisition of ING Car Lease to increase Alphabet pays off for BMW

In particular the acquisition of ING Car Lease's 240,000 cars has raised Alphabet to a significant sales channel for BMW in Europe with a fleet size of approximately 630,000 of the global fleet of 690,000 cars being under management in Europe.<sup>20</sup> The following case study is based on Deloitte estimations derived from publicly available information and shows the relevance of Alphabet for the BMW Group as a sales channel:

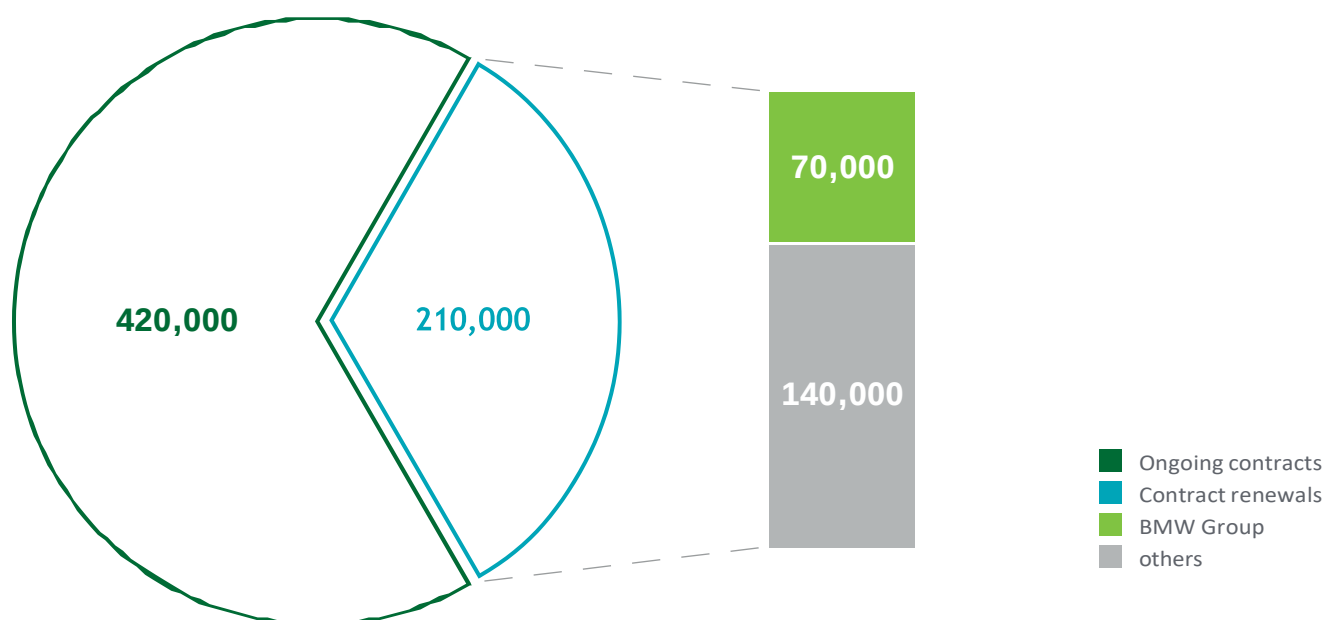
Based on an average expected leasing contract duration of three years and a share of BMW Group cars of around one-third in Alphabet's fleet results in annual renewals of roughly 70,000 BMW and Mini vehicles by Alphabet customers. This implies that Alphabet contributed to approximately 6.4% total of 1,092,000 BMW Group sales in Europe in 2016.<sup>20</sup>

Apart from pure per unit sales, Alphabet has two additional positive effects on BMW:

- Possibility of converting existing non-BMW contracts into future BMW sales after current contract expires
- Challenge other OEMs by firstly demanding significant discounts (skimming their sales margin) for multi-brand cars and secondly routing these vehicles around the after sales network of other competitors (skimming their after sales margin)

# Strong benefits for the core business of the acquirer

Fig. 10 – Alphabet's relevance as a sales channel for BMW<sup>20</sup>



Source: Deloitte analysis, BMW (2017): Annual report 2016<sup>20</sup>



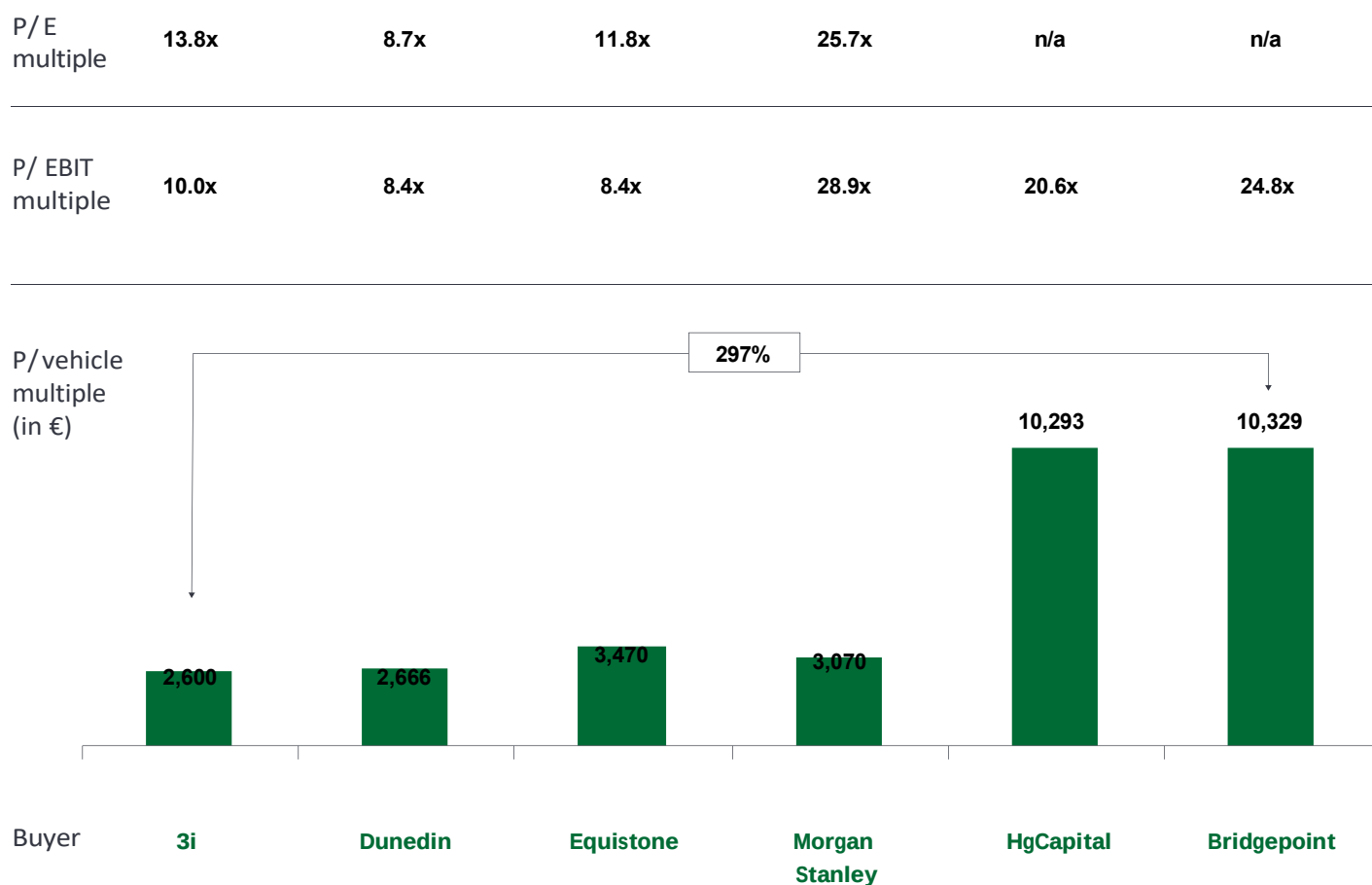
## Case Study: Zenith Group Holdings Ltd – object of speculation similar to the real estate market

Established in 1989, Zenith is one of the UK's largest independent leasing and fleet management companies. During the last 14 years it was sold seven times between various well-known private equity funds. During this time Zenith's portfolio increased from 10,000 to 85,000 units in operation. Meanwhile, its valuation increased from € 26M in 2003 to € 878 million in 2017.

Zenith is working in a cooperation with Santander to optimize its refinancing and access Santander's customer base.

The Zenith case proves fleet management companies to be a solid investment case for banks and private equity funds searching for opportunities with high profitability and moderate risk in an environment of low interest rates.

**Fig. 11 – Development of the valuation of Zenith Group Holdings Ltd**



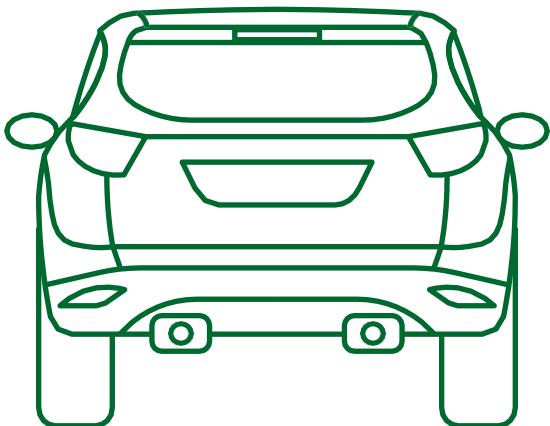
Source: Deloitte analysis, Zenith Group Holdings Ltd press releases



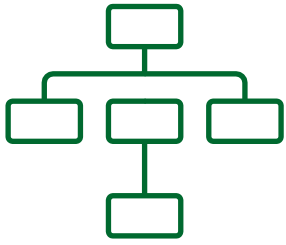
# Business model analysis

Fleet management has become a service business – funding and efficiency are key factors.

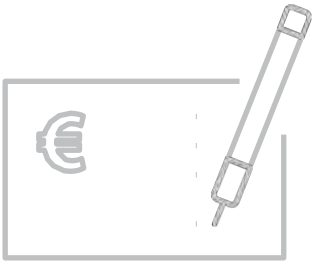
Finance







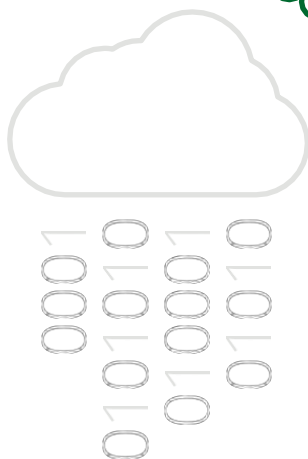
# Remarketing



## Insurance



# Service



## Purchase

Figure 12 (below) illustrates the typical main components of the value chain of a fleet management company and the corresponding profit allocation.

Today, the core profit driver of an FMC remains financing the assets. Funding and leasing alone contribute about 30–35% to the total profit.

Forecasting the right residual value of the vehicle at the end of its contract is the most crucial capability for determining monthly payments but also to enable profit creation when remarketing the vehicle at the end of the contract.

Apart from financing, vehicle remarketing is the second largest profit contributor. About 20% of total profits are connected to the used car remarketing process. On the one hand, remarketing profits are realized if the used car is sold for a higher price than the original forecast residual value. On the other, FMCs tend to charge their customers a variety of penalty fees, e.g., for small damages or for exceeding the original contracted mileage of the fleet car.

Purchasing plays a significant role in an FMC's business. FMCs' high order quantities usually correspond with a strong purchasing power which allows them to

demand major discounts from OEMs which are often between 15–25%. While the majority of these discounts are passed on the clients to offer competitive monthly rates, the remaining discounts are counted as revenue for the FMCs.

Services account for roughly 50% of the total profit of an FMC. This profit is usually split across multiple services. Often FMCs outsource at least some of their offered services to specialized third parties (Figure 13 provides an overview of the typical service portfolio of an FMC). In this case FMCs charge a handling fee on these services while managing the customer contact.

**Fig. 12 – Fleet management profit allocation along the value chain**

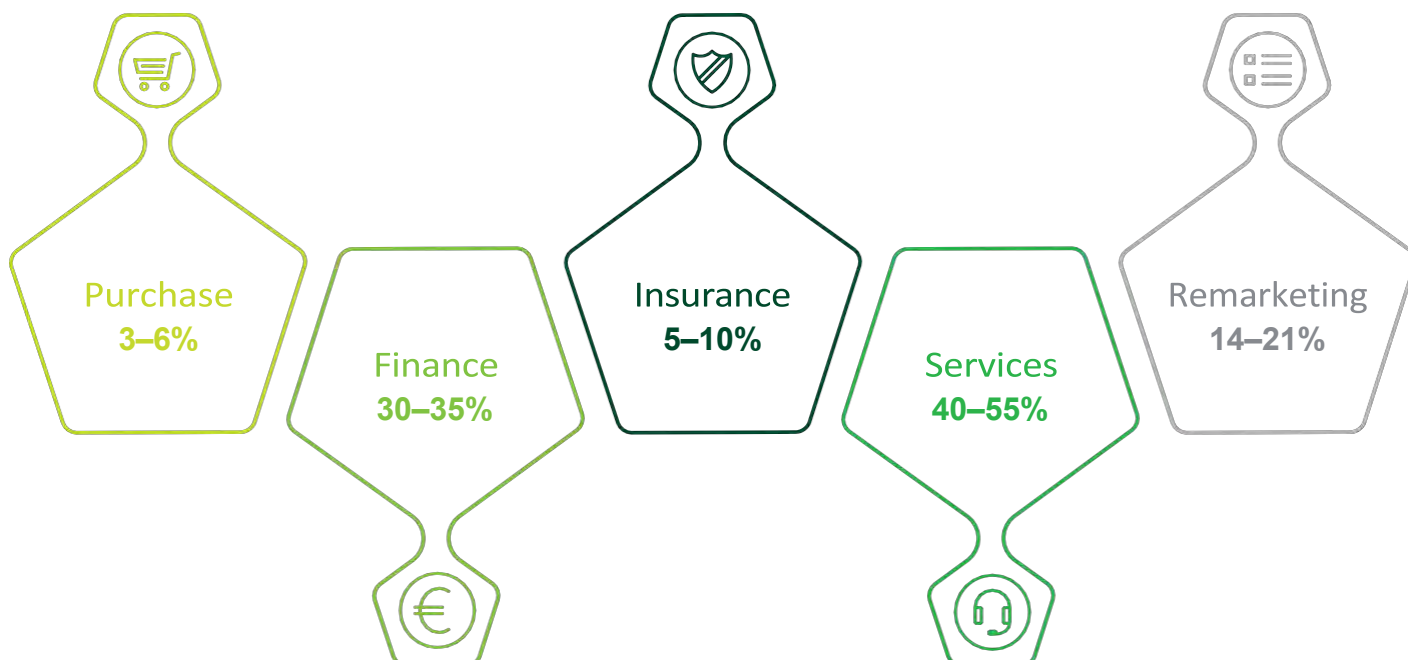


Fig. 13 – At least 10 core services are typically offered by top fleet management companies



#### Licensing, Title & Registration

Management of the increasingly complex registration process



#### Tolls & Violation Management

Reducing administrative tasks while ensuring compliance



#### Risk & Safety

Driver training programs, motor vehicle record checks, driver risk profiles



#### Fuel Management

Fuel cards with discounts and systematic detection of abuse



#### Tire Management

Winter & summer tire change, storage of the second set during other season



#### Telematics

Manage fleet efficiency, increase driver productivity, lower operating costs



#### Maintenance Management

Network of shops, certified technical advisors, 24/7 service



#### Interim Car Management

Providing a replacement car in case of accident or maintenance



#### Personal Usage Management

Track personal mileage online, real-time reporting, compliance with IRS

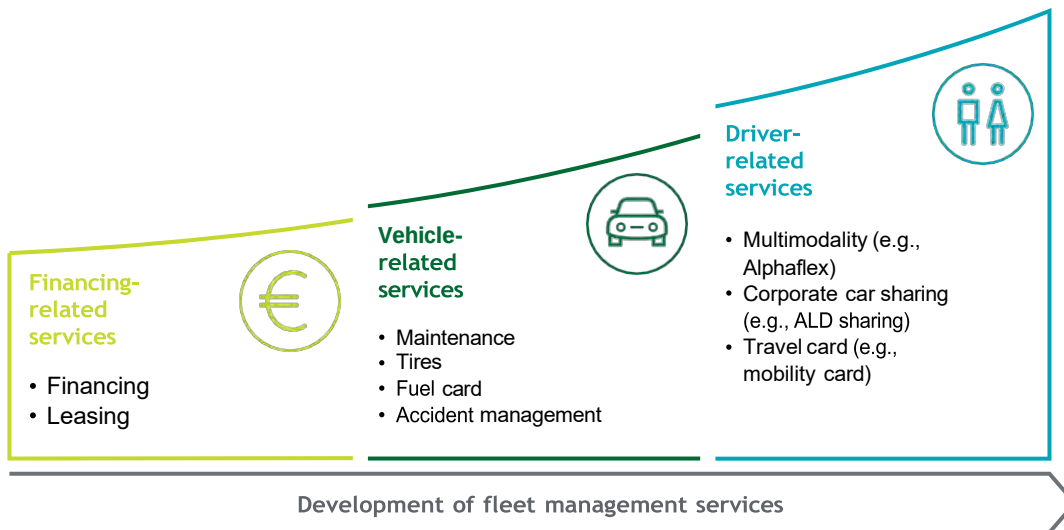


#### Accident Management

Repair shop assignments, provide subrogation services, documentation



**Fig. 14 – Development of fleet management services towards driver-related services**



Source: Deloitte analysis

FMCs will evolve into providers of multimodal mobility for their customers. Their heritage, the fleet vehicle, will just be one part of the future customer's daily mobility journey.

#### Development of services

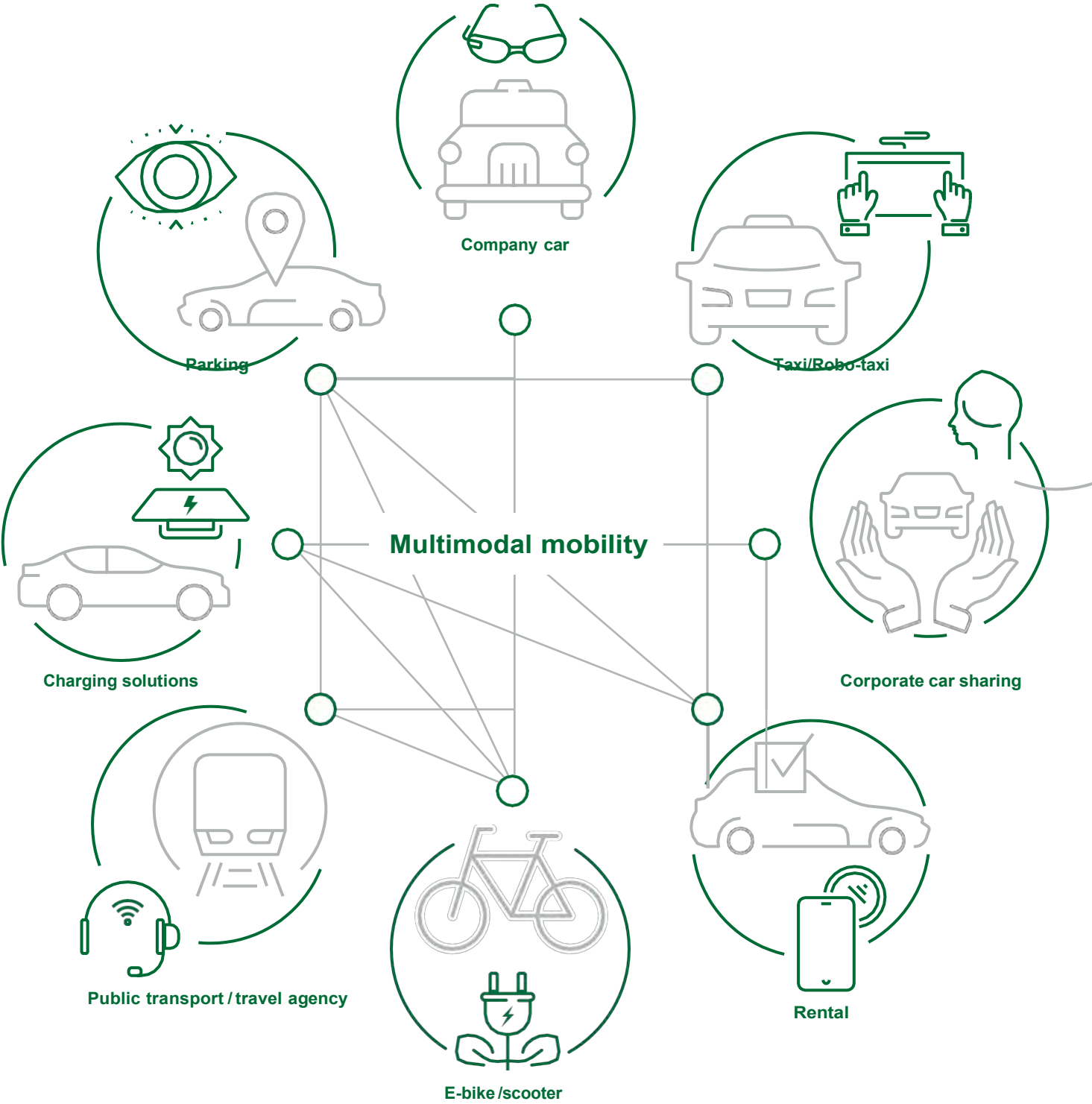
Historically, FMCs' service and product offering focused on financing and vehicle-related offerings such as leasing, repair & maintenance, or tire management.

Today, FMCs have already expanded their offering to driver-related services, e.g., fee management or personal usage management. Innovative products such as corporate car sharing are on the rise, focusing on the needs of the driver (employee).

As the next step, Deloitte foresees the expansion of FMCs also into the area of in-vehicle-related services (for instance in vehicle multimedia offerings such as Netflix or Spotify flat rates) as well as non-vehicle-related mobility services (e.g., travel agency). FMCs will evolve into providers of multimodal mobility for their customers. Their heritage, the fleet vehicle, will just be one part of the future customer's daily mobility journey.



Fig. 15 – Multimodal mobility offers the future customer seamless mobility



Source: Deloitte analysis





Fig. 16 – Financial comparison of leading European fleet management companies based on publicly available information

| KPI          | Non-Captive                |                  |                   | Captive  |                  |
|--------------|----------------------------|------------------|-------------------|----------|------------------|
| Top 5 player | Arval<br>BNP Paribas Group | LeasePlan        | ALD<br>Automotive | Alphabet | Athlon           |
| Revenue      | n/a                        | € 9.2B<br>(2016) | € 7.5B<br>(2016)  | n/a      | € 1.6B<br>(2015) |
| Profit       | € 361M<br>(2015)           | € 455M<br>(2016) | € 512M<br>(2016)  | n/a      | € 135M<br>(2015) |
| RoE          | 25%<br>(2015)              | 14.9%<br>(2016)  | 17.2%<br>(2016)   | n/a      | n/a              |
| RoA          | 2.7%<br>(2015)             | 1.9%<br>(2016)   | 3.8%<br>(2016)    | n/a      | n/a              |

Source: Deloitte analysis, annual reports, company websites



## Fleet management – most profitable business unit for Société Générale

An analysis of profitability measured by return on equity (ROE) of the individual business units of Société Générale – France's second largest bank – underlines the profitability of fleet management.

With its fleet management business unit ALD, the bank generates approximately double the ROE than with its investment banking division.

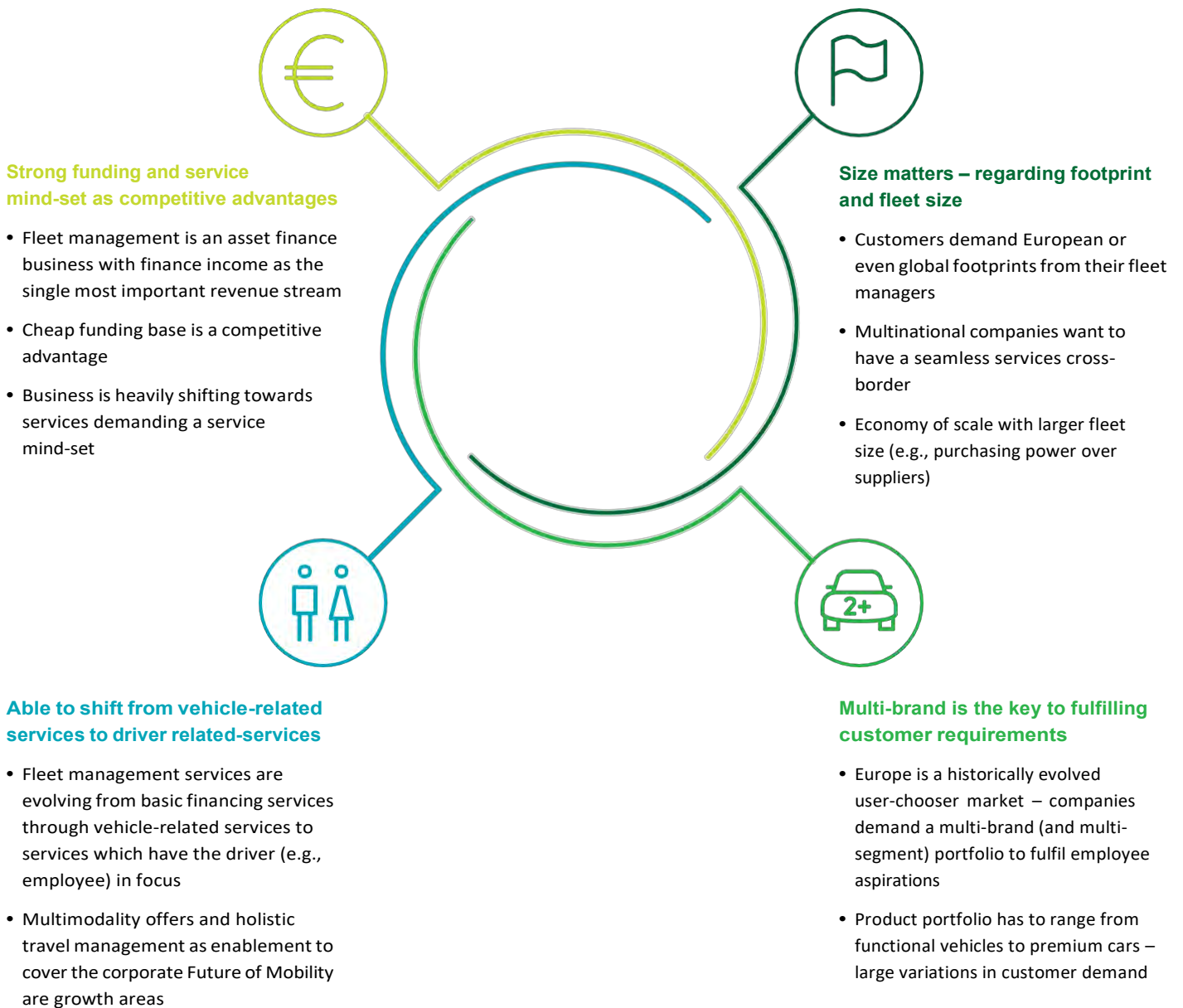
With only one percent of the group's total assets, ALD accounted for nearly nine percent of the bank's profits in the first half of 2016.<sup>22</sup>

Early in 2017 Société Générale publicly announced plans to sell a minority stake in ALD on the stock exchange via an initial public offering (IPO). The bank stated that it will remain the controlling shareholder and main funding provider of ALD.

The money that will be raised by an IPO is intended to fuel further growth, most likely with acquisitions of competitors as described in the previous section of this study.<sup>22</sup>

# Fleet management is a highly profitable business

**Fig. 17 – Key success factors for fleet management**

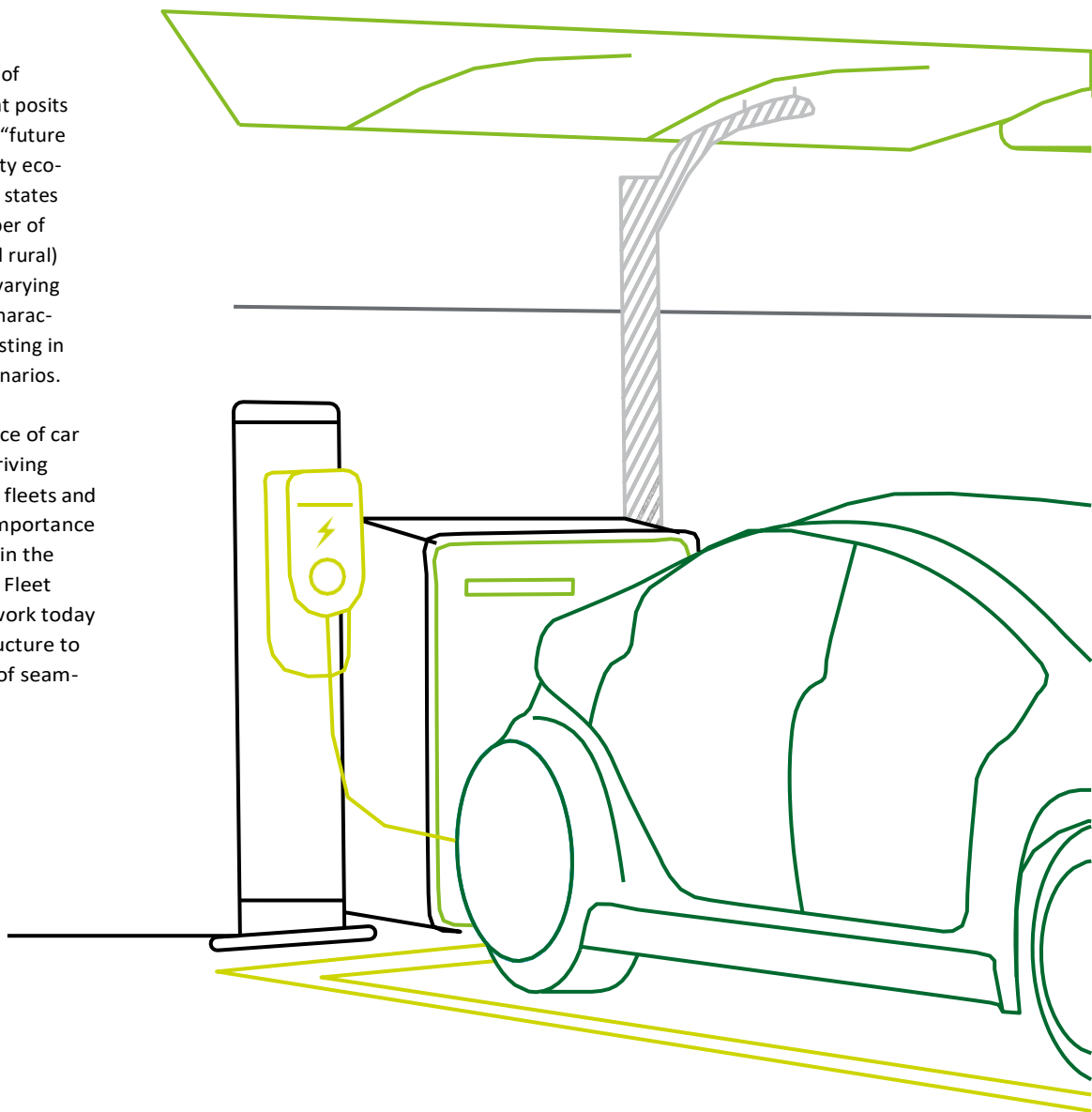


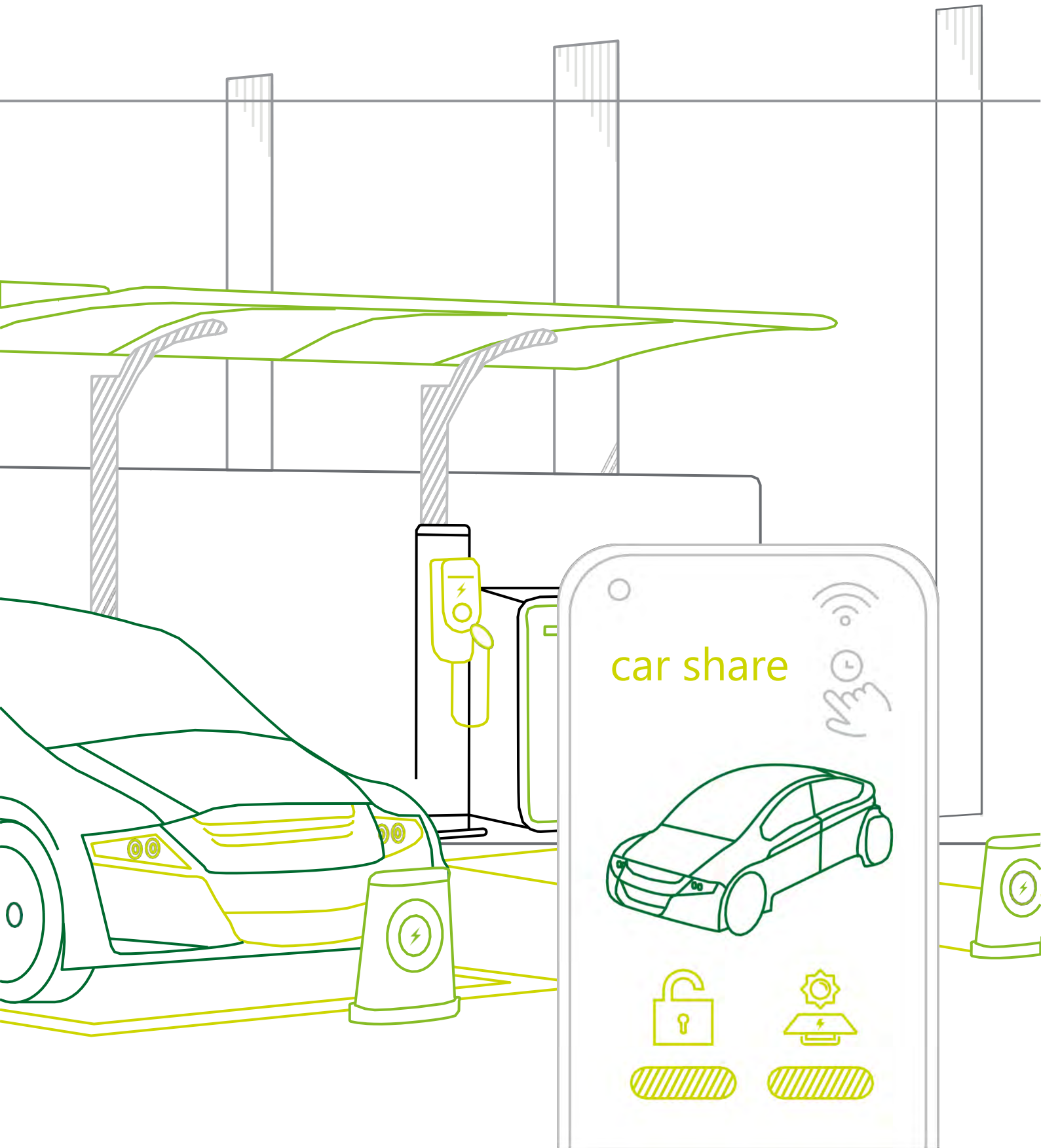
The Future of Mobility  
will be enabled by  
fleet management

# Future of Mobility and implications for fleet management

Deloitte's publication "The Future of Mobility" lays out a framework that posits the emergence of four concurrent "future states" emerging within the mobility ecosystem. A key factor is that all four states are likely to co-exist across a number of geographies (urban, suburban, and rural) and consumer demographics to a varying extent and, therefore, represent characterizations of market segments existing in parallel rather than alternative scenarios.

Deloitte sees a growing importance of car and ride-sharing as well as self-driving vehicles. For both developments, fleets and fleet management gain greater importance and will be a key to participating in the prospective mobility value chain. Fleet managers should lay the groundwork today by enabling vehicles and infrastructure to be prepared for the future state of seamless door-to-door mobility.









# Four states of the Future of Mobility

Fig. 18 – Future of Mobility: Changing Usage and Sales

3

### Future state 3 – The driverless revolution

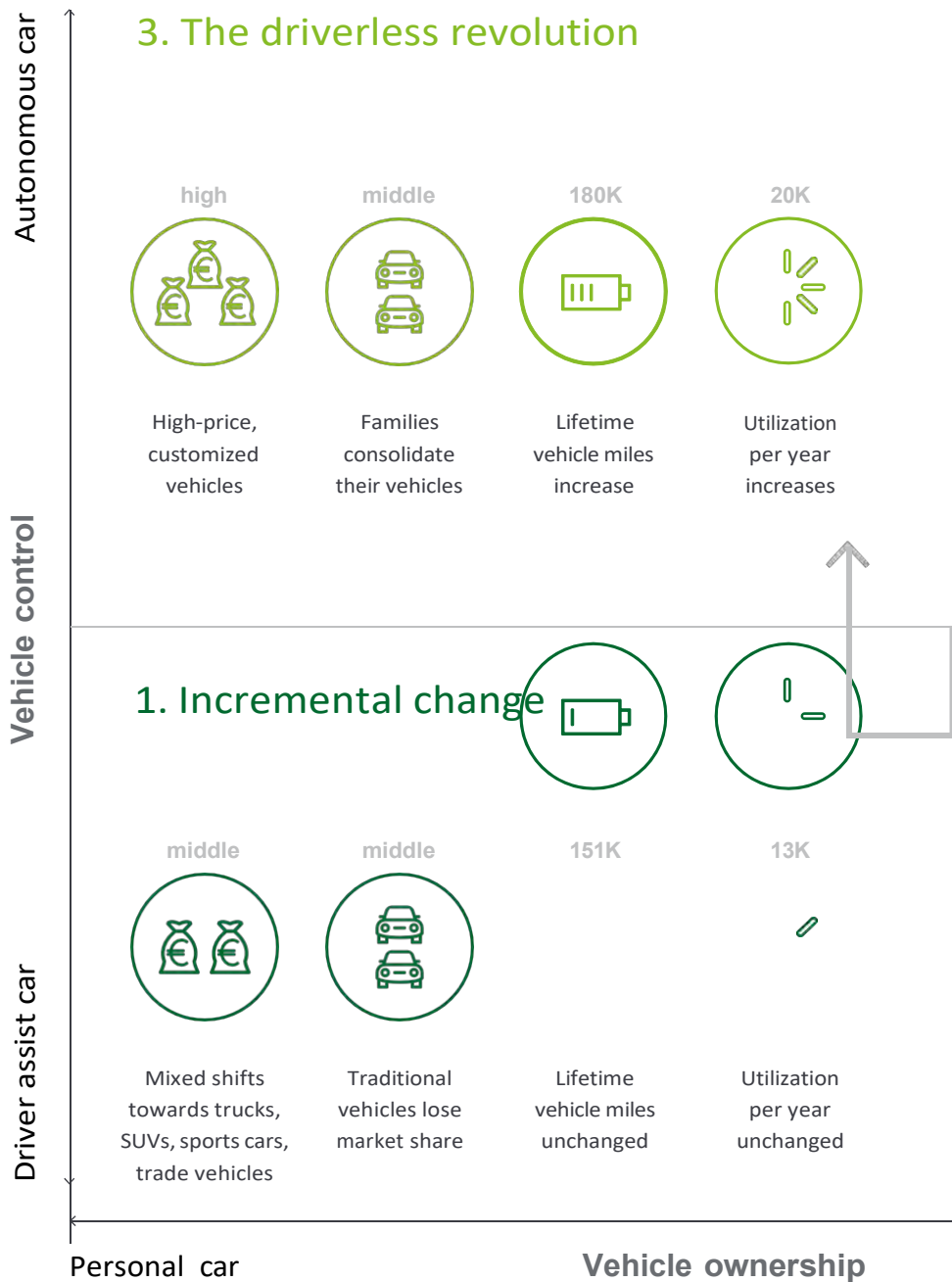
Future state 3 sees the wide-spread adoption of autonomous vehicles, but private ownership remains dominant. Drivers still prefer owning their own vehicles but seek driverless functionality for its safety and convenience.

### Future state 1 –

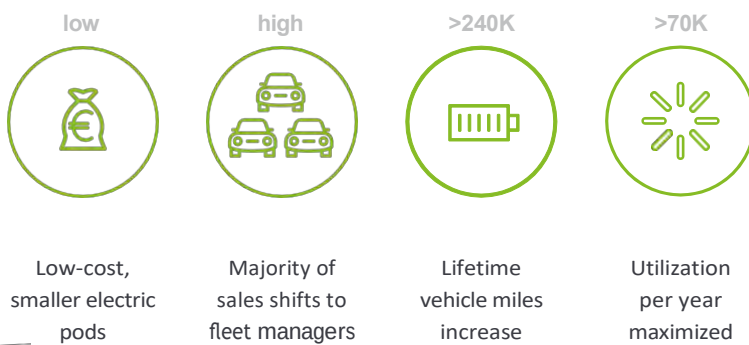
1

### Incremental change

A world where private ownership remains the norm as consumers opt for the forms of privacy, flexibility, security, and convenience that come with owning a human-driven vehicle. While incorporating driver-assist technologies, this future state assumes that fully autonomous vehicles do not completely displace driver-controlled vehicles at any time in the near future.



## 4. A new age of accessible autonomy

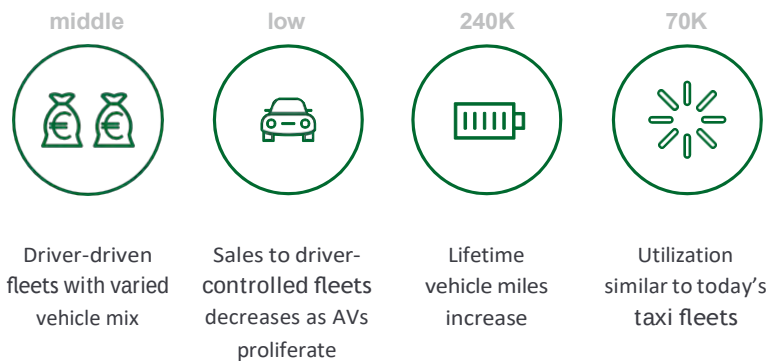


### Future state 4 – A new age of accessible autonomy

Future state 4 anticipates a convergence of both the autonomous and vehicle-sharing trends. Mobility management companies and fleet operators offer a range of passenger experiences to meet widely varied

needs at differentiated price points, initially in urban areas but spreading rapidly into suburban communities.

## 2. A world of car sharing



### Future state 2 – A world of car sharing

Future state 2 imagines how continued growth of ride-sharing and car sharing may impact both companies and people. Economic scale and increased competition could drive the expansion of shared vehicle services into new geographic territories and more specialized customer segments. As shared mobility serves a greater proportion of local transportation needs, it might reduce the need for personal vehicles, particularly in homes that have several.

Vehicle ownership

Shared car



# Generation Y

## Shift from ownership to sharing will further increase relevance of fleet management

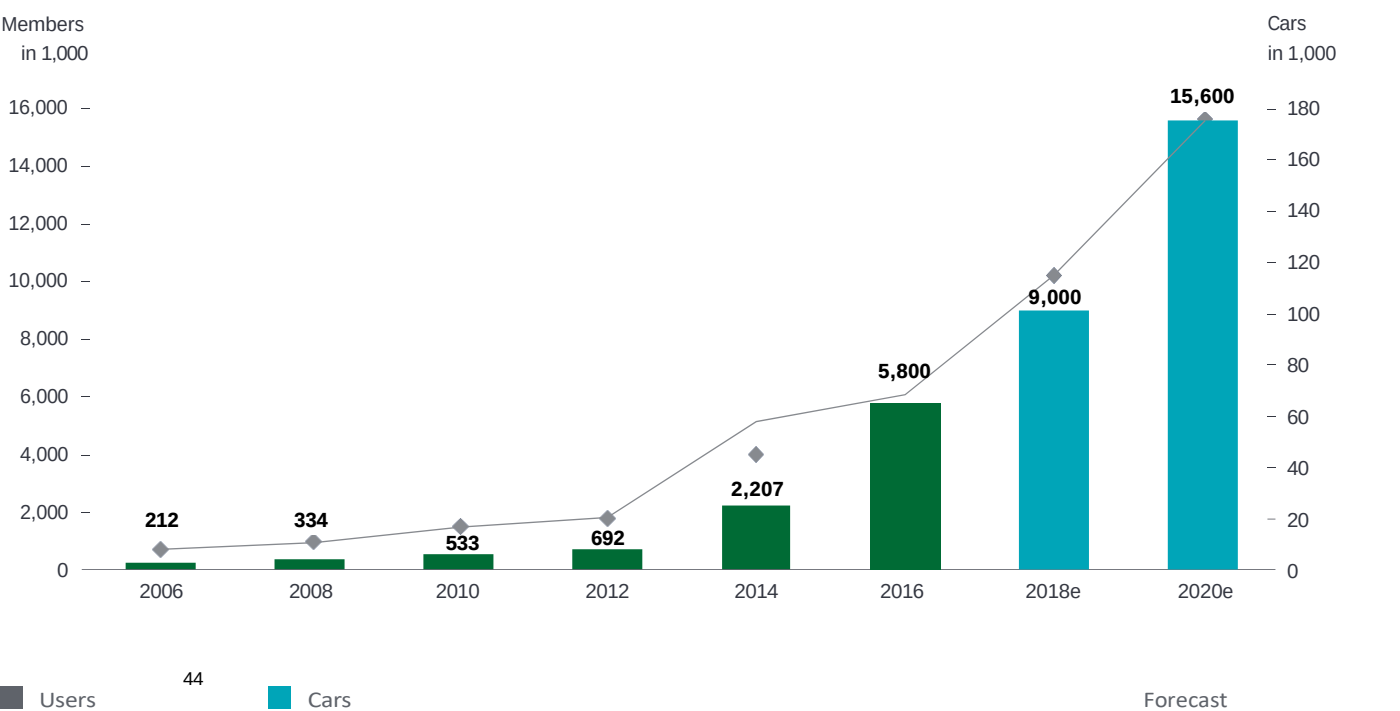
Deloitte's recent Global Automotive Consumer study highlighted the fact that Gen Y (those born between 1977 and 1994) desire connectivity and convenience and can choose from an ever-increasing range of transportation types, apart from vehicle ownership, for getting from A to B. While Baby Boomers tend to gravitate towards traditional vehicle ownership models and younger generations are highly interested in models that provide access to mobility, allow them to remain connected (and productive) at a reduced cost. The emerging mobility patterns of (young) adults are

shaping an industry in which on-demand service providers such as Uber, DriveNow and car2go have experienced and are still experiencing significant growth and are unquestionably among the defining phenomena of our future mobility as well as the digital era. These providers are changing the way individuals move, by seamlessly connecting either drivers to passengers (taxi, car pooling) or passengers to cars (car sharing). Younger generations are leading the way towards pay-per-use mobility in place of owning a car, nearly 50% of Gen Y consumers like using a smartphone app for transport and already plan travel so they can multitask.<sup>25</sup>

In 2006, the world reached a critical midpoint with over half of the world's population living in cities and urban areas. The trend is expected to accelerate, with approximately 70% of the world's population expected to live in cities by 2050.

Car sharing extends the benefits of auto-mobility to individuals without them having to bear the cost and effort of car ownership. Europe accounts for about 50% of the global car sharing market and is expected to grow further to almost 16m users by 2020 (figure 19).

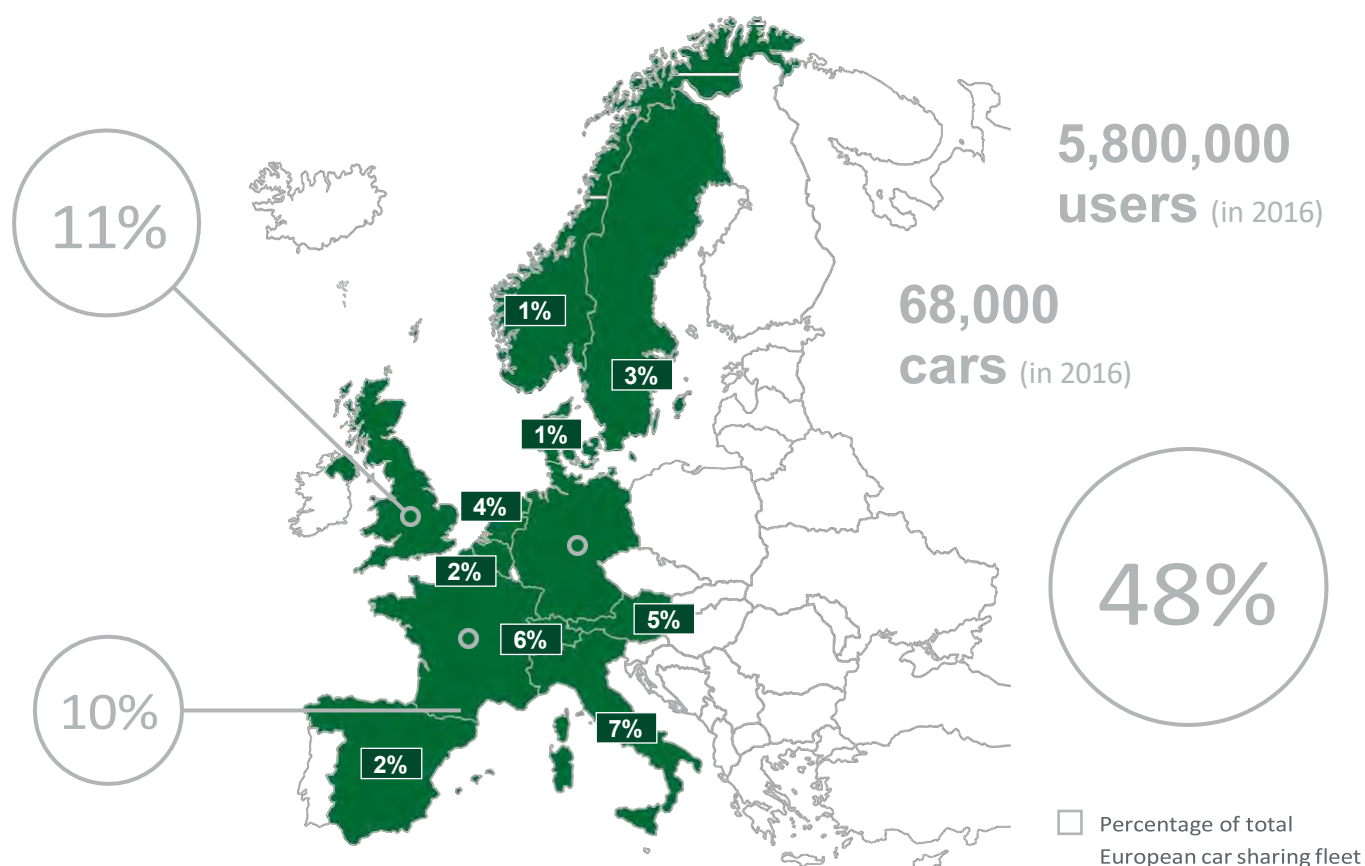
Fig. 19 – market development in Europe (2006–2020, in '000)





Source:  
Deloitte  
analysis<sup>26</sup>

Fig. 20 – Distribution of car sharing vehicles in Europe



The car sharing approach does not have to stop at a company door. In recent years a growing number of FMCs started to offer corporate car sharing programs. New in-car technologies and advanced telematics enable companies to use their corporate cars as a sharing asset for their employees. Key advantages are an optimized pool car usage, a reduction of the carbon footprint as well as large cost saving potential in terms of TCM.

With a high acceptance by young employees and a growing awareness of the total cost of employee mobility, the corporate car sharing market is expected to grow rapidly. With a prospective fleet size of 84,000 cars by 2020, this market will reach almost half the size of the conventional car sharing market.<sup>27</sup>

In a future mobility ecosystem Deloitte sees a growing importance of car and ride-sharing as well as self-driving vehicles. For both developments, fleets and fleet management gain greater importance and will be a key to participating in the prospective mobility value chain. Fleet managers should lay the groundwork today by enabling vehicles and infrastructure to be prepared for the future state of seamless door-to-door mobility.

**Fleet management will be the key to enabling sharing-based mobility services**

# From ride-hailing to robo-taxi – autonomous revolution powered by Blockchain

## Ride-hailing

With the exception of a few cities such as London and Paris, Uber, as the world's largest ride-hailing provider, did not manage to establish a significant footprint on European soil. In many European jurisdictions Uber has run into regulatory roadblocks.

In Europe, Uber challenges homegrown ride-hailing competitors who have leveraged their better knowledge of local market dynamics to build successful businesses. Businesses such as myTaxi, founded in 2009, may share some similarities with the Uber model, but they differentiate themselves by working in accordance with local regulations. Daimler's myTaxi has become Europe's largest taxi-hailing provider with over 6 million customers in 2016.<sup>28</sup> This is an astonishing growth from 2 million customers in 2015. Other European ride-hailing services have specialized in exclusive limousine transport or van/bus services. First attempts to integrate autonomous driving technology with the outlook of providing independent "robo-taxis" have been made.

## Robo-taxi

Especially in the ride-hailing business where a high percentage of the costs are associated with the driver, self-driving cars could drastically decrease these costs. A recent Deloitte study ("DUP: Future of Mobility") shows that about 50% of the cost of taxis are connected with the cost of the driver.<sup>24</sup> Self-driving robo-taxis would not only be cheaper than taxis today, the utilization of the vehicle would increase distinctly.

This development implies a growing number of vehicles going to fleet instead of to private persons. Deloitte's study "The Future of Mobility: What's next?" predicts a share of 70% autonomous driving fleet vehicles in an urban environment in new registrations by 2035.<sup>29</sup> In a connected urban environment the attractiveness of owning a car declines rapidly if one has access to a pool of cars whenever needed.<sup>31</sup>

To guarantee a seamless operation of these fully autonomous taxis a few technical issues have to be solved. Payment is a crucial part of that. Today, ride-hailing companies offer cashless payments directly via their smartphone apps, but the next revolution is just

around the corner. Blockchain technology could enable the cars to send and receive money, schedule, and pay for their own maintenance meetings in times of low utilization, etc. Blockchain could support making the car also autonomous on the financial side.

## The future is fleet

Several automotive companies have already reacted and are increasing their activities in the fleet management environment to avoid being reduced to the role of hardware providers. In the end, the winners in this race for customer contact will be those companies who are able to provide a seamless customer experience at a limited cost. Blockchain can become the enabling technology for automotive companies to reach this goal and to maintain a key role as the direct provider of mobility services to end customers. Deloitte has given further insights into this topic in a recent publication "Blockchain @ Auto Finance – How Blockchain can enable the future of mobility".<sup>30</sup>

Up to  
**68%** would be willing  
to pay extra for  
autonomous driving

**35%** of customers believe  
in the breakthrough  
of autonomous  
driving

Up to  
**85%** of GenY–Z customers  
question their need to  
own a car due to use  
of ride-hailing

**500%** of cost for ride-  
hailing vs connected  
driver

Fig. 21 – Forecast of new vehicle sales distribution (for urban areas in USA)

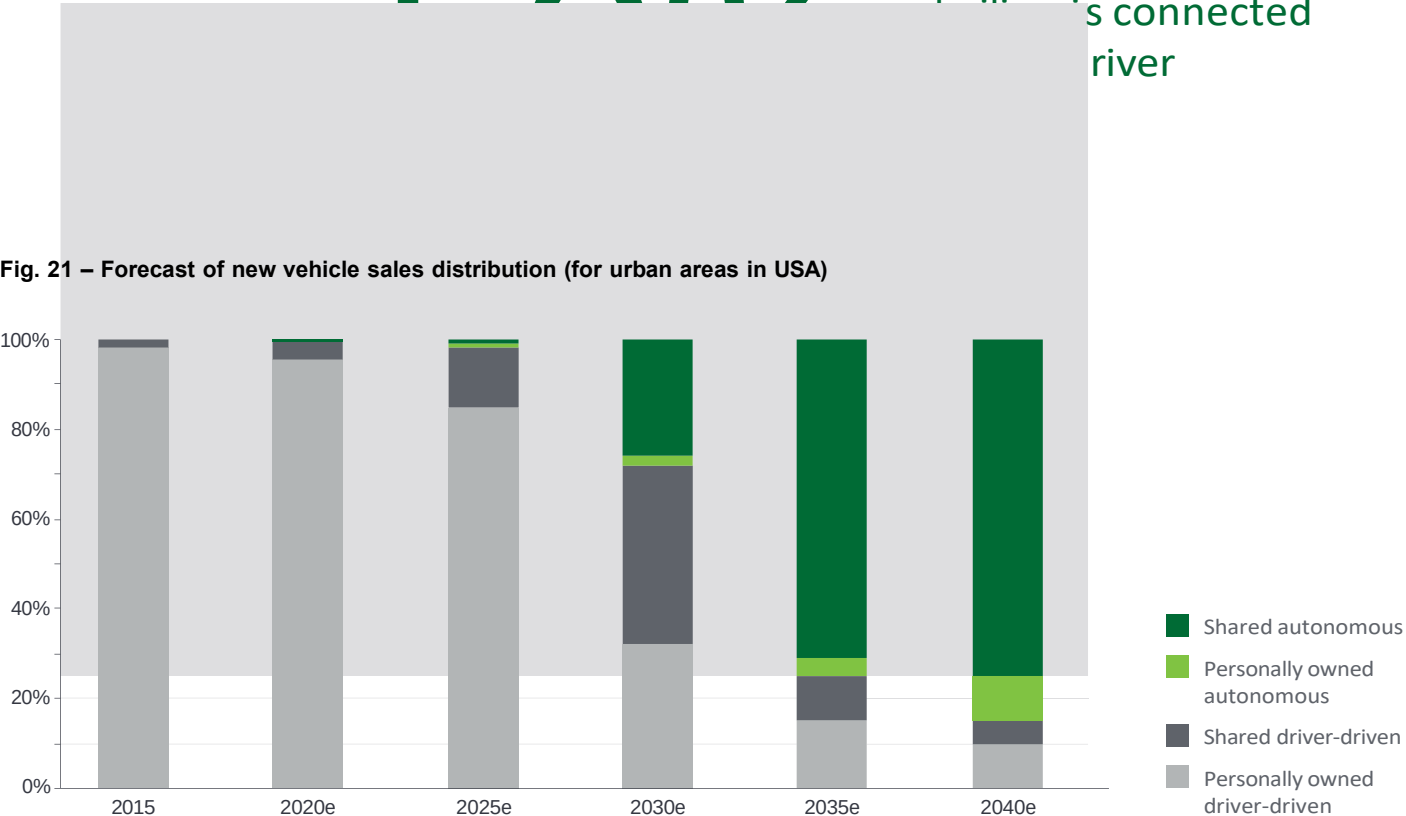


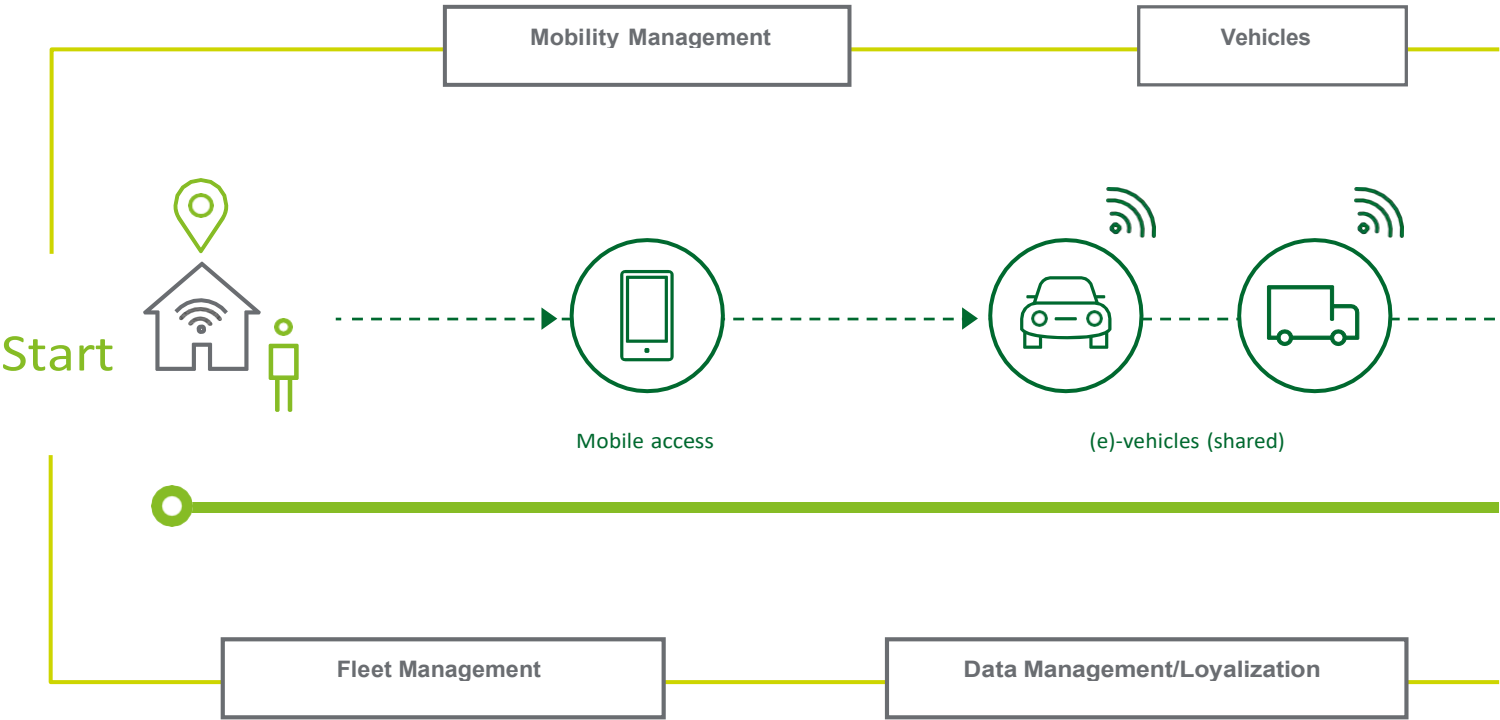




Fig. 22 – The Future of Mobility ecosystem: integrated and multi-modal inner-city customer journey

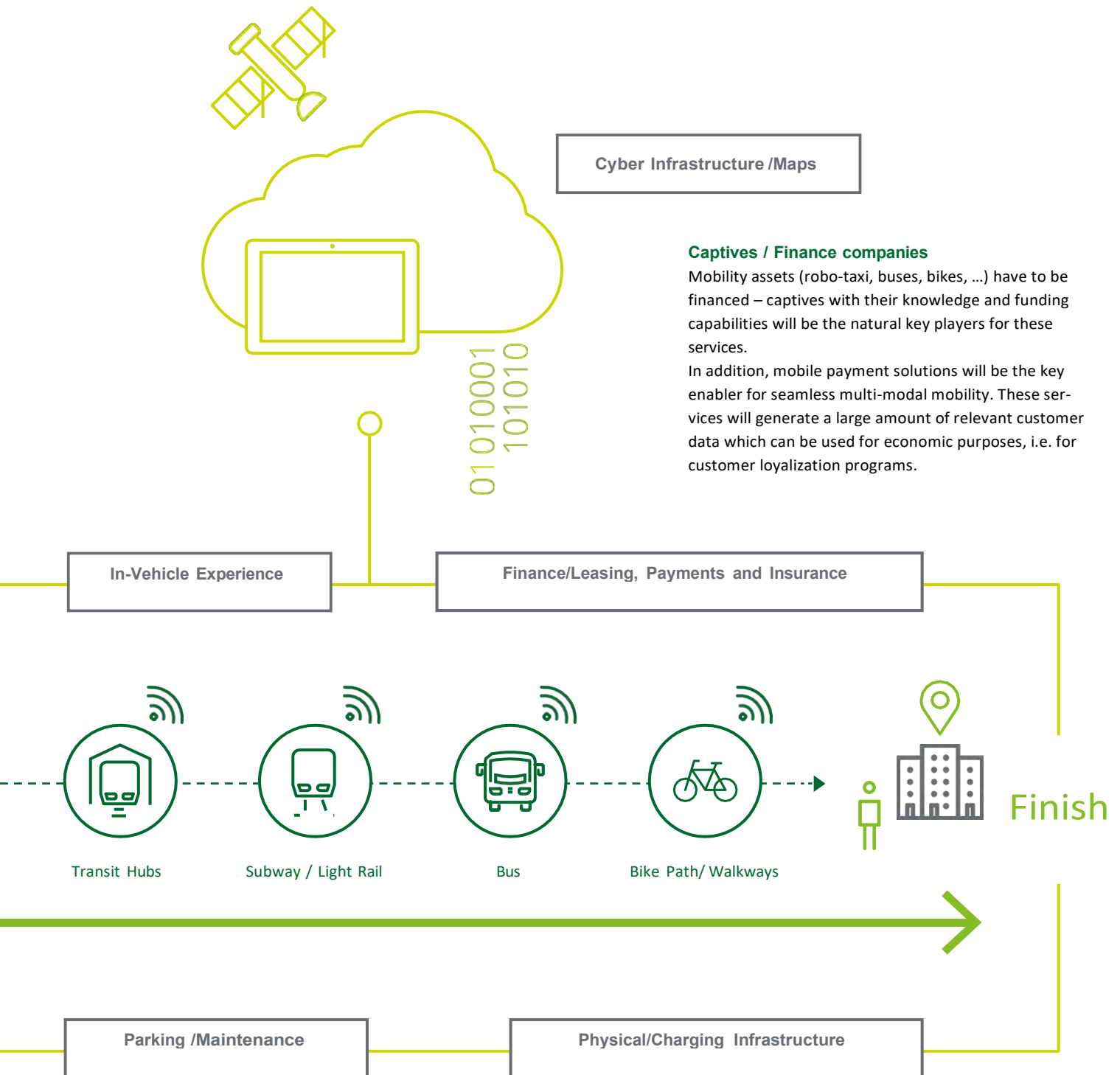
**Mobility management providers**

Mobility management services combine an individual’s specific history and current circumstances with data from millions of others and information from different modes of travel across the city. Using advanced analytics, they offer users tailored, seamless travel options.



**OEMs / Fleet Management companies**

Fleet operators store, maintain, and deploy shared autonomous vehicles throughout the city. Vehicle manufacturers build an array of shared self-driving options to meet the varying needs of millions of travelers.



### Additional providers

The in-vehicle experience is enhanced by content providers offering a variety of options, from entertainment to business applications, and supported by advertisers and subscription fees.

City planners work closely with the private sector to operate and maintain critical infrastructure, from bike racks to train platforms or electric charging stations. Those physical assets are increasingly smart and connected, allowing constant, real-time monitoring.

# Strategic fields of action regarding fleet management

Fig. 23 – Market entry rationales from the perspective of various industries

|                                 | <br><b>OEMs</b>                                                                                                                                                                                                                                                                                                                                                         | <br><b>Banks</b>                                                                                                                                                                                                                                                                   | <br><b>Platforms / Tech Companies</b>                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Strategic considerations</b> | <ul style="list-style-type: none"> <li>• React to sales channel shift from private to corporate and prepare for self-driving fleets</li> <li>• Protect the core business with regard to sales discounts and after sales revenue</li> <li>• Expand the value chain with focus on services and residual value</li> <li>• Secure customer access</li> <li>• Leverage full-service leasing and fleet management as capability for mobility services</li> </ul> | <ul style="list-style-type: none"> <li>• Enter in a reasonably stable, non-cyclical industry with recurring revenues</li> <li>• Diversified revenue stream in times of low interest rates based on fee-generating services</li> <li>• Locked-in customers based on sticky customer relationships with potential to up- and cross-sell within core business</li> </ul> | <ul style="list-style-type: none"> <li>• Enter into mobility market to expand value chain</li> <li>• Leverage mobility behavior information generated by fleet management data for core business (location-based services)</li> <li>• Build mobility management capability to transfer to private user market</li> <li>• Prepare foundation for a future world of autonomous shared fleets to own ecosystem regarding in-car entertainment and apps</li> </ul> |
| <b>Competitive advantage</b>    | <ul style="list-style-type: none"> <li>• Established dealer network throughout Europe and global footprint</li> <li>• Asset know-how regarding vehicles and usage behavior</li> <li>• Holistic view of the value chain and vehicle lifetime</li> </ul>                                                                                                                                                                                                     | <ul style="list-style-type: none"> <li>• Bank branch network as sales channel</li> <li>• Access to and detailed knowledge of small and medium entities</li> <li>• Strong understanding of funding business</li> </ul>                                                                                                                                                 | <ul style="list-style-type: none"> <li>• Strong knowledge in partner management and integration</li> <li>• Truly customer-centric mentality</li> <li>• Expertise in data management and analytics (telematics)</li> <li>• Platform integration capability towards multi-modal mobility</li> </ul>                                                                                                                                                              |



# Strategic recommendations for fleet management companies

The increasing demand for full service leasing and associated fleet management has significantly fueled the growth and profitability of fleet management companies in recent years. This growth sparked the interest of several other players such as automotive companies and banks that are (re)entering this market based on their own core products, be it vehicles or leasing business.

On the other hand, platform and technology companies see this industry as the entry point for their data-driven and customer-centric business models towards the Future of Mobility.

Today, the fleet management companies are still ahead in this rather complex business, with the competition catching up. To keep that lead over the competition fleet management companies should not rest on their merits and strong financial results but strategically position themselves towards the future.

The key success factors in fleet management of the future are diverse. It is essential to build a global footprint and have the capability to provide seamless service offerings across borders. Fleet customers will increasingly demand consulting services to reduce the cost of their fleets. This can on the one hand be addressed by sophisticated data and driver behavior analysis based on telematics to increase efficiency. On the other hand, innovative mobility solutions such as corporate car sharing and similar can also bear the possibility of earning revenues based on the corporate fleet. In addition, driver-centric and non-car related services will be increasingly important in the future.

Based on these capabilities, it is a logical step for fleet management companies to further expand their client base towards the private channel and to be prepared for the Future of Mobility where, due to sharing behavior and self-driving cars the differences between the private and corporate channels will become more and more blurred.

# Conclusion

Fleet management in Europe is a multi-billion-euro industry based on a profitable business model and the increasing shift of new car sales towards the corporate channel. The top five players combined make up for more than 50% of the managed cars. Current key players are predominantly bank-backed coming from the roots of this asset-based business. Nevertheless, more and more OEMs are putting focus on this market as they see an increasing relevance for their core business in a world of changing mobility.

The relevance of this market will further increase in the future due to multiple influencing factors. The younger generation will buy fewer cars in the future. Firstly, the relevance of owning a car for social status is strongly declining (also blurring the importance of brand perception of cars). Secondly, the increasing urbanization drastically reduces the attractiveness of owning a car, amongst other things due to the high cost and hassle associated with finding a parking space alone. The increasing shift from ownership towards usage fueled by the increasing mobility offerings and business models especially in urban areas will further shift new car sales towards the corporate channel. Corporates will start to see their company fleets not only as a cost but also as a potential revenue model leveraging services such as corporate car sharing. In the further future with autonomous cars such as robo-taxis being a reality the trend described will further accelerate.

The increasing customer demand for multi-modal integrated mobility will require only a limited amount of truly integrated mobility platform providers. These players will be in a unique position to take ownership of customer access and data (mobility, payment, etc.) which will be the key to monetizing the mobility ecosystem.

To answer these trends requires bold strategic choices under uncertainty. The fields of action for current or potential future actors in this environment differ depending on their background and strategic aspiration. OEMs face the threat of losing ownership of the customer contact and large parts of their value chain and being reduced to sole providers of hardware. Fleet managers need to rethink their position as asset-managers towards integrated mobility providers also offering services that are not necessarily related to the vehicles. Platform providers and tech companies might think about entering the market top-down, leveraging their existing customer access.

Fleet management will be one of the key capabilities to be successful in this Future of Mobility. Deloitte is ready to support you in deriving the necessary strategies and actions.





# Sources

1. Global Fleet, "Europe compared to the United States: Understand the key differences before taking full advantages of the similarities", 2015
2. Fleetnews.co.uk: <http://www.fleetnews.co.uk/fleet-leasing/news/latest-fleet-leasing/2016/08/23/salary-sacrifice-caught-in-the-crossfire-of-hmrc-crackdown>, 2015
3. Fleetnews.co.uk: <http://www.fleetnews.co.uk/news/fleet-industry-news/2016/11/23/partial-reprieve-for-salary-sacrifice-and-company-car-tax-changes-announced>, 2016
4. Fleetnews.co.uk: <http://www.fleetnews.co.uk/fleet-leasing/news/latest-fleet-leasing/2016/12/01/zenith-welcomes-chancellor-s-announcement-on-salary-sacrifice>, 2016
5. Handelsblatt.com: <http://www.handelsblatt.com/auto/nachrichten/eigenzulassungen-wenn-hersteller-selbst-ihre-besten-kunden-sind/12790362.html>, 2016
6. Istituto nazionale di statistica, 2016
7. International Energy Agency: <https://www.iea.org/policiesandmeasures/pams/spain/name-38020-en.php>, 2016
8. N332 – Driving in Spain: <http://n332.es/2015/05/07/replacing-older-cars-for-new-plan-pive/>, 2015
9. Financial Accounting Standards Board: [http://www.fasb.org/jsp/FASB/Page/BridgePage&cid=1351027207574#section\\_5](http://www.fasb.org/jsp/FASB/Page/BridgePage&cid=1351027207574#section_5), 2016
10. Verordnung (EG) Nr. 715/2007 des Europäischen Parlaments und des Rates vom 20. Juni 2007 über die Typgenehmigung von Kraftfahrzeugen hinsichtlich der Emissionen von leichten Personenkraftwagen und Nutzfahrzeugen (Euro 5 und Euro 6) und über den Zugang zu Reparatur- und Wartungsinformationen für Fahrzeuge (Text von Bedeutung für den EWR)
11. Focus: [http://www.focus.de/auto/ratgeber/kosten/wltp-zyklus-vs-nezf-ist-der-wltp-zyklus-wirklich-besser\\_id\\_5749720.html](http://www.focus.de/auto/ratgeber/kosten/wltp-zyklus-vs-nezf-ist-der-wltp-zyklus-wirklich-besser_id_5749720.html), 2016
12. Verband der Automobilindustrie: <https://www.vda.de/de/themen/umwelt-und-klima/abgasemissionen/wltp-weltweit-harmonisierter-zyklus-fuer-leichte-fahrzeuge.html>, 2016
13. Umweltbundesamt: <https://www.umweltbundesamt.de/sites/default/files/medien/461/publikationen/3773.pdf>, 2010
14. Department for Transport, Office for Low Emission Vehicles, and The Rt Hon John Hayes CBE: <https://www.gov.uk/government/news/more-drivers-choose-ultra-low-emission-vehicles>, 2016
15. Office for Low Emission Vehicles: <https://www.gov.uk/government/organisations/office-for-low-emission-vehicles>, 2017
16. SWR: <http://www.swr.de/swraktuell/bw/massnahmenpaket-zur-luftverbesserung-in-stuttgart-fahrverbote-fuer-aeltere-diesel-ab-2018/-/id=1622/did=19050542/nid=1622/7wvi7n/>, 2017
17. Spiegel: <http://www.spiegel.de/auto/aktuell/diesel-fahrverbot-in-hamburg-auf-max-brauer-allee-a-1145774.html>, 2017
18. Deloitte analysis based on Kraftfahrtbundesamt
19. mergermarket.com
20. Deloitte analysis, estimation of multi-make of two thirds in Alphabet's EU fleet based on BMW annual reports, Alphabet press statements, <http://www.wiwo.de/unternehmen/leasing-verlorener-vorteil-seite-3/5258432-3.html>
21. Deloitte analysis based on LeasePlan: Annual Report 2015 p.24, ALD (2015): Investor presentation, 2016
22. Bloomberg: <https://www.bloomberg.com/news/articles/2016-11-02/at-societe-generale-returns-from-car-leasing-dwarf-banking>, 2016
23. Bloomberg: <https://www.bloomberg.com/news/articles/2017-02-09/socgen-posts-profit-that-tops-estimates-plans-car-leasing-ipo>, 2016
24. Deloitte University Press: "Future of Mobility", <https://dupress.deloitte.com/dup-us-en/focus/future-of-mobility.html>, 2016
25. Deloitte: What's ahead for fully autonomous driving, 2017
26. Monitor Deloitte: Car sharing on the rise, 2017
27. Frost & Sullivan: Future of Mobility – Press Release, 2014
28. Daimler Annual Report 2016
29. Deloitte University Press (2016): Future of Mobility – What's next?, 2016
30. Deloitte: Blockchain @ Auto Finance - How Blockchain can enable the future of mobility, 2017
31. Autonomes Fahren in Deutschland – wie Kunden überzeugt werden, 2016









Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see [www.deloitte.com/de/UeberUns](http://www.deloitte.com/de/UeberUns) for a more detailed description of DTTL and its member firms.

Deloitte provides audit, risk advisory, tax, financial advisory and consulting services to public and private clients spanning multiple industries; legal advisory services in Germany are provided by Deloitte Legal. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte’s more than 244,000 professionals are committed to making an impact that matters.

This communication contains general information only not suitable for addressing the particular circumstances of any individual case and is not intended to be used as a basis for commercial decisions or decisions of any other kind. None of Deloitte Consulting GmbH or Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte network”) is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.



**El futuro de la movilidad.  
Cómo la tecnología del  
transporte y las tendencias  
sociales están creando un  
nuevo ecosistema de negocios**

# El futuro de la movilidad

Cómo la tecnología del transporte y las tendencias sociales están creando un nuevo ecosistema de negocios



El Futuro de la Movilidad es una publicación de Deloitte LLP. Deloitte es líder en proveer servicios de auditoría, consultoría e impuestos a la industria automotriz, incluyendo a muchas de las marcas más admiradas del mundo y el 80% de las empresas del índice Fortune 500. Nuestra gente trabaja en más de 20 sectores industriales con un objetivo: brindar resultados cuantificables y duraderos. Los clientes cuentan con Deloitte para ayudarlos a transformar la incertidumbre en posibilidad, y el cambio rápido en progreso duradero. Nuestra gente sabe cómo anticipar, colaborar, e innovar, y crear oportunidades aun desde el obstáculo imprevisto.



# Sobre los Autores

**Scott Corwin** es director de Deloitte Consultoría en Estrategia y Métodos de Transformación de Negocios. Tiene más de 25 años de experiencia trabajando junto a líderes corporativos desarrollando e implementando transformaciones basadas en la estrategia; específicamente en temas de globalización, I&D avanzado, innovación tecnológica, y nuevos modelos de negocios. Corwin trabaja con clientes en una amplia gama de industrias, incluyendo la automotriz, tecnología, industria, medios, productos para el consumidor, minorista, salud, telecomunicaciones, sector público, y sin fines de lucro. Es el líder de la iniciativa de Deloitte “El Futuro de la Movilidad”, y socio líder de consultoría para varias de las cuentas claves de la firma, incluyendo una de las automotrices líderes.

**Joe Vitale** es el líder de industria automotriz global para Deloitte Touche Tomatsu Limited, y además es el socio global líder de servicio al cliente para una de las automotrices líderes. Es responsable de brindar las soluciones multidisciplinarias de Deloitte, incluyendo consultoría, gestión de riesgo empresarial, impuestos, y servicios de asesoría financiera a empresas automotrices en todo el mundo. Vitale se especializa en estrategia corporativa, Fusiones y Adquisiciones, optimización de cadenas de suministro, y desarrollo de nuevos productos.

**Eamonn Kelly** es director de Deloitte Consulting LLP y Director de Marketing de la práctica de Estrategia y Operaciones. Durante más de dos décadas ha asesorado a ejecutivos en corporaciones líderes en varios sectores de la industria, agencias públicas clave globales y nacionales, e importantes fundaciones filantrópicas. Antes de formar parte de Deloitte, fue socio de Grupo de Monitoreo y también fue CEO de la Red de Negocios Global, donde fue líder de ideas sobre el futuro, escribió dos libros y numerosos artículos. Brindó su perspectiva y nuevas metodologías para dominar el cambio y la incertidumbre.

**Elizabeth Cathles** es gerenta de la práctica de Estrategia y Operaciones de Deloitte Consulting LLP. Tiene más de 10 años de experiencia en estrategia e innovación, se especializa en estrategia de crecimiento, estrategia de marketing y cliente, gestión organizativa, I&D, y estrategia de lanzamiento de productos. Su experiencia incluye la creación e implementación de nuevos procesos y estructuras para el desarrollo de productos; estrategias para el lanzamiento y crecimiento de productos en geografías múltiples; asistencia para diseñar sistemas e capacitación organizativa para trabajar con líderes globales; e implementar enfoques innovadores a la experiencia del cliente.

# Índice

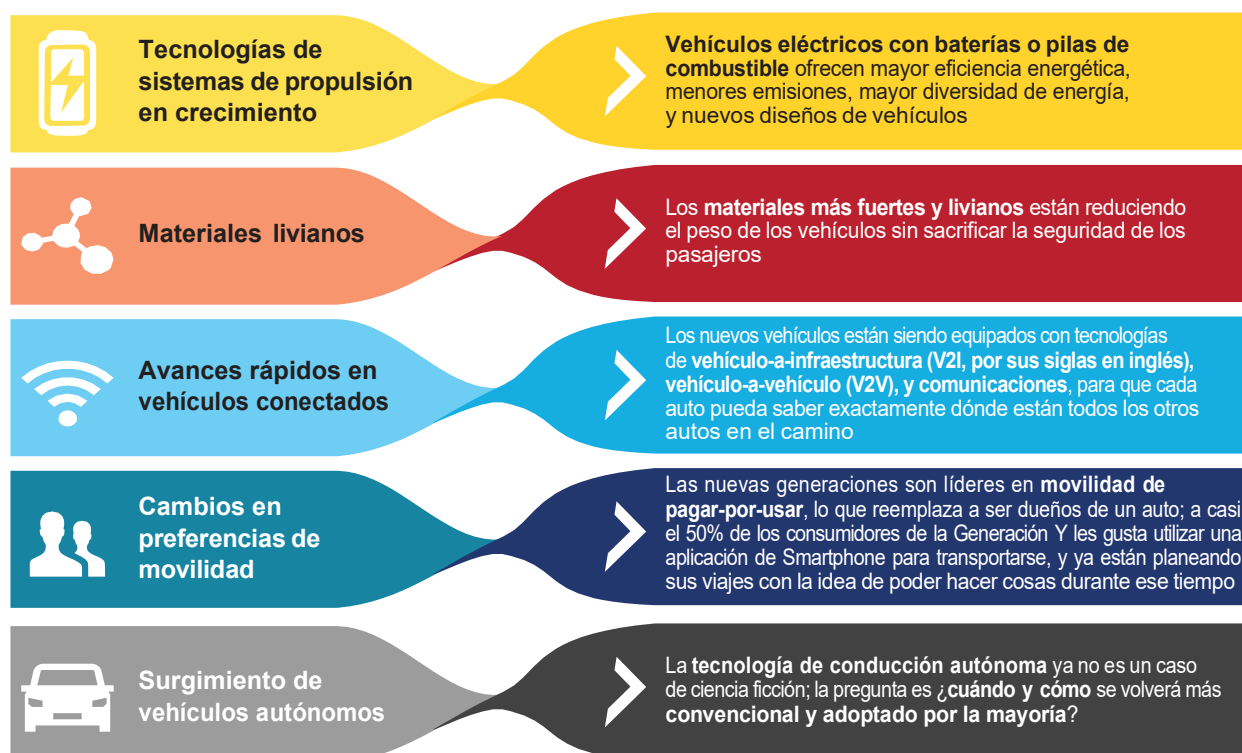
|                                                |  |    |
|------------------------------------------------|--|----|
| Introducción                                   |  | 1  |
| La importancia de la industria automotriz      |  | 3  |
| Dos visiones divergentes                       |  | 5  |
| Cuatro futuros a la vez                        |  | 8  |
| ¿Cuánto por kilómetro?                         |  | 11 |
| El camino del cambio                           |  | 13 |
| El futuro de la industria automotriz extendida |  | 16 |
| Conclusiones                                   |  | 21 |
| Notas                                          |  | 22 |
| Contactos                                      |  | 26 |
| Agradecimientos                                |  | 27 |

# Introducción

**U**N diálogo sobre la evolución futura del transporte y movilidad, de importancia crítica, está teniendo lugar en todo ámbito vinculado con la industria automotriz. El debate está impulsado por la convergencia de una serie de fuerzas con el poder de cambiar la industria y establecer mega-tendencias (ver cuadro 1). Las tecnologías innovadoras están cambiando

cómo las empresas desarrollan y fabrican sus vehículos. Los sistemas motrices (“powertrain”) eléctricos e híbridos tienden a ofrecer mayor propulsión con menor inversión energética, y con menores niveles de emisiones.<sup>1</sup> Materiales nuevos y livianos les permiten a los fabricantes reducir el peso de los vehículos sin sacrificar la seguridad de los pasajeros.<sup>2</sup>

**Cuadro 1. Fuerzas convergentes transforman la evolución futura del transporte automotriz y la movilidad**





Mayores adelantos impulsan el advenimiento de los vehículos autónomos; cada día hay más informes con noticias que cuentan que los autos sin conductor pronto serán una realidad comercial.<sup>3</sup> Hemos visto avances rápidos en el “auto conectado”, innovaciones que integran tecnologías de comunicación y la Internet de las cosas para proporcionar valiosos servicios a los conductores.<sup>4</sup> Los vehículos con módulos de control y sensores que pueden establecer comunicaciones vehículo-a-vehículo (V2V) y vehículo-a-infraestructura (V2I) pueden proactivamente recalcular el camino para evitar peligros, y pedir ayuda en caso de accidente.<sup>5</sup> Muy pronto, va a ser normal para los autos tener conciencia exacta de dónde están en relación a otros vehículos y potenciales peligros, y podrán tomar acción preventiva para evitar accidentes.<sup>6</sup>

Del mismo modo los jóvenes adultos, junto con la población urbana, están gravitando hacia un modelo de consumo de movilidad personal basado en pagar-por-usar en vez de la compra directa de un bien de capital, lo que

implica un cambio fundamental en el modelo de consumo actual, centrado en la propiedad personal de autos.<sup>7</sup>

En resumidas cuentas, un sistema consolidado desde hace un siglo está por sufrir una transformación radical que podría resultar en la aparición de un nuevo ecosistema<sup>8</sup> de movilidad personal.

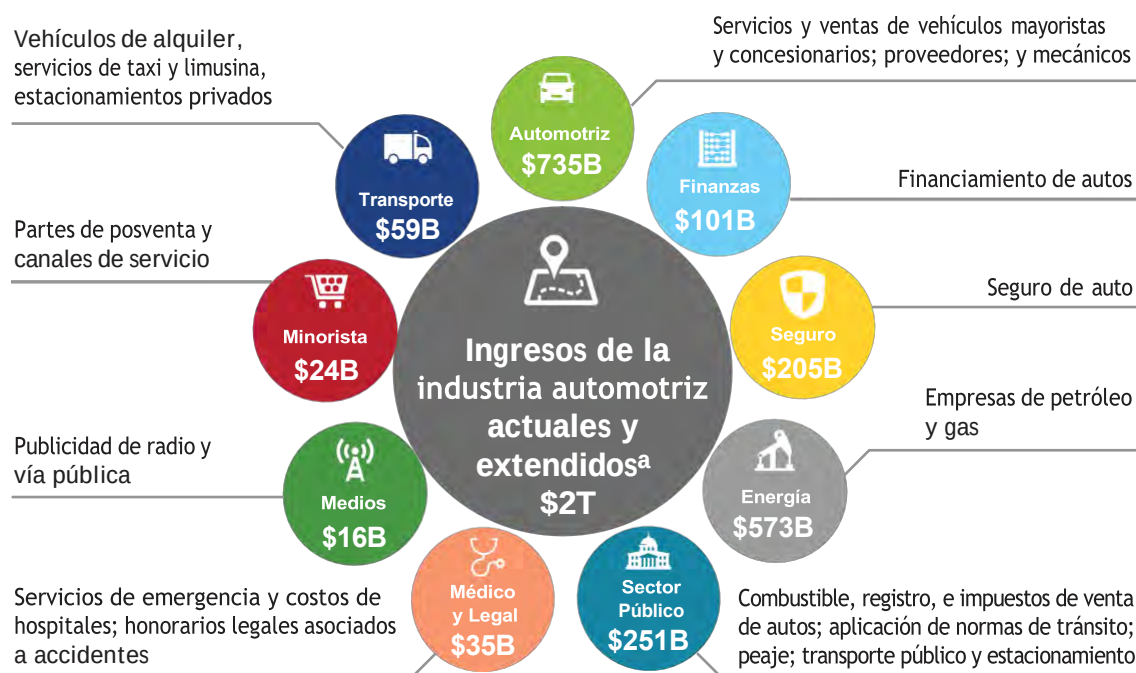
El debate actual está centrado en si la industria automotriz extendida evolucionará incrementalmente hacia algún ecosistema futuro de movilidad, o si el cambio ocurrirá a un ritmo más extremo y de forma altamente disruptiva. Nadie sabe el alcance total y la magnitud de los cambios que vendrán, qué implican, o cómo evolucionarán. Sin embargo, estas fuerzas tienen el potencial de alterar las estructuras actuales de la industria, los modelos de negocios, las dinámicas competitivas, la creación de valor, y las proposiciones de valor de cliente. Puede que estemos en el umbral del cambio más grande que haya visto la industria.

# La importancia de la industria automotriz

**N**o es ningún misterio por qué le prestamos tanta atención a las idas y vueltas de la industria automotriz: su cadena de valor extendida es un motor esencial del crecimiento económico global. En EEUU, el sector generó dos trillones de dólares de ingresos anuales en 2014 (ver cuadro 2), lo que representa 11.5%

del PBI de EEUU<sup>9</sup>. Esto proviene de fabricantes de autos, proveedores, concesionarios, empresas de servicios financieros, empresas de petróleo, minoristas de combustible, estacionamiento público y privado, impuestos de sector público, peajes y aplicación de normas de tránsito, atención médica, y otros.

**Cuadro 2. Ingresos de la industria automotriz extendida 2014**



Fuente: Análisis de Deloitte basado en IBISWorld Industry Reports, IHS, DOT, US Census, EIA, Auto News, TechCrunch. Los ingresos actuales representan cifras de 2014 (o anteriores si no había datos de 2014 disponibles) en EEUU.

<sup>a</sup> Los ingresos totales son \$1.99T.

Gráfico: Deloitte University Press | DUPress.com



En Deloitte nos hemos embarcado en un estudio profundo y abarcativo de la industria automotriz extendida y el impacto potencial de cada elemento en las industrias relacionadas.<sup>10</sup> Hemos concluido que el cambio sucederá sistemáticamente: una marea creciente, no un tsunami. En ningún momento ocurrirá que el mundo tendrá que decidir entre dos opciones opuestas: o zambullirse completamente en un sistema de movilidad sin conductores y pagar-por-usar, o que no cambie nada. El nuevo ecosistema de movilidad personal probablemente surgirá de forma irregular en diferentes geografías, grupos demográficos, y otras dimensiones, y en el futuro evolucionará en fases.

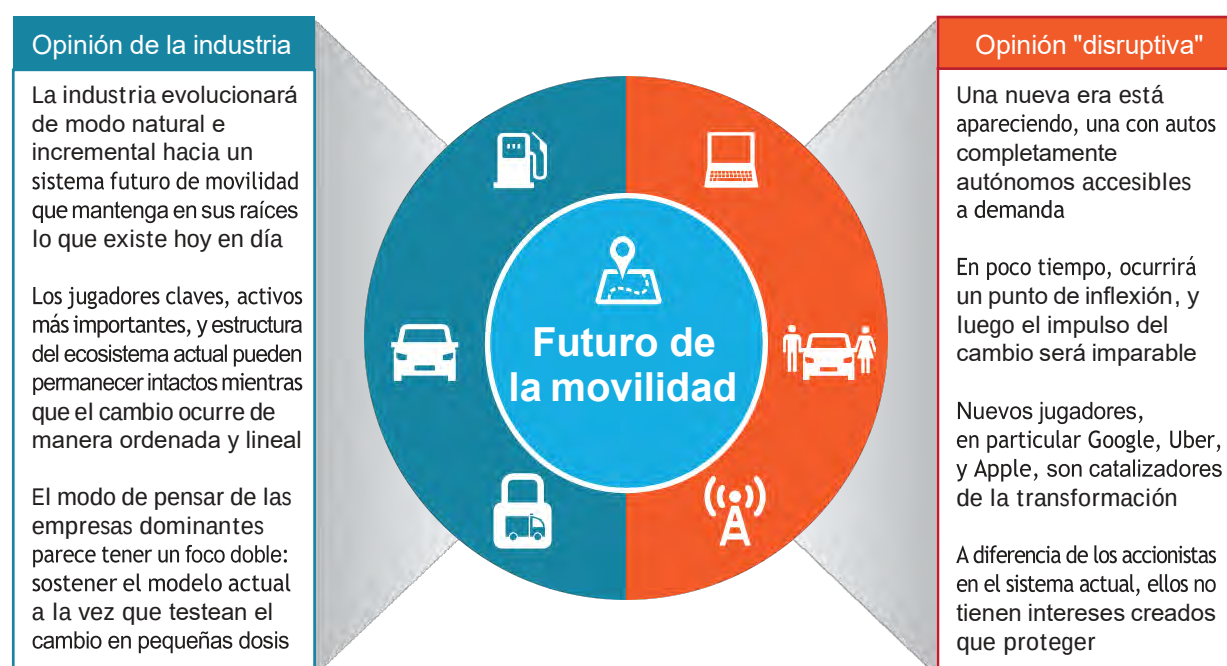
# Dos visiones divergentes

**H**ay dos visiones profundamente diferentes sobre el futuro de la movilidad. La diferencia fundamental es si el sistema actual de propiedad personal de vehículos controlados por conductores permanecerá relativamente sin cambios, o si en el futuro migraremos a un sistema sin conductores de movilidad predominantemente compartida. También hay una diferencia crítica sobre el camino futuro.

La opinión “de la industria” sostiene que el sistema actual puede progresar de un modo ordenado y lineal, en el que los activos actuales de la industria y la estructura fundamental permanecerán esencialmente intactos.

La opinión “disruptora” sostiene que habrá un punto de inflexión con un futuro muy diferente, un futuro con grandes beneficios potenciales para la sociedad.

**Cuadro 3. Opiniones "de la industria" y "disruptoras" sobre el futuro de la movilidad**







Dentro de la comunidad tecnológica, las empresas están trabajando para alcanzar algo radicalmente diferente al sistema actual de automóviles de propiedad personal conducidos por humanos. Dentro de esta perspectiva, que llamamos la opinión disruptiva, estamos ante el advenimiento de una nueva era, en la que habrá autos autónomos accesibles a demanda. Puede que el progreso hacia ese objetivo sea inicialmente moderado, pero antes de mucho tiempo ocurrirá un punto de inflexión, luego del cual el impulso del cambio aumentará su velocidad. Imagine un mundo donde todas estas ideas son verdad:

- Los vehículos casi nunca chocan. La conducción autónoma ha eliminado la causa de casi todos los accidentes: el error humano.<sup>11</sup>
- Los embotellamientos son algo raro, gracias a sensores que permiten que haya menos espacio entre vehículos, y sistemas de dirección con conciencia en tiempo real de las congestiones.
- La demanda energética disminuye, dado que los autos tienen menor masa y peso, y esto les permite ser impulsados por sistemas motrices más compactos, eficientes, y ecológicos.
- Los costos de los viajes se desploman, y el costo promedio de pasajero por milla baja del actual precio de un dólar a 30 centavos, gracias a tasas de utilización de activos dramáticamente más altas.
- La infraestructura se financia por tarifas por uso real, dado que la tecnología de autos conectados permite a los sistemas calcular exactamente el uso de camino por persona.
- Desaparecen los estacionamientos, al disminuir la necesidad de tenerlos, con los autos de conducción autónoma y los modelos en los que se comparten los autos.
- La policía deja de tener relación con el tránsito, dado que los vehículos autónomos están programados para no exceder el límite de velocidad o violar ninguna norma de tránsito.
- La velocidad de los servicios se acelera y los costos se abaratan con el nacimiento de redes completamente autónomas de camiones de largo recorrido que pueden operar durante períodos de tiempo más extendido y cubrir distancias más largas con menores costos laborales.
- El transporte multimodal continuo se convierte en la nueva norma, y la mayor interoperabilidad le permite a los consumidores ir del punto A al punto B mediante modos de transporte múltiples y conectados, y a un costo fijo y único que se cobra en un solo sistema de pagos.

La mayor parte de la tecnología que permitirá convertir esta visión en realidad ya existe, y los disruptores están trabajando en implementarla, y de ese modo catalizar la transformación. Los autos sin conductor de Google ya han recorrido más de un millón y medio de kilómetros en modo autónomo, y la empresa está efectuando programas piloto y de testeo con pequeñas flotas de vehículos autónomos en Mountain View, California, y Austin, Texas.<sup>12</sup> Menos deslumbrantes tecnológicamente pero igualmente disruptivos (y mucho más maduros) son los servicios de autos compartidos y de viajes compartidos: El movimiento que comenzó con el Zipcar últimamente ha engendrado los conceptos de viajes compartidos de Uber y Lyft; Sólo Uber genera un millón de viajes por día en todo el mundo<sup>13</sup> y está creciendo rápidamente.

Sin embargo, puede que estas tecnologías que redefinen la industria no alcancen a llegar a una escala de transformación total, o al menos que no lo hagan dentro de un tiempo que sea estratégicamente relevante. La industria actual, que ha hecho una gran inversión en mantener el estado actual, opina

que el cambio evolucionará lentamente hacia un futuro que estará basado en lo que existe actualmente.

Vemos a las empresas automotrices más importantes seguir estrategias que se ocupan de modo incremental de las fuerzas convergentes, creando opciones de valor en el futuro al mismo tiempo que preservan la flexibilidad. Estos esfuerzos e inversiones por parte de los jugadores de la industria ya están produciendo un flujo continuo de beneficios para los clientes. Por ejemplo, al incluir tecnología de autos conectados, los fabricantes ofrecen a los conductores muchos de los beneficios asociados con la conducción autónoma sin alterar fundamentalmente la forma en la que los humanos interactuamos con los vehículos.

Los fabricantes de autos están experimentando e inventando, y existen voces apasionadas dentro de sus equipos que describen futuros con grandes cambios. La mayoría han abierto oficinas en Silicon Valley para estar más cerca del desarrollo tecnológico y la financiación temprana. Dentro de los ejemplos más notables de iniciativas orientadas al futuro son los 25 proyectos de movilidad Ford,<sup>14</sup> los iVentures de BMW,<sup>15</sup> los avances de ingeniería de Daimler en el campo de la conducción inteligente,<sup>16</sup> y la funcionalidad “Super Cruise” de Cadillac.<sup>17</sup> Además, sociedades estatales-privadas como la recientemente inaugurada Mcity en Ann

Arbor, Michigan, brindan una plataforma para permitir pruebas más eficientes y efectivas de vehículos (y funciones) automáticos.<sup>18</sup>

Este enfoque es consistente con las normas históricas, en las que los fabricantes de autos invierten en nuevas tecnologías, como por ejemplo frenos antibloqueantes, control de estabilidad electrónico, cámaras de retroceso, y telemática. Todas estas tecnologías fueron adoptadas en principio por vehículos de alta gama y luego fueron incluyéndose en modelos más económicos, a medida que de afianzaba la economía de escala.<sup>19</sup> En nuestras continuas conversaciones con líderes de la industria automotriz, ellos postularon repetida y colectivamente que aquellos ajenos a la industria no comprenden la enorme complejidad de desarrollar un vehículo hoy en día, el desafío de incluir tecnologías de avanzada en la arquitectura de un vehículo, o el rigor y la inercia de las regulaciones. Todo esto alienta a las empresas dominantes a creer que podrán gestionar activamente los tiempos y el ritmo de estas fuerzas convergentes.

Pero puede que la interacción de las fuerzas convergentes del cambio sea menos predecible, y que ocasione trastornos más rápido de lo que ellos creen. Puede que los fabricantes de autos estén sobreestimando el poder que tendrán para influir en los eventos futuros.

# Cuatro futuros a la vez

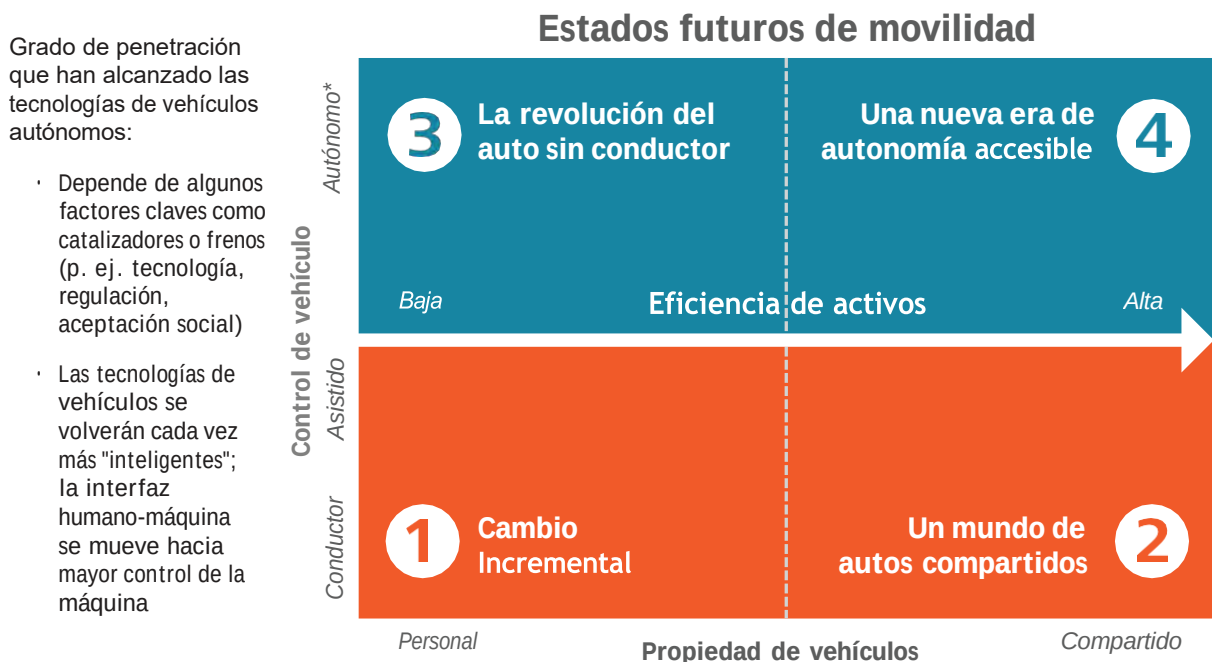
**C**oNsideraNdO la disparidad de fuerzas que configuran el paisaje, imaginamos cuatro futuros diferentes de movilidad personal que surgirán de la intersección de dos tendencias fundamentales (ver Cuadro 4):

- Control vehicular (conductor versus autónomo)

- Propiedad (personal versus compartida)

Nuestro análisis concluye que el cambio sucederá de forma irregular en todo el mundo, con diferentes poblaciones requiriendo diferentes modos de transporte, lo que significa que los cuatro estados futuros bien pueden existir de modo *simultáneo*. En otras palabras,

**Cuadro 4. Cuatro estados futuros potenciales**



Grado en el que los vehículos son de propiedad personal o compartidos:

- Depende de las preferencias personales y la economía
- Un grado más alto de propiedad compartida aumenta la eficiencia sistemática de los activos

Nota: Conducción completamente automática significa que la Unidad Central de Procesamiento del vehículo tiene responsabilidad total de control sobre su operación, y es inherentemente diferente de las formas más avanzadas de asistencia de conducción. Está demarcada en el cuadro anterior con una clara línea divisoria (un "ecuador").



los líderes de negocios deberán preparar sus organizaciones para ser capaces de operar en cuatro futuros diferentes, con distintos grupos de clientes, algunos de ellos de edades tan tempranas como 5-15 años. Aquí ofrecemos una descripción de alto nivel de cada estado futuro y las condiciones que promueven su eventual aparición.

## Estado futuro 1: Cambio incremental

La visión más conservadora del futuro da gran importancia a los grandes activos inmersos en el sistema actual, y presupone que los dueños de esos activos no los van a abandonar voluntariamente, ni tampoco van a transferir capital a las nuevas empresas con resultados inciertos. Esta visión sostiene que la propiedad personal continuará siendo la norma, y los consumidores optarán por tener la privacidad, flexibilidad, seguridad, y conveniencia que les da ser los dueños de vehículos. Es importante destacar que esta visión presupone que la conducción completamente autónoma no estará disponible para todos en un futuro cercano, aunque se puedan ir incorporando tecnologías de asistencia de conducción.

Al predecir tan poco cambio, este estado futuro refuerza la confianza de los fabricantes de autos en un modelo de negocios que prioriza las ventas de vehículos. Continúan invirtiendo en el desarrollo y presentación de nuevas líneas de vehículos con tecnologías avanzadas, y los concesionarios siguen a cargo de la responsabilidad de la experiencia de cliente. Otros jugadores de la industria tienen similares incentivos para confiar en las prácticas y estructuras arraigadas hace décadas.

## Estado futuro 2: Un mundo en el que se comparten los autos

El segundo estado futuro supone el crecimiento continuo de los servicios en los que se comparte el acceso a los vehículos.<sup>20</sup> En este estado, la escala económica y la mayor

competencia impulsan la expansión de tales servicios a nuevos territorios y segmentos de clientes más especializados. En este modelo, los pasajeros valoran fuertemente la conveniencia del transporte punto-a-punto que han creado estos servicios de vehículos y viajes compartidos, porque les ahorran el engorro de navegar por el tránsito y encontrar estacionamiento. Además, el sistema ofrece opciones para los que no conducen, p. ej. los jubilados, familias de bajos ingresos, y menores de edad sin registro.

En este estado futuro, al bajar el costo por milla algunos ven los vehículos compartidos como una forma de transporte más económica, conveniente, y sustentable, especialmente para movimientos cortos de punto-a-punto (ver nuestro análisis a continuación sobre los factores económicos de la movilidad). Al satisfacer los servicios de vehículos compartidos una proporción cada vez mayor de las necesidades locales de transporte, los hogares que los han adoptado pueden reducir el número de autos que tienen, mientras que otros pueden abandonar la propiedad completamente, lo que a su vez reduce la demanda futura.

## Estado futuro 3: La revolución de los autos sin conductor

El tercer estado es el que la tecnología de conducción autónoma demuestra ser viable, segura, conveniente, y económica; aun así la propiedad personal continúa siendo la norma. La colaboración entre destacados académicos, agencias regulatorias, y empresas acelera el progreso hacia este futuro.<sup>21</sup> Tanto las empresas de tecnología como las automotrices continúan invirtiendo fuertemente para aumentar las capacidades “V2X” (V2V y V2I). A la vez, madura la tecnología de autos sin conductor, y el éxito de los primeros pilotos fomenta su rápida popularización.

Este estado futuro presupone que la mayoría de los conductores preferirá ser los dueños de sus propios vehículos. Las personas buscarán tener la funcionalidad “sin conductor” por seguridad y otros beneficios potenciales, pero continuarán siendo dueños por muchas de



las mismas razones anteriores a esta nueva tecnología. Incluso puede que inviertan más en sus vehículos en caso de que comience una nueva era de personalización, y sea atractivo utilizar vehículos adaptados a ocasiones y circunstancias específicas.<sup>22</sup> Sin embargo, las prestaciones en las que los dueños quieran invertir pueden cambiar, como también pueden cambiar los diseños de los vehículos mismos. Puede que este nuevo segmento del mercado ofrezca vehículos más livianos y técnicamente avanzados, que adopten principios de diseño muy diferentes del actual, en el que hay cuatro puertas y el conductor está adelante a la izquierda aferrado al volante.

#### Estado futuro 4: Una nueva era de autonomía accesible

El cuarto estado anticipa una convergencia de dos tendencias: la de conducción autónoma y de servicios de vehículos compartidos. En este futuro, las empresas de gestión de movilidad ofrecen una gama de experiencias de pasajeros para satisfacer diferentes necesidades, a precios diferenciados.<sup>23</sup> Los que adopten este modelo primero y con más ansias serán aparentemente los que viven en las afueras y viajan al centro

para trabajar todos los días, dado que los vehículos altamente automatizados tienen potencial para hacer estos viajes más rápidamente y con distancias reducidas, además de que las rutas se verán mejoradas por el conocimiento en tiempo real de las condiciones de tránsito. Con el tiempo, se expandirá una infraestructura inteligente, y la utilización de conductores llegará a un punto de inflexión, y flotas de vehículos autónomos de propiedad compartida harán el trayecto de centros urbanos a suburbios densamente poblados, y más allá.

Las avanzadas tecnologías de comunicación coordinarán la experiencia de movilidad punto-a-punto del cliente: Las interfaces intuitivas le permitirán a los usuarios encargar que los busque un vehículo en pocos minutos, y los lleve del punto A al B de forma eficiente, segura, y costo-efectiva. Los que podrán tener mayores oportunidades para monetizar el valor de la atención de los pasajeros en tránsito (además de metadatos relacionados con la utilización del sistema) son los operadores de sistemas de redes de tráfico vehicular, los proveedores de contenido y experiencias dentro del vehículo (p. ej. firmas de software e información y entretenimiento), y los dueños de datos (p. ej. empresas de telecomunicaciones).



# ¿Cuánto por kilómetro?

**H**emos hecho un análisis para calcular el costo promedio por kilómetro en cada uno de estos cuatro escenarios; este análisis muestra que los consumidores podrían beneficiarse de costos más bajos por kilómetro en los estados 2, 3, y 4 (el Cuadro 5 tiene un resumen de estos costos por escenario, y el Cuadro 6 tiene un desglose más detallado de los costos asociados).

De acuerdo con nuestros cálculos, los vehículos de propiedad personal actualmente tienen costos de aproximadamente \$0,60 por kilómetro. Esto incluye la depreciación del vehículo, la financiación, el seguro, el combustible, y el valor individual del tiempo del conductor. Al ajustar estas variables clave en cada estado futuro, hemos desarrollado un análisis

**Cuadro 5. Resumen de cálculos de costo por milla para cada estado futuro**



Fuente: Análisis de Deloitte, basado en información disponible públicamente (US DOT, AAA, etc.)

Nota: Conducción completamente automática significa que la Unidad Central de Procesamiento del vehículo tiene responsabilidad total de

control sobre su operación, y es inherentemente diferente de las formas más avanzadas de asistencia de conducción. Está demarcada en el cuadro anterior con una clara línea divisoria (un "ecuador").

Gráfico: Deloitte University Press | DUPress.com

Cuadro 6. Desglose del costo por milla para cada estado futuro

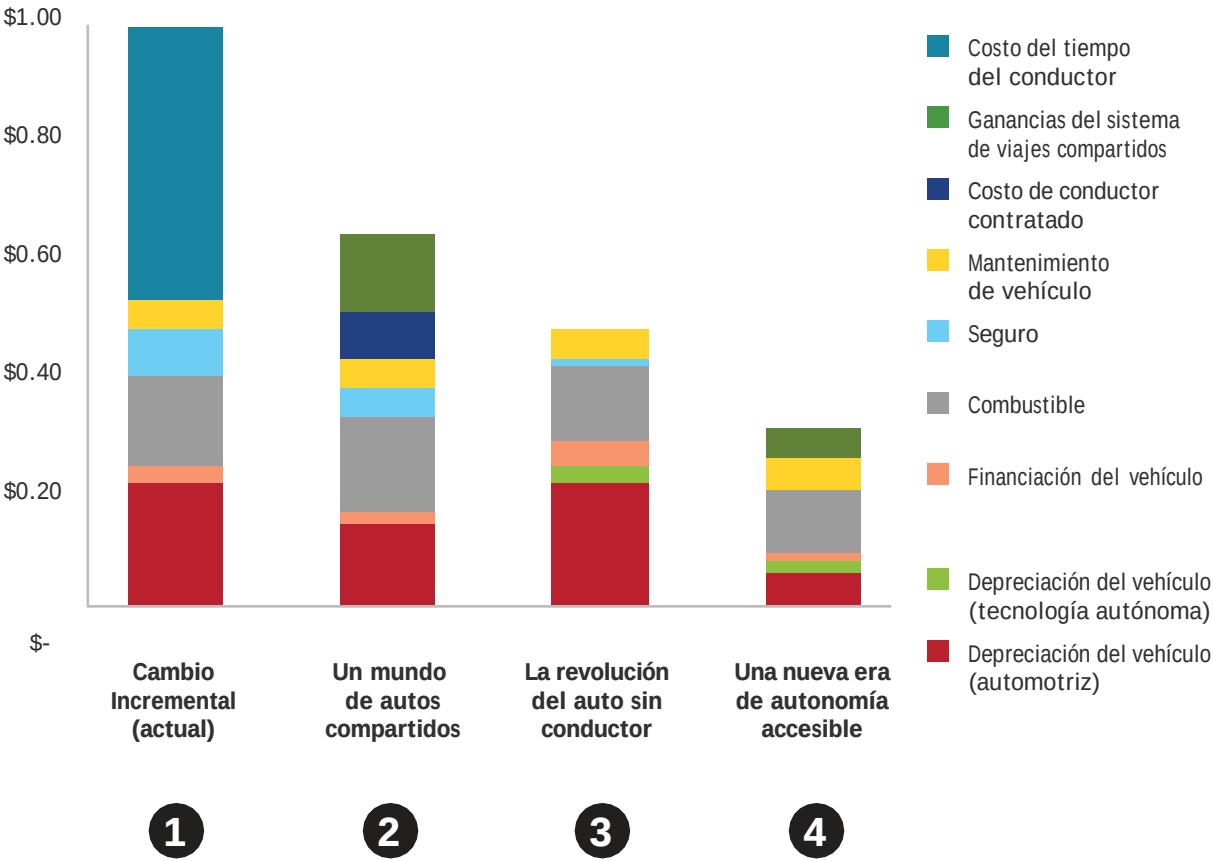


Gráfico: Deloitte University Press | DUPress.com

direcciona de alto nivel de costos estimados por kilómetro de cada escenario futuro en su madurez.

Nuestras proyecciones indican que en el futuro estado 2 de movilidad compartida, la economía se vuelve más favorable en comparación con la propiedad individual de vehículos, a causa de mayor utilización de bienes y menor tiempo del consumidor empleado en conducción. Con el tiempo, la eficiencia de la mayor utilización de bienes compensa los mayores costos asociados con la contratación de un conductor. Nuestro análisis sugiere que un modelo de servicios de vehículos compartidos a escala completa costaría aproximadamente \$0,40 por kilómetro.

Si los vehículos de conducción autónoma de propiedad personal fueran ampliamente adoptados (estado futuro 3), la proyección de costo por kilómetro se vuelve más difícil, dado que los cálculos dependen de las suposiciones

acerca del valor de reasignar el tiempo y la productividad del conductor. Basándonos en estimados conservadores sobre el valor de este tiempo, el estado futuro 3 costaría aproximadamente \$0,28 por kilómetro.<sup>24</sup>

Y en un mundo de vehículos compartidos con conducción autónoma (estado futuro 4), nuestro análisis concluye que la economía sería altamente favorable: El costo por kilómetro bajaría tanto como \$0,19 por viajes de una sola persona. En otras palabras, bajaría unos dos tercios con respecto al costo de conducir hoy en día. Este ahorro proviene parcialmente de suposiciones clave que giran alrededor de la disponibilidad de vehículos más livianos (por ejemplo, módulos para dos personas con un precio tan bajo como \$10.000), lo que reduciría los costos de capital; altas tasas de utilización de bienes (mucho más altas que el 4% actual), y el valor puesto en liberar tiempo de conducción para propósitos más productivos.



# El camino del cambio

**C**reemos que los cambios al estado actual de movilidad ocurrirán más rápidamente hacia el escenario de acceso compartido, lo que a su vez catalizará la (creciente) adopción de la conducción autónoma. Vemos que esta progresión ocurrirá en una serie de pasos, como se ve en el Cuadro 7.

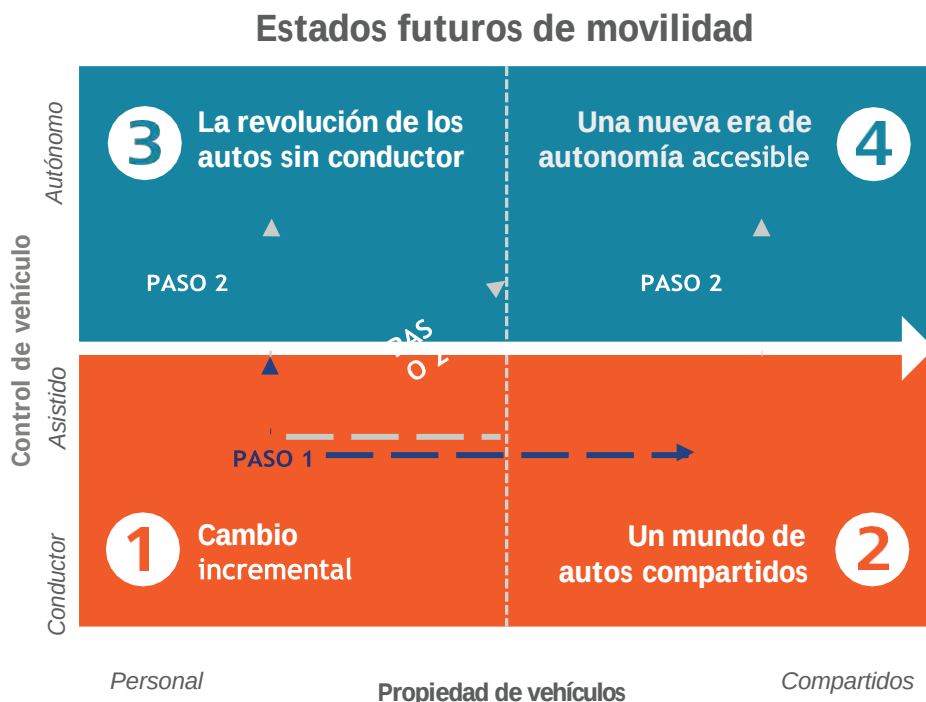
## Paso 1: Adopción gradual de acceso compartido

El cambio de propiedad personal pura de vehículos a un sistema que se basa más en acceso compartido (es decir, del cuadrante 1 al

**Cuadro 7. El camino del cambio**

Grado de penetración que han alcanzado las tecnologías de vehículos autónomos:

- Depende de algunos factores claves como catalizadores o frenos (p. ej. tecnología, regulación, aceptación social)
- Las tecnologías de vehículos se volverán cada vez más "inteligentes"; la interfaz humano-máquina se mueve hacia mayor control de la máquina



Grado en el que los vehículos son de propiedad personal o compartidos:

- Depende de las preferencias personales y la economía
- Un grado más alto de propiedad compartida aumenta la eficiencia sistemática de los activos.

Nota: Conducción completamente automática significa que la Unidad Central de Procesamiento del vehículo tiene responsabilidad total de control sobre su operación, y es inherentemente diferente de las formas más avanzadas de asistencia de conducción. Está demarcada en el cuadro anterior con una clara línea divisoria (un "ecuador").



cuadrante 2 del cuadro 7), ya está ocurriendo en algunas partes de EEUU. Algunos servicios de autos compartidos como por ejemplo Zipcar han duplicado su base de clientes en los últimos seis años,<sup>25</sup> mientras que los servicios de viajes compartidos como Uber han estado sumando 50.000 conductores por mes, y han llegado a 140 millones de viajes en todo el mundo sólo en 2014.<sup>26</sup> Los sistemas de software y hardware que utilizan estos servicios para conectar a los conductores con sus pasajeros están evolucionando rápidamente, incorporando información sobre comportamientos observados para mejorar las experiencias de tanto los conductores como sus pasajeros.<sup>27</sup> Además, la intensa competencia puede bajar los precios del mercado, al afianzarse las mejoras económicas relacionadas con la mayor utilización de bienes.

## Paso 2: El punto de inflexión hacia un escenario sin conductor

Actualmente, la aceptación generalizada de la conducción autónoma parece estar más lejos en el futuro que una cultura popular de vehículos y viajes compartidos.<sup>28</sup> Algunas de las fuentes de demora son la necesidad de resolver las limitaciones tecnológicas existentes, como por ejemplo que los sensores funcionen en cualquier condición climática, y la amplia disponibilidad de mapas 3D, y también resolver temas de ciberseguridad y responsabilidad civil.<sup>29</sup> La velocidad con la que se resolverán estos y otros problemas será un factor determinante en el grado de adopción de la conducción autónoma.

Las empresas automotrices, tanto en sociedad como en competencia con las empresas de tecnología, están siguiendo un camino de cambio de control, de conducción sólo humana a conducción asistida, a conducción autónoma. Si la conducción autónoma fuera el único vector de cambio, la aceptación quizás crecería gradualmente, siguiendo el patrón de adopción que ya es clásico en la industria automotriz. En nuestra opinión, ese es el camino del cuadrante 1 al cuadrante 3, cambio incremental a la revolución de la conducción autónoma, que ya está ocurriendo.

Sin embargo, también vemos que el cambio va por un segundo carril, un vector paralelo con dirección norte: de un mundo de autos compartidos hacia una nueva era de autonomía accesible. En este camino, también está en curso un impulso adicional hacia la conducción autónoma. Recientemente, Uber se asoció con la Universidad Carnegie Mellon y la Universidad de Arizona para inaugurar un Centro de Tecnologías Avanzadas en Pittsburgh, y testear autos de conducción autónoma y óptica para tecnologías de mapeado.<sup>30</sup> Los servicios de viajes compartidos tienen incentivos económicos para acelerar la adopción de vehículos autónomos, dado que podría reducir uno de los mayores costos operativos del sistema: el conductor. Estas empresas podrían capturar una porción significativa del valor de superávit del consumidor mediante la reducción de este costo. Si la conducción autónoma es viable para los servicios de viajes compartidos, esto podría acelerar drásticamente su popularización, al tener los consumidores mayores oportunidades para experimentar la tecnología, y al mismo tiempo implementar reducciones significativas en el costo de la movilidad personal.

Finalmente, otros jugadores de alta tecnología están emprendiendo el camino hacia la conducción autónoma. Por ejemplo, el programa de autos autónomos de Google está evaluando autos que no confían en la progresión de asistencia al conductor, sino que inmediatamente hacen el salto a completamente autónomos; Google ha expresado públicamente que “sacar al conductor de la ecuación” es el camino más seguro.<sup>31</sup> Y a largo plazo, todavía no está claro si la intención de Google es elegir entre la movilidad autónoma compartida, la propiedad personal, o ambas.

Antes que seguir el patrón histórico de innovación tecnológica, la conducción autónoma, cuando llegue, podría ser un cambio radical. Y los cambios resultantes al ecosistema de movilidad personal podrían desplegarse mucho más rápido que lo que muchas de las empresas más grandes podrían imaginar. (Ver “Fuerzas de demora o aceleración.”)





## FUERZAS DE DEMORA - O ACELERACIÓN

Las fuerzas inerciales que demoran el proceso que Joseph Schumpeter llamó “destrucción creativa”<sup>32</sup> en el campo de la movilidad personal no deben ser subestimadas. El cuadro siguiente resume los principales impulsores que podrían demorar o acelerar significativamente la adopción de las nuevas tecnologías.

| Fuerzas de demora o aceleración  | Cambios y/o impactos                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Regulación y gobierno            | <ul style="list-style-type: none"> <li>Legislación y regulación global, federal, estatal y local.</li> <li>Impuestos e ingresos</li> <li>Leyes que rigen la captación, utilización, almacenamiento, y la transferencia de datos</li> </ul>                                                                                                                                     |
| Actitudes sociales               | <ul style="list-style-type: none"> <li>Prejuicios sobre el rol de la interfaz humano-máquina, ideas que vienen desde hace mucho sobre propiedad de vehículos y su uso, etc.</li> <li>Seguridad</li> <li>Crecimiento continuado de la economía de compartir</li> </ul>                                                                                                          |
| Desarrollo tecnológico           | <ul style="list-style-type: none"> <li>Resultados de experimentos previos y programas piloto</li> <li>Surgimiento de innovaciones o descubrimientos tecnológicos</li> </ul>                                                                                                                                                                                                    |
| Privacidad y seguridad           | <ul style="list-style-type: none"> <li>Estándares y protocolos de ciber-seguridad y comunicación</li> <li>Protección de la información de identificación personal</li> </ul>                                                                                                                                                                                                   |
| Bolsas y Mercados                | <ul style="list-style-type: none"> <li>Tasaciones corporativas</li> <li>Disponibilidad de capital para invertir</li> <li>Nivel de inversión (tecnología, presentación al mercado, etc.)</li> </ul>                                                                                                                                                                             |
| Impacto a las partes interesadas | <ul style="list-style-type: none"> <li>Cambios potenciales a modelos de empleo actuales, incluyendo efectos de desplazamiento, costos, y gestión de cambio</li> <li>Oportunidades de mayor empleo futuro (tipo y tamaño)</li> <li>Reacciones de las partes interesadas y próximos pasos (p. ej. trabajadores, gremios, concesionarios, empleadores, gobierno, etc.)</li> </ul> |

# El futuro para la industria automotriz extendida

**E**l reciente informe de *Tendencias de Negocios* de Deloitte “Los Ecosistemas de Negocios Alcanzan la Madurez”<sup>33</sup> describe un patrón general en el que muchas de las industrias que componen la economía global están experimentando un tipo de metamorfosis. Lo que heredamos del siglo 20, son “industrias estrictamente definidas creadas en torno a grandes corporaciones, integradas verticalmente, y sobre todo “autónomas”. Pero en los últimos años, en gran medida gracias a las tecnologías digitales, estos gigantes se han desintegrado en negocios independientes, tremendamente enfocados, y altamente interconectados, muchos de los cuales desempeñan sus funciones especializadas cruzando las antiguas fronteras de las industrias. Nosotros opinamos que “Las fronteras fundamentales que definían las relaciones, interacciones, y posibilidades de la mayoría de los negocios están esfumándose y disolviéndose con rapidez.”<sup>34</sup> Todavía existen las necesidades humanas básicas que motivaron la creación de esas industrias, pero actualmente se las satisface mediante ecosistemas mucho más fluidos. En el futuro sistema de movilidad, todavía existen las necesidades de movilidad que motivaron la creación de esas industrias, pero probablemente surgirán ecosistemas mucho más fluidos para satisfacerlas. Y esto presagia que el cambio significativo a los modelos de negocios actuales, y las sociedades (p. ej. entre la industria y los disruptores) serán de importancia fundamental para crear una nueva movilidad.

Un análisis complementario del Center for the Edge de Deloitte sostiene que un nuevo ecosistema de movilidad podría generar una cadena de valor “virtual” en la que la capacidad de capturar, agregar, y analizar datos relacionados a la movilidad serán una fenomenal fuente de valor. En esta visión, el valor aumentará para los que:

1. Proporcionen movilidad continua de punto a punto
2. Gestionen el sistema operativo de redes de movilidad
3. Creen y gestionen la experiencia de dentro del vehículo de forma holística

Podrá haber grandes recompensas para los jugadores que sean capaces de capturar, analizar, y monetizar (con seguridad) el conocimiento de dónde viaja la gente, las rutas que utilizan para llegar, y qué hacen durante el trayecto. Mientras que habrá terceros que sin dudas paguen por acceder a esta información, probablemente el mayor valor será de los nuevos jugadores en el mercado que surjan como “consultores confiables”, y que nos ayudarán a todos nosotros a navegar el nuevo ecosistema y a incrementar nuestro “rendimiento de movilidad”. Puede que estas empresas también permitan al ecosistema monetizar nuevos servicios y modelos de propiedad.



El sistema futuro de movilidad también necesitará empresas para desarrollar y gestionar el sistema de información de redes de tránsito y operación de vehículos que ayuda a dirigir y controlar el movimiento de los vehículos autónomos y flotas de movilidad compartida. Las empresas de tecnología todavía tienen acceso a información sobre pasajeros e intentarán capturar este valor, pero probablemente tengan que enfrentar desafíos con los nuevos jugadores con nuevos modelos de negocios.<sup>35</sup> Los fabricantes de vehículos podrían desarrollar vehículos no para satisfacer a los conductores sino para enfocarse en la experiencia de los pasajeros, lo que potencialmente facilitaría la aparición de nuevas estructuras y formas de vehículos.

Mientras tanto, es razonable anticipar una saludable tensión entre las automotrices, altamente atadas al sistema actual centrado en el producto, y los innovadores tecnológicos que buscan un nuevo mundo virtual de opciones de movilidad.<sup>36</sup> Y en este caso, dado que los autos de propiedad compartida podrían hacer que disminuyan las ventas totales de autos, las automotrices podrían ser reticentes a aceptar esa visión.

Pero casi no quedan dudas de que surgirá alguna versión, o quizás múltiples versiones, de un nuevo ecosistema, basado en acceso compartido y conducción autónoma. En el momento y en el lugar que ocurran, puede que el cambio sea profundo: menor costo por kilómetro, mayor seguridad, menor necesidad de estacionamientos y control de las normas de tránsito, impacto ambiental significativamente menor, y más. Hay preguntas sobre qué va a pasar con el sector automotriz actual, y cómo afectará todo esto a los Fabricantes de Equipos Originales, proveedores, concesionarios, empresas petroleras, minoristas de combustible, servicios de post-venta y autopartistas, compañías de seguros, estacionamiento público y privado, cumplimiento de normas de tránsito, y otros. Sin importar de qué manera ocurran las fuerzas de cambio, cada empresa deberá determinar, en palabras de Roger Martin, "dónde jugar y cómo ganar."<sup>37</sup>

A continuación veremos una reseña inicial de la enorme magnitud del cambio que podrá afectar a las principales partes interesadas en el sistema actual, además del nuevo ecosistema de movilidad.

### **Los Fabricantes Automotrices**

**Globales** deberán tomar decisiones difíciles y trascendentes. La industria automotriz está actualmente luchando contra los factores económicos fundamentales de un negocio intensamente competitivo con enormes exigencias de capital; los márgenes operativos y la rentabilidad se mantienen bajos.<sup>38</sup> La industria está operando con un considerable exceso de capacidad productiva. Globalmente, es posible producir 113 millones de vehículos anualmente, mientras que las ventas se mantienen alrededor de los 70 millones.<sup>39</sup> Además, las exigencias regulatorias (como CAFE, vehículos de emisión cero, y estándares de seguridad) son cada vez más estrictos y caros.<sup>40</sup> Y los consumidores demandan constantemente las últimas tecnologías.

Los Fabricantes deberán decidir si quieren evolucionar de ser un negocio de producción de capital (relativamente) fijo, de primera transacción y venta de productos, a un negocio centrado en ser un proveedor de servicios de movilidad de punto a punto. Esto representaría un profundo cambio de modelo de negocios, y el desarrollo de capacidades completamente nuevas para poder ser viables, competitivos, y sustentables.

Como mínimo, deberán sopesar cómo satisfacer las necesidades de un mercado cambiante en el que los consumidores utilizan movilidad compartida cada vez más, y se interesan por vehículos de conducción autónoma, propiedad personal, y altamente personalizados.<sup>41</sup> Puede que esto requiera innovación, transformación del desarrollo de productos, y reconfiguración de las cadenas de suministro y los sistemas operativos de producción para que sean cada vez más eficiente, flexible, y que permita la personalización.

Al mismo tiempo, los consumidores podrían comenzar a pedir vehículos autónomos compartidos para diferentes tipos de viaje, lo que puede llevar a la creación de tipos de

vehículo más variados. Esto podría llevar al desarrollo de proyectos de vehículos de alta velocidad y bajo costo, para crear y producir vehículos con marcos livianos, software personalizado y enfocado en la experiencia, e interiores altamente personalizados y con elementos de diseño. Pueden fabricarse vehículos livianos de conducción autónoma para utilizar la energía de modo altamente eficiente y con mayor autonomía de manejo. Esto puede hacer que los vehículos eléctricos sean más viables, y ayudar a las automotrices a cumplir con las estrictas normas regulatorias.

**Los proveedores de las automotrices** deberán adaptarse a medida que estas se transformen. A medida que crezcan las ventas de los vehículos de conducción autónoma, los proveedores necesitarán que sus operaciones sean eficientes y ágiles para poder satisfacer las demandas altamente variables del mercado de vehículos de propiedad personal. Aunque puede que la mayoría de los principales sistemas de dirección, chasis, frenos, y componentes eléctricos sea standard, lo que le dará a los proveedores algunos beneficios de escala operativa, es probable que el packaging de los vehículos de propiedad personal sea personalizado. La construcción de vehículos más estandarizados (necesarios para la ofrecer soluciones de movilidad compartida) podría significar grandes volúmenes, y la demanda probablemente pase por productos menos complejos y de menor valor agregado. Por lo tanto, la economía en este nuevo mercado favorecerá fuertemente a los productores de menor costo.

**Las firmas de tecnología** son las que impulsan gran parte del cambio que está sucediendo. Anteriormente nos referimos a estas empresas como disruptoras; su visión estratégica es que derribar antiguas estructuras y marcos institucionales puede generar muchísimo valor. A diferencia de los fabricantes y los dueños de bienes en el sistema actual, tienen pocos intereses creados en el ecosistema automotriz actual, y ven el mercado de la movilidad como una nueva frontera. Comparten la convicción de que la fuente

dominante de valor en el sistema puede ser la creación y gestión del sistema operativo y la experiencia de tránsito, además de minar los datos que se generen.

Estas empresas han demostrado ser expertas en la creación de redes de información y sistemas operativos grandes y complejos, la utilización de inteligencia artificial para minimizar el error humano y el azar, la creación de entornos atractivos que impulsen la conducta del consumidor, y la creación de comunidades digitales. Ven al vehículo como otra plataforma en un mundo con múltiples dispositivos. Los sensores de vehículos y los dispositivos personales podrían generar cantidades de datos cada vez mayores, cuya comprensión podría producir una experiencia de cliente y servicios personalizados.<sup>42</sup> Los sistemas de información integrada pueden permitir el transporte intermodal. Y los sistemas móviles, inalámbricos, basados en la ubicación pueden crear nuevas oportunidades para que los modelos de precio dinámico, pago único, y basados en el consumo se popularicen. Los líderes tecnológicos en general, en comparación con los líderes tradicionales de la industria automotriz, están en posiciones altamente ventajosas para capturar esta información y valor virtual.

**La entrega de carga y el transporte de camiones de larga distancia** actualmente enfrentan desafíos significativos que el ecosistema futuro de movilidad podrían aliviar. En la versión más ambiciosa del futuro, el transporte de cargas y los sistemas de suministro podrían ser principalmente autónomos mediante una conexión en cadena u operación remota; un escenario atractivo, considerando que la industria de camiones en EEUU tiene cada vez menos trabajadores: actualmente hay unos 30.000 puestos de trabajo disponibles y una tasa de rotación del 92%.<sup>43</sup> Los vehículos autónomos ofrecen una manera de superar las restricciones de horas manejadas, y aumentar la capitalización. Dado que los ingresos anuales del transporte de larga distancia son \$700 mil millones,<sup>44</sup> las principales flotas, como UPS y USPS, tienen

un importante incentivo económico para explorar activamente cómo operar durante períodos más prolongados, cubrir distancias más largas sin paradas, y reducir el costo de los conductores (actualmente el 26% de los costos operativos).<sup>45</sup> Con cifras tan contundentes, este sector podría convertirse en uno de los primeros campo de prueba para las tecnologías de conducción autónoma.

**Los aseguradores** deberán responder una serie de preguntas complejas y estratégicas sobre cómo van a ocuparse de los diferentes segmentos, geografías, y grupos demográficos dependiendo qué estados futuros ocurran.

Las apuestas son altas, con más de \$205 mil millones en responsabilidad personal, choque, y seguro contra todo riesgo. Al operar dentro en un mercado altamente regulado, los aseguradores deberán continuar apoyando el modelo de seguros clásico, en el que los accidentes suelen ser a causa de error del conductor, pero al mismo tiempo adaptarse a un mundo de conducción automática en el que el riesgo es más técnico y relacionado a una falla en el sistema de auto-guía. Al cambiar la composición demográfica de los factores de riesgo, también cambiarán las estructuras de costo. Otra posibilidad es que el flujo de nueva información proporcionada por vehículos conectados ofrezca la posibilidad de evaluar el riesgo de manera más exacta.

**El sector público de EEUU** probablemente deba determinar de qué modo compensar los \$251 mil millones anuales que generan los impuestos al combustible, tarifas de transporte público, peajes, impuestos de ventas de vehículos, estacionamiento municipal, e ingresos por registro y licencia; se prevé que esta cifra disminuya. Todos esos ingresos están atados a la realidad actual de vehículos de

propiedad personal y operados por individuos: por ejemplo, la necesidad de tener estacionamientos disminuye con el advenimiento de la movilidad compartida y la conducción autónoma. Puede que las agencias deban evaluar alternativas, p. ej. cobrar impuestos por “movimiento” y no por propiedad.

En el futuro, la monetización del uso de los caminos podría llevar a un modelo mucho más dinámico basado en la hora del día, la demanda de mercado, las rutas utilizadas, la distancia, y la forma del vehículo; esto vincularía la utilización de bienes públicos más directamente que el sistema actual. Por otra parte, al disminuir el volumen de vehículos, puede que las municipalidades vean menor desgaste de su infraestructura, y tengan la oportunidad de reasignar el espacio de estacionamiento (y otros) para propósitos que les den más valor. Los costos del gobierno (como el Registro Automotor) podrían bajar significativamente y potencialmente compensar algo de la baja de ingresos del sector público.

Los cambios de valor para esta y otras industrias podrían tener un impacto tremendo en los ingresos de todo el ecosistema.

El Cuadro 8 resume algunos de los efectos posibles que tendría el cambio en el futuro ecosistema de movilidad. El gráfico también incluye los posibles beneficios sociales que se esperan como resultado de la conducción autónoma y de los avances tecnológicos de la movilidad compartida. El análisis todavía no da cuenta de nuevos modelos de negocios que podrían evolucionar dentro del ecosistema futuro; simplemente intenta ilustrar los efectos potenciales y el impacto direccional que los vehículos autónomos y la movilidad compartida podrían tener en el ecosistema actual.

Cuadro 8. Cambios posibles de valor



|                             |                                                                     |                                     |                                                         |
|-----------------------------|---------------------------------------------------------------------|-------------------------------------|---------------------------------------------------------|
| Beneficios para la sociedad | 40%–90%<br>disminución de emisiones de los automóviles <sup>a</sup> | 32K+<br>vidas salvadas <sup>b</sup> | 100B horas<br>de productividad recuperadas <sup>c</sup> |
|-----------------------------|---------------------------------------------------------------------|-------------------------------------|---------------------------------------------------------|

<sup>a</sup> Análisis de Deloitte; la disminución anual de porcentaje se calcula con anterioridad a cualquier cambio de mezcla de combustible, y es equivalente a una disminución de 10% a 25% de las emisiones totales de EEUU.

<sup>b</sup> Las cifras de 2013 son sólo para EEUU; la cifra global es 1.24 millones anuales (OMS).

<sup>c</sup> Análisis de Deloitte basado en millas que se manejaron en EEUU en 2014 (DOT) y la velocidad promedio de viaje en millas por hora (Universidad de Columbia).

Fuente: Análisis de Deloitte.

Gráfico: Deloitte University Press | DUPress.com



# Conclusiones

**E**N los cuatro escenarios futuros posibles del ecosistema de movilidad, las fuentes de valor cambian profundamente. Dado que esta evolución está formando un nuevo ecosistema, queremos compartir con ustedes algunas reflexiones de las implicancias estratégicas y operativas para las empresas históricamente dominantes, los participantes de la industria extendida, y los disruptores, al analizar todos ellos su futura dirección. Específicamente:

1. **Las industrias se levantan y caen.** Los ciclos tardan mucho tiempo en completarse, pero finalmente el cambio ocurre.
2. **Los posibles beneficios al sistema, y los fundamentos económicos de la visión disruptora son muy convincentes.**
3. **Existe un camino para que la industria automotriz actual sea líder en la transición hacia el futuro de la movilidad personal, pero requerirá un cambio de modelo fundamental y expeditivo.** Será necesario crear capacidades nuevas y diferentes para competir eficazmente en el ecosistema de movilidad futuro. Todos en el sector automotriz extendido actual deben reevaluar cómo operarán y crearán valor durante la existencia de los cuatro estados, y en el largo plazo, cuando la movilidad autónoma y compartida sea más predominante.
4. **Los conocedores de la industria y los disruptores se necesitan mutuamente.** Sin duda alguna, será la competencia feroz lo que caracterice este panorama comercial de movilidad personal. Pero a pesar de su recelo y sus diferentes visiones y perspectivas, los líderes actuales de la industria automotriz y los nuevos jugadores formarán un nuevo ecosistema con altos niveles de interdependencia, prestaciones mutuas, y simbiosis.
5. **La profunda disrupción se extenderá mucho más allá de la industria automotriz.** Cada aspecto de la economía moderna basado en la suposición de que los vehículos son conducidos por humanos y de propiedad personal será cuestionado. Cada empresa en este nuevo ecosistema deberá decidir dónde jugar y cómo ganar. Como siempre durante las transformaciones a gran escala, podemos esperar el surgimiento de nuevos jugadores, con capacidades diferenciadas, que cambiarán la dinámica fundamental de dónde y cómo se crea el valor. Finalmente será el mercado, en su incesante búsqueda de mejores resultados a menores costos, quien decida quién gana y quién pierde.

*Deloitte seguirá compartiendo, de modo periódico, reflexiones sobre esta evolución como parte de una serie continua. Nuestro propósito es contribuir al diálogo al mismo tiempo que lidiamos con el impacto y las consecuencias del futuro de la movilidad. Nuestro objetivo es ayudar a construir puentes entre una visión del futuro altamente incierta, las realidades de la industria actual, y caminos posibles hacia realidades alternativas de futuro.*



# Notas

1. *Consumer Reports*, "The pros and cons on alternative fuels," February 2014, [www.consumerreports.org/cro/2011/05/pros-and-cons-a-reality-check-on-alternative-fuels/index.htm](http://www.consumerreports.org/cro/2011/05/pros-and-cons-a-reality-check-on-alternative-fuels/index.htm), accessed September 14, 2015.
2. As an example, Ford Motor is now using aluminum in its new F-150 trucks, reducing weight by 700 pounds per truck. See James R. Healey, "2015 Ford F-150 makes radical jump to aluminum body," *USA Today*, January 14, 2014, [www.usatoday.com/story/money/cars/2014/01/13/redesigned-2015-ford-f-series-pickup-f-150-aluminum/4421041/](http://www.usatoday.com/story/money/cars/2014/01/13/redesigned-2015-ford-f-series-pickup-f-150-aluminum/4421041/), accessed September 14, 2015.
3. In September 2015, Google hired John Krafcik, an auto industry insider, to head its driverless car project, leading to news sources speculating that the company is moving quickly to commercialize autonomous vehicle technology. Alistair Barr and Mike Ramsey, "Google brings in chief for self-driving cars," *Wall Street Journal*, September 13, 2015, [www.wsj.com/articles/google-brings-in-chief-for-self-driving-cars-1442199840](http://www.wsj.com/articles/google-brings-in-chief-for-self-driving-cars-1442199840), accessed September 14, 2015.
4. For a more complete discussion of the connected car, see Simon Ninan, Bharath Gangula, Matthias von Alten, and Brenna Sniderman, *Who owns the road? The IoT-connected car of today—and tomorrow*, Deloitte University Press, August 18, 2015, <http://dupress.com/articles/internet-of-things-iot-in-automotive-industry/>.
5. There are multiple examples of these technologies, including BMW's Real Time Traffic Information, a navigation system for traffic avoidance re-routing, and GM's OnStar automatic emergency crash response. BMW, "Make progress instead of standing still," 2013, [www.bmw.com/com/en/insights/technology/connecteddrive/2013/services\\_apps/rtti.html](http://www.bmw.com/com/en/insights/technology/connecteddrive/2013/services_apps/rtti.html); OnStar, "Emergency," [www.onstar.com/us/en/services/emergency.html](http://www.onstar.com/us/en/services/emergency.html), both accessed September 14, 2015.
6. Liane Yvkoff, "One step closer to autonomous cars: 10 automakers to make automatic emergency braking standard," *Forbes*, September 11, 2015, [www.forbes.com/sites/lianeyvkoff/2015/09/11/automatic-emergency-braking-to-be-standard-on-10-manufacturers/](http://www.forbes.com/sites/lianeyvkoff/2015/09/11/automatic-emergency-braking-to-be-standard-on-10-manufacturers/), accessed September 14, 2015.
7. Craig Giffi and Joe Vitale, "2014 Gen Y automotive consumer study: The changing nature of mobility," Deloitte Automotive, 2014, [www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-auto-global-automotive-consumer-study-100914.pdf](http://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-auto-global-automotive-consumer-study-100914.pdf).
8. What do we mean by "ecosystem"? Botanist Arthur Tansley developed the concept to describe co-evolved and co-dependent networks of organisms in the natural world; by analogy, in the commercial world, it's the set of separate but interrelated entities and capabilities that together comprise a solution to a human need. All these components, in Tansley's words, "influence each other, and their environment; they compete and collaborate, share and create resources and co-evolve; and they are inevitably subject to external disruptions, to which they adapt together." In the realm of transportation, these components include vehicles, infrastructure, forms of energy, services, and more. Danone, "Arthur Tansley: The founding father of ecology was an 'honnête homme,'" *Down to Earth*, August 14, 2012, <http://downtoearth.danone.com/2012/08/14/arthur-tansley-the-founding-father-of-ecology-was-an-honnete-homme/>, accessed September 14, 2015.

9. 2014 annual GDP listed at \$17,420.7 billion. US Bureau of Economic Analysis, "Gross Domestic Product: Fourth quarter and annual 2014," released January 27, 2015, [www.bea.gov/news-releases/national/gdp/2015/pdf/gdp4q14\\_adv.pdf](http://www.bea.gov/news-releases/national/gdp/2015/pdf/gdp4q14_adv.pdf), accessed September 18, 2015.
10. The goal of the analysis is to estimate the cost per mile as well as capture the potential gains, losses, or shifts in value for each industry across each of the four future states described in the paper. Deloitte first analyzed the total cost per mile for road passengers today to evaluate consumers' cost of mobility. The components of cost per mile include depreciation, fuel, insurance, cost of driver time, maintenance, etc. Since the cost-per-mile calculation does not capture all of the changes' implications for each industry affected by the transformation to the future mobility ecosystem, we developed a baseline of the revenue generated by each sector in today's extended US auto industry. We then analyzed the impact of the future mobility ecosystem based on industry-specific hypotheses and macroeconomic analysis. We estimated the change in value from the current industry baseline across the four future states by understanding changes to components of cost per mile today and mapping each cost to the industry that collects the corresponding revenue. We conducted further analysis to estimate a future "steady state" that incorporates adoption rates across all future states. The value shifts are summarized at a sector level to illustrate the potential directional impact that autonomous cars and shared mobility could have on today's extended auto industry. Factoring in availability of data and the scope of the analysis, all data and figures used are from the United States as of 2015 (using 2014 dollars). The analysis does not assume a specific timeline or adoption curve. Rather, it is a blended model of four potential future states intended to provide directional insights about the future at maturity. Forthcoming installments of the Future of Mobility series will include a more detailed explanation of the analysis Deloitte conducted as well as the results.
11. Ninety-four percent of crashes are due to human error. National Highway Traffic Safety Administration, "Critical reasons for crashes investigated in the National Motor Vehicle Crash Causation Survey," February 2015, [www.nrd.nhtsa.dot.gov/Pubs/812115.pdf](http://www.nrd.nhtsa.dot.gov/Pubs/812115.pdf), accessed September 14, 2015.
12. Google, "Google self-driving car project monthly report," July 2015, <http://static.googleusercontent.com/media/www.google.com/en/selfdrivingcar/files/reports/report-0715.pdf>, accessed September 14, 2015. "One million" in this sentence refers to the amount driven in self-driving mode, vs. the total.
13. Philip Cardenas, Uber head of global safety, "Our commitment to safety," December 17, 2014, <http://newsroom.uber.com/2014/12/our-commitment-to-safety/>, accessed September 14, 2015.
14. Ford, "Ford at CES announces smart mobility plan and 25 global experiments designed to change the way the world moves," January 6, 2015, <https://media.ford.com/content/fordmedia/fna/us/en/news/2015/01/06/ford-at-ces-announces-smart-mobility-plan.html>, accessed September 14, 2015.
15. Austin Carr, "BMW to launch NYC tech incubator with \$100 million investment fund," *Fast Company*, March 31, 2011, [www.fastcompany.com/1743933/bmw-launch-nyc-tech-incubator-100-million-investment-fund](http://www.fastcompany.com/1743933/bmw-launch-nyc-tech-incubator-100-million-investment-fund), accessed September 14, 2015.
16. Mercedes-Benz USA, "Self-driving," April 6, 2015. TV commercial, [www.youtube.com/watch?v=Tna7rU\\_Tfhg](http://www.youtube.com/watch?v=Tna7rU_Tfhg), accessed September 14, 2015.
17. Anita Lienert and John O'Dell, "GM and Toyota take major step toward autonomous driving," *Edmunds*, September 8, 2014, [www.edmunds.com/car-news/2017-cadillac-cts-to-take-major-step-toward-autonomous-driving.html](http://www.edmunds.com/car-news/2017-cadillac-cts-to-take-major-step-toward-autonomous-driving.html).
18. Michael Martinez, "U-M autonomous vehicle test site to be unveiled Monday," *Detroit News*, July 17, 2015, [www.detroitnews.com/story/business/autos/2015/07/17/mcity-debut-mon-day/30316151/](http://www.detroitnews.com/story/business/autos/2015/07/17/mcity-debut-mon-day/30316151/), accessed September 14, 2015.
19. Discussion with Lawrence Burns, professor of engineering at University of Michigan, a consultant to Google's self-driving car project, and former corporate vice president of R&D at General Motors, February 2015.
20. Andrew Bender, "Uber's astounding rise: Overtaking taxis in key markets," *Forbes*, April 10, 2015, [www.forbes.com/sites/andrewbender/2015/04/10/ubers-astounding-rise-overtaking-taxis-in-key-markets/](http://www.forbes.com/sites/andrewbender/2015/04/10/ubers-astounding-rise-overtaking-taxis-in-key-markets/), accessed Aug. 21, 2015.
21. Ninan, Gangula, von Alten, and Sniderman, *Who owns the road?*
22. Deloitte's analysis suggests that the added cost to the purchaser of autonomous-drive technology will range between \$3,000

and \$10,000, with an assumed  
additional cost of \$5,000 for our

valuations.

23. Chad Vanderveen, "A glimpse into the future of fleet management," FutureStructure, June 5, 2014, [www.govtech.com/fs/news/A-Glimpse-into-the-Future-of-Fleet-Management.html](http://www.govtech.com/fs/news/A-Glimpse-into-the-Future-of-Fleet-Management.html), accessed August 21, 2015.
24. Reasonable people may disagree on the value of redirected driver attention in autonomous vehicles. Even if the analysis excludes the cost of drivers' time, the results still suggest a lower overall economic cost per mile for autonomous vehicles than either of today's approaches, given increased efficiencies and higher asset utilization.
25. Susan Shaheen and Adam Cohen, "Innovative mobility carsharing outlook," UC Berkeley Transportation Sustainability Research Center, November 11, 2014, <http://tsrc.berkeley.edu/sites/default/files/Fall%202014%20Carsharing%20Outlook%20Final.pdf>, accessed September 14, 2015. Ellen Huet, "Uber says it's doing 1 million rides per day, 140 Million in last year," *Forbes*, December 17, 2014, [www.forbes.com/sites/ellenhuet/2014/12/17/uber-says-its-doing-1-million-rides-per-day-140-million-in-last-year/](http://www.forbes.com/sites/ellenhuet/2014/12/17/uber-says-its-doing-1-million-rides-per-day-140-million-in-last-year/), accessed September 14, 2015.
26. Ellen Huet, "Uber says it's doing 1 million rides per day, 140 million in last year," *Forbes*, December 17, 2014, [www.forbes.com/sites/ellenhuet/2014/12/17/uber-says-its-doing-1-million-rides-per-day-140-million-in-last-year/](http://www.forbes.com/sites/ellenhuet/2014/12/17/uber-says-its-doing-1-million-rides-per-day-140-million-in-last-year/), accessed September 14, 2015.
27. Bradley Voytek, "Optimizing a dispatch system using an AI simulation framework," Uber, August 11, 2014, <http://newsroom.uber.com/2014/08/semi-automated-science-using-an-ai-simulation-framework/>, accessed September 14, 2015.
28. As of September 2015, Uber is available in 324 cities and 60 countries. Uber, "Uber cities," [www.uber.com/cities](http://www.uber.com/cities).
29. Doron Levin, "The cold, hard truth about autonomous vehicles and weather," *Fortune*, February 2, 2015, <http://fortune.com/2015/02/02/autonomous-driving-bad-weather/>, accessed August 21, 2015.
30. Byron Spice, Ken Walters, and Kristin Carvell, "Uber, Carnegie Mellon announce strategic partnership and creation of advanced technologies center in Pittsburgh," *Carnegie Mellon University News*, February 2, 2015, [www.cmu.edu/news/stories/archives/2015/february/uber-partnership.html](http://www.cmu.edu/news/stories/archives/2015/february/uber-partnership.html); Kirsten Kirosec, "Uber's mapping cars have

- high-tech home," *Fortune*, <http://fortune.com/2015/08/25/uber-self-driving-cars-arizona/>, both accessed September 14, 2015.
31. Chris Urmson, "How a driverless car sees the road," TED2015, [www.ted.com/talks/chris\\_urmson\\_how\\_a\\_driverless\\_car\\_sees\\_the\\_road?language=en](http://www.ted.com/talks/chris_urmson_how_a_driverless_car_sees_the_road?language=en).
  32. Joseph A. Schumpeter, *Capitalism, Socialism, and Democracy* (Harper and Brothers, 1942).
  33. Eamonn Kelly, *Introduction: Business ecosystems come of age*, Deloitte University Press, April 15, 2015, <http://dupress.com/articles/business-ecosystems-come-of-age-business-trends/>.
  34. Eamonn Kelly, *Blurring boundaries, uncharted frontiers*, Deloitte University Press, April 15, 2015, <http://dupress.com/articles/business-ecosystems-boundaries-business-trends/>.
  35. Discussion with John Hagel, co-chairman for Deloitte LLP's Center for the Edge, with more than 35 years of experience as a management consultant, author, speaker, and entrepreneur, April 2015.
  36. For a fuller discussion of this tension, see Ninan, Gangula, von Alten, and Sniderman, *Who owns the road?*
  37. Roger Martin, "Five questions to build a strategy," *Harvard Business Review*, May 26, 2010, <https://hbr.org/2010/05/the-five-questions-of-strategy.html>, accessed August 21, 2015.
  38. ROE for the automotive industry in the United States is 10.89 percent compared to the 13.24 percent cross-industry average (adjusted to include R&D costs). Aswath Damodaran, "Return on equity by sector (US)," *NYU Stern*, January 2015, [http://pages.stern.nyu.edu/~adamodar/New\\_Home\\_Page/datafile/roe.html](http://pages.stern.nyu.edu/~adamodar/New_Home_Page/datafile/roe.html), accessed September 14, 2015.
  39. Statista, "Capacity of the global automobile production industry from 2012 to 2017 (in million units)," 2015, [www.statista.com/statistics/266852/capacity-of-the-global-automobile-production-industry/](http://www.statista.com/statistics/266852/capacity-of-the-global-automobile-production-industry/); Statista, "Number of cars sold worldwide from 1990 to 2015 (in million units)," 2015, [www.statista.com/statistics/200002/international-car-sales-since-1990/](http://www.statista.com/statistics/200002/international-car-sales-since-1990/), both accessed September 14, 2015.
  40. Bill Vlasic, "U.S. sets higher fuel efficiency standards," *New York Times*, August 28, 2012, [www.nytimes.com/2012/08/29/business/energy-environment/obama-unveils-tighter-fuel-efficiency-standards.html](http://www.nytimes.com/2012/08/29/business/energy-environment/obama-unveils-tighter-fuel-efficiency-standards.html); Carolyn Whetzel,

- "California adopts strict new car standards, updates zero-emissions vehicle mandate," *Bloomberg*, January 30, 2012, [www.bna.com/california-adopts-strict-n12884907528/](http://www.bna.com/california-adopts-strict-n12884907528/), both accessed September 14, 2015.
41. GM, "A car for every purse and purpose," Generations of GM History Timeline, 1924, [https://history.gmheritagecenter.com/wiki/index.php/1924\\_%22A\\_Car\\_for\\_Every\\_Purse\\_and\\_Purpose%22](https://history.gmheritagecenter.com/wiki/index.php/1924_%22A_Car_for_Every_Purse_and_Purpose%22), accessed September 14, 2015.
42. Patrick Lin, "What if your autonomous car keeps routing you past Krispy Kreme?," *Atlantic*, January 22, 2014, [www.theatlantic.com/technology/archive/2014/01/what-if-your-autonomous-car-keeps-routing-you-past-krispy-kreme/283221/](http://www.theatlantic.com/technology/archive/2014/01/what-if-your-autonomous-car-keeps-routing-you-past-krispy-kreme/283221/), accessed September 14, 2015.
43. Mamta Badkar, "There's a huge shortage of truck drivers in America—here's why the problem is only getting worse," *Business Insider*, August 4, 2014, [www.businessinsider.com/americas-truck-driver-shortage-2014-7](http://www.businessinsider.com/americas-truck-driver-shortage-2014-7), accessed August 21, 2015.
44. American Trucking Association, "Trucking revenues top \$700 billion for the first time according to new report," May 11, 2015, [www.trucking.org/article.aspx?uid=70210058-bb81-44df-a565-492f899fc139](http://www.trucking.org/article.aspx?uid=70210058-bb81-44df-a565-492f899fc139), accessed August 21, 2015.
45. Trucker's Report, "The real cost of trucking— per mile operating cost of a commercial truck," [www.thetruckersreport.com/infographics/cost-of-trucking/](http://www.thetruckersreport.com/infographics/cost-of-trucking/), accessed September 14, 2015.

# Agradecimientos

Los autores querrían agradecer especialmente a los siguientes asesores y colaboradores, cuyas ideas y conocimiento fueron invaluable para la creación de este estudio: **Andrew Adams, Andrew Blau, Matthew Budman, Jonathan Copulsky, Mark Cottleer, Craig Giffi, John Hagel, Tim Hanley, Julia Kirby, Michelle Drew Rodriguez, y Steve Schmith.**

Externamente, **Lawrence Burns**, profesor de la práctica de ingeniería en la Universidad de Michigan, asesor del proyecto de conducción autónoma de Google, y ex Vicepresidente Corporativo de I&D y planeamiento de General Motors, y **Ron Goldsberry**, director de Deloitte y ejecutivo de Ford (retirado), me brindaron orientación significativa y conocimiento profundo en sus respectivas áreas de conocimiento.

Además, muchos colegas de Deloitte contribuyeron con su tiempo y visión de sus industrias respectivas. Otros colaboradores clave fueron: **Bruce Brown, Andrew Dinsdale, Masa Hasegawa, Joseph Kwederis, Sean Peasley, and Thomas Schiller** del sector automotriz; **Christian Grant, Kevin Matthews, y James Hendrickson** del sector energético; **Joe Guastella, Neal Baumann, Cindy MacFarlane, Bill Mullaney, Sandeep Puri, y Malika Gandhi** del sector de seguros; **Gerald Belson** del sector medios; **William Eggers, Tiffany Fishman, Felix Martinez, Jim Templeton, y Peter Viechnicki** del sector público; **Dan Haynes y Joann Michalik** del sector de fabricaciones; **Steve Atkins, David Couture, Atin Gupta, Simon Ninan, Andy Daecher, Arun Perinkolam, e Irfan Saif** del sector de tecnología; **Jack Fritz, Nitin Jain, y Phil Wilson** del sector de telecomunicaciones; y **Karen Bowman y Scott Rosenberger** del sector de transporte.

Apreciamos el fuerte apoyo y respaldo del liderazgo de Deloitte, incluyendo a **Sam Balaji, Michael Canning, Ambar Chowdhury, Amy Feirn, Jason Girzadas, Tom Marriott, Jim Moffatt, y Rich Penkoski.**

Finalmente, los autores querrían agradecer al equipo central que se ocupó de las actividades diarias, y fue fundamental para el desarrollo y la gestión de este informe. El equipo incluyó a **Jacob Darby, Elizabeth Kong, John Krentz, John McGlynn, Katerina Petraki, Veronica Saron, Zach Shore, Andy Sussman, y Philipp Willigmann.**

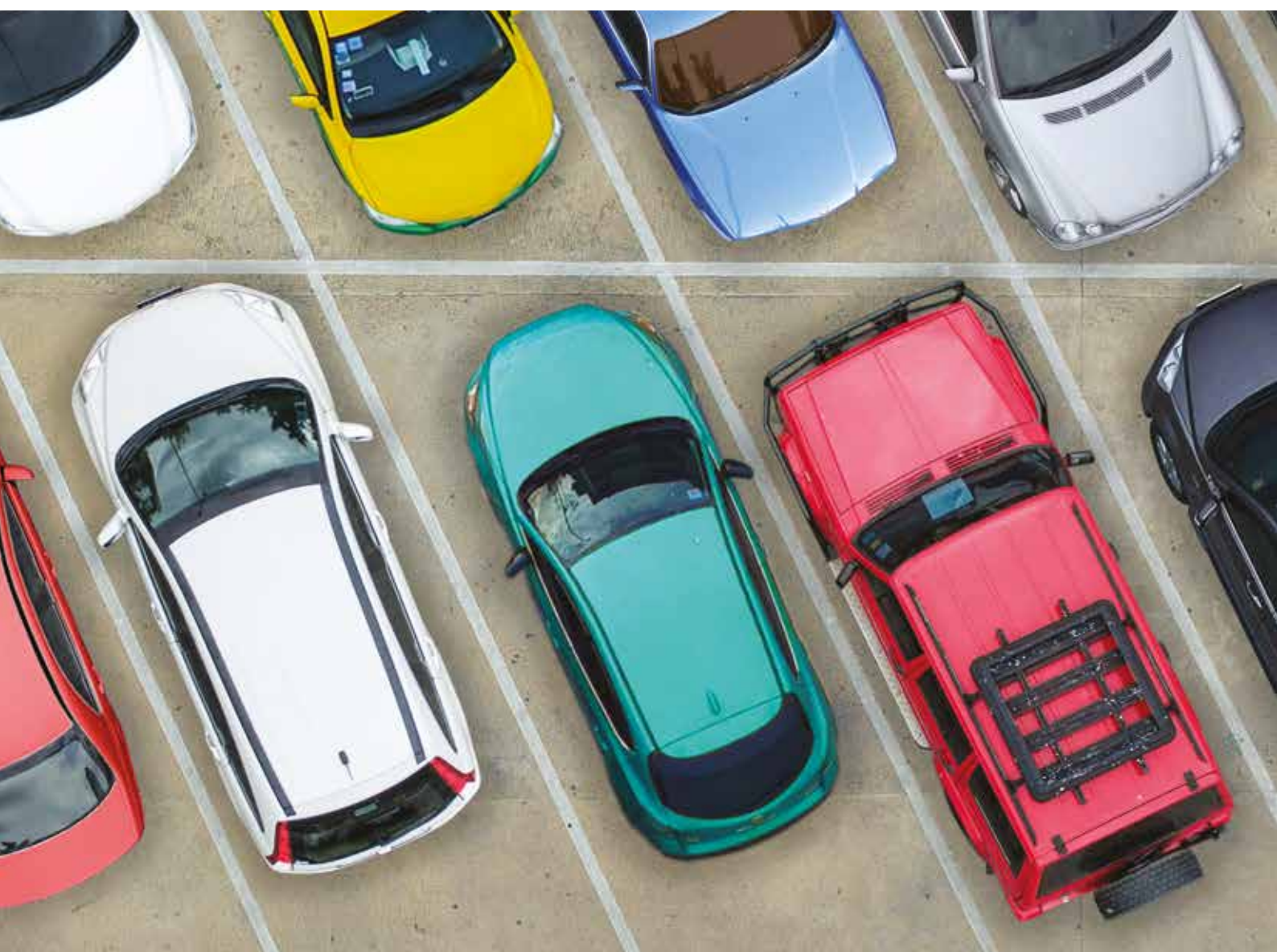


# **Tendencias en la flota mundial de vehículos 2023. Gestión del cambio a los SUV y la transición a los vehículos eléctricos**



# TRENDS IN THE GLOBAL VEHICLE FLEET 2023

## MANAGING THE SUV SHIFT AND THE EV TRANSITION



## ACKNOWLEDGMENTS

The project was developed at the European Transport and Energy Research Centre of the Institute of Transportation Studies, University of California, Davis, and managed by Pierpaolo Cazzola.



This report was authored by Pierpaolo Cazzola, Leonardo Paoli, and Jacob Teter. All authors contributed to the development of the data processing methodology, building on earlier experiences, in particular with previous GFEI benchmarking reports. Leonardo Paoli led on updating the data and making them publicly available.

Sheila Watson (FIA Foundation) provided feedback on the draft report and John Pap (FIA Foundation) managed the editorial process.

The authors would like to thank peer reviewers who provided essential feedback to improve the quality of the report. They include Elizabeth Connelly (IEA [International Energy Agency]); Matteo Craglia (International Transport Forum); Francois Cuenot (United Nations Economic Commission for Europe); Eduardo Espitia Echeverria (World Bank); Lew Fulton (University of California, Davis); Mathilde Huismans (IEA); Alex Körner (United National Environment Programme); Aditya Ramji (University of California, Davis), María Santos Alfageme (Instituto Superior Técnico, Lisbon); Jules Sery (IEA); and Jacopo Tattini (Joint Research Center, European Commission).

The project was funded by the FIA Foundation.

Design by Diana Fauner and John Rigby.

Photography by Alamy, Getty Images, iStock and Shutterstock.

DOI: [10.7922/G2HM56SV](https://doi.org/10.7922/G2HM56SV)

Dataset on Zenodo. DOI: [10.5281/zenodo.10148349](https://doi.org/10.5281/zenodo.10148349)  
November 2023



# TRENDS IN THE GLOBAL VEHICLE FLEET 2023 MANAGING THE SUV SHIFT AND THE EV TRANSITION



# CONTENTS

|                                                                                                                |           |  |  |
|----------------------------------------------------------------------------------------------------------------|-----------|--|--|
| <a href="#">Executive Summary</a>                                                                              | <b>1</b>  |  |  |
| <b>1</b> <a href="#">Introduction</a>                                                                          | <b>5</b>  |  |  |
| <b>2</b> <a href="#">Key developments in light-duty vehicle markets</a>                                        | <b>6</b>  |  |  |
| 2.1 <a href="#">New sales of passenger cars and light commercial vehicles</a>                                  | 6         |  |  |
| 2.2 <a href="#">Energy efficiency of new vehicles</a>                                                          | 8         |  |  |
| 2.2.1 <a href="#">Technical determinants of the energy efficiency of vehicles</a>                              | 11        |  |  |
| 2.2.2 <a href="#">Tailpipe carbon emissions of new light-duty vehicles</a>                                     | 13        |  |  |
| 2.3 <a href="#">Vehicle sales by powertrain</a>                                                                | 13        |  |  |
| 2.4 <a href="#">Vehicle sales by segment</a>                                                                   | 15        |  |  |
| 2.5 <a href="#">Vehicle size and weight</a>                                                                    | 19        |  |  |
| <b>3</b> <a href="#">Analysis of the vehicle market developments and implications for policy action</a>        | <b>21</b> |  |  |
| 3.1 <a href="#">Impacts of the shift towards SUVs</a>                                                          | 21        |  |  |
| 3.1.1 <a href="#">Energy and CO<sub>2</sub> emissions</a>                                                      | 21        |  |  |
| 3.1.2 <a href="#">Vehicle weight</a>                                                                           | 21        |  |  |
| 3.1.3 <a href="#">Road safety</a>                                                                              | 23        |  |  |
| 3.1.4 <a href="#">Equity</a>                                                                                   | 23        |  |  |
| 3.2 <a href="#">The role of EVs in the shift towards SUVs</a>                                                  | 25        |  |  |
| 3.3 <a href="#">Impacts of the EV transition</a>                                                               | 26        |  |  |
| 3.3.1 <a href="#">Energy and CO<sub>2</sub> emissions</a>                                                      | 26        |  |  |
| 3.3.2 <a href="#">Vehicle weight</a>                                                                           | 27        |  |  |
| 3.3.3 <a href="#">Road safety</a>                                                                              | 30        |  |  |
| 3.3.4 <a href="#">Equity</a>                                                                                   | 31        |  |  |
| 3.4 <a href="#">Are SUVs and EVs increasing the risk of a global divide?</a>                                   | 31        |  |  |
| 3.5 <a href="#">Need for policy action to address existing challenges</a>                                      | 32        |  |  |
| <b>4</b> <a href="#">Policy options</a>                                                                        | <b>35</b> |  |  |
| 4.1 <a href="#">Regulatory policy frameworks on energy, environment and safety</a>                             | 37        |  |  |
| 4.1.1 <a href="#">Environmental regulations</a>                                                                | 37        |  |  |
| 4.1.2 <a href="#">Road safety regulations</a>                                                                  | 39        |  |  |
| 4.1.3 <a href="#">Use of regulations in vehicle trade</a>                                                      | 40        |  |  |
| 4.1.4 <a href="#">Urban access restrictions</a>                                                                | 40        |  |  |
| 4.1.5 <a href="#">Targeted regulatory requirements for specific usage profiles</a>                             | 40        |  |  |
| 4.2 <a href="#">Regulatory changes to address vehicle weight increases and equity-related challenges</a>       | 40        |  |  |
| 4.2.1 <a href="#">Regulations on vehicle footprint</a>                                                         | 41        |  |  |
| 4.2.2 <a href="#">Regulations on battery capacity</a>                                                          | 41        |  |  |
| 4.2.3 <a href="#">Other regulatory requirements applying specifically to batteries</a>                         | 41        |  |  |
| 4.2.4 <a href="#">Changes in existing environmental regulations</a>                                            | 42        |  |  |
| 4.2.5 <a href="#">Changes in existing road safety regulations</a>                                              | 44        |  |  |
| 4.2.6 <a href="#">Changes in targeted regulatory requirements for specific usage profiles</a>                  | 44        |  |  |
| 4.3 <a href="#">Vehicle taxation</a>                                                                           | 45        |  |  |
| 4.3.1 <a href="#">Country-level taxation frameworks</a>                                                        | 45        |  |  |
| 4.3.2 <a href="#">Key examples of country-wide differentiated vehicle registration taxes</a>                   | 45        |  |  |
| 4.3.3 <a href="#">Vehicle taxation related to international trade</a>                                          | 46        |  |  |
| 4.3.4 <a href="#">Local vehicle taxes and charges</a>                                                          | 47        |  |  |
| 4.4 <a href="#">Changes in vehicle taxes to address vehicle weight increases and equity-related challenges</a> | 48        |  |  |
| 4.4.1 <a href="#">Changes in country-level taxation frameworks</a>                                             | 48        |  |  |
| 4.4.2 <a href="#">Changes in vehicle taxation related with international trade</a>                             | 49        |  |  |
| 4.4.3 <a href="#">Changes in local vehicle taxes and charges</a>                                               | 50        |  |  |
| 4.5 <a href="#">Fuel taxation and carbon prices</a>                                                            | 50        |  |  |
| 4.5.1 <a href="#">Road user charges to complement or progressively replace fuel taxation</a>                   | 51        |  |  |
| 4.6 <a href="#">Alternative energy infrastructure (EV chargers)</a>                                            | 52        |  |  |
| 4.7 <a href="#">Sustainable finance and development aid funding</a>                                            | 54        |  |  |
| <b>Annex: Methodological note</b>                                                                              | <b>55</b> |  |  |
| A.1 <a href="#">Description of data sources</a>                                                                | 55        |  |  |
| A.1.1 <a href="#">Fuel economy in major car markets (2005-2017) data, GFEI_0517</a>                            | 55        |  |  |
| A.1.2 <a href="#">GFEI 2021 data, IEA_19</a>                                                                   | 55        |  |  |
| A.1.3 <a href="#">Automotive sales data from Marklines</a>                                                     | 55        |  |  |
| A.1.4 <a href="#">CO<sub>2</sub> emissions from cars and vans, EEA, EEA</a>                                    | 57        |  |  |
| A.2 <a href="#">Description of data processing steps</a>                                                       | 57        |  |  |
| A.2.1 <a href="#">Preparing Marklines sales data</a>                                                           | 57        |  |  |
| A.2.2 <a href="#">Preparing IEA specific energy consumption data</a>                                           | 57        |  |  |
| A.2.3 <a href="#">Preparing EEA data</a>                                                                       | 57        |  |  |
| A.2.4 <a href="#">Matching of powertrain categories with Marklines categories</a>                              | 59        |  |  |
| A.2.5 <a href="#">Joining specific energy consumption, weight, and footprint data to sales data</a>            | 59        |  |  |
| A.2.6 <a href="#">Improvements in ICE vehicle efficiency technologies</a>                                      | 59        |  |  |
| A.2.7 <a href="#">Mismatch between vehicle factory shipments and registrations in China</a>                    | 59        |  |  |
| A.3 <a href="#">Applying new WLTC corrections</a>                                                              | 60        |  |  |
| A.3.1 <a href="#">Re-benchmarking NEDC to WLTC conversion factors</a>                                          | 61        |  |  |
| A.4 <a href="#">Regional aggregations</a>                                                                      | 61        |  |  |
| <b>Abbreviations and acronyms</b>                                                                              | <b>66</b> |  |  |
| <b>Units of measure</b>                                                                                        | <b>66</b> |  |  |
| <b>References</b>                                                                                              | <b>67</b> |  |  |
| <b>Endnotes</b>                                                                                                | <b>77</b> |  |  |



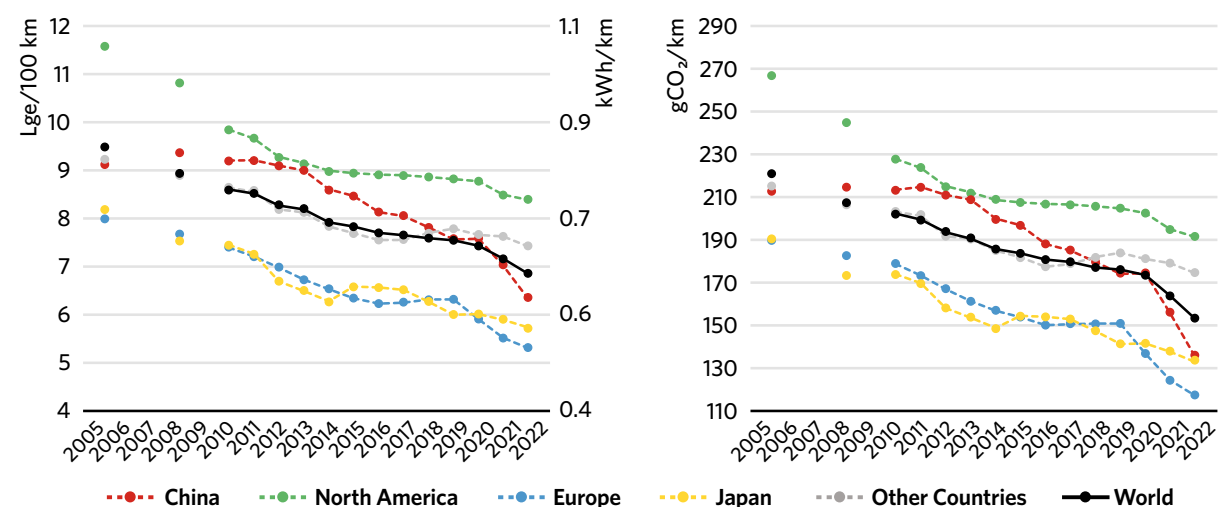
# EXECUTIVE SUMMARY

This is the latest update of a benchmarking report looking at the specific fuel consumption of light-duty vehicles (LDVs). While reporting data starting in 2005, it focuses on changes that occurred between 2019 and 2022.

Key developments include a 15% contraction of global LDV sales in 2020 as a consequence of the pandemic, and a limited recovery in sales through 2022. The sales-weighted specific energy consumption of LDVs

decreased in all major car markets from 2019 to 2022, improving at an average yearly rate of 3.2% and reaching 6.9 Lge/100 km in 2022 (0.64 kWh/km). This is a doubling of the average improvement rate observed between 2005 and 2019 (1.6%) (Figure ES1). Direct CO<sub>2</sub> emissions have declined even faster, at a rate of 2.1% per year between 2005 and 2022, as electrification affects carbon emissions more than energy consumption.

**FIGURE ES1:** Trends in the specific energy consumption of new light duty vehicles in major markets



**Notes:** Lge stands for litres of gasoline equivalent, and it is used to standardise fuel consumption according to their volumetric energy content, like kWh/km. There are 9.3 kWh per Lge. Historical specific energy consumption values have been benchmarked according to new understanding of the ratio between NEDC and WLTP test cycle energy intensity and CO<sub>2</sub> emissions performance. This revision has improved the real-world representativeness of the reported specific energy consumption.

**Sources:** this assessment (details in the Annex) based on IEA, 2019a; IEA, 2021a; EEA, 2023a; EEA, 2023b and Marklines data.

The global average annual rate of energy intensity reductions in the period from 2020 to 2022 was 4.2%. If this rate of improvement could be sustained through 2030, it would bring LDVs very close to meeting the GFEI target of doubling the energy efficiency of new LDV sales by 2030 from a 2005 baseline.

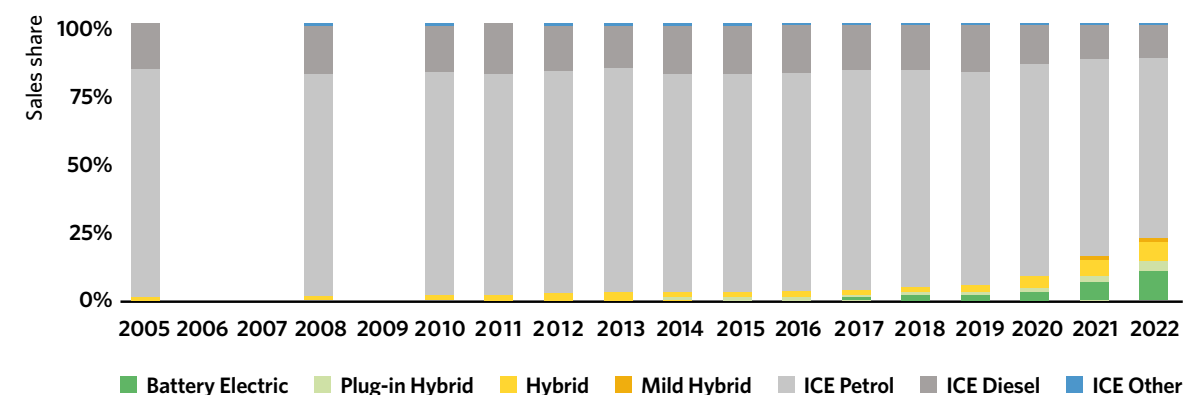
The rapid acceleration in energy efficiency seen in recent years is mainly due to the uptake of electric light-duty vehicles (EVs, which include both battery electric vehicles [BEVs] and plug-in hybrids [PHEVs]) (Figure ES2). Electric powertrains consume three to six times less energy than internal combustion engine vehicles to cover a unit of distance and their sales share reached 15% in

2022. The yearly rate of energy efficiency improvement between 2019 and 2022 was more pronounced (close to 6%) in markets where EV sales increased the most, namely China and Europe. In North America, lower uptake of EVs and a continued trend in sales of larger and heavier vehicles has resulted in a yearly improvement rate of 1.6%. In countries where EVs are not widely deployed, annual improvement rates are also close to 1.5%.

The efficiency of new vehicles is also linked with the size, weight, and power of new cars. A long-term shift towards

Sport Utility Vehicles (SUVs), underpinning increases in larger, heavier, and more powerful vehicles, has continued in major automotive markets and across nearly all countries (Figure ES3). In 2022, sales of SUVs overtook sales of conventional cars at a global level, reaching 51% of the total. Globally, the average vehicle weight of LDVs has also reached an all-time maximum, at 1530 kg. Average footprint has stagnated after 2019/2020 at about 4.2 m<sup>2</sup>. Increases took place in low- and medium-income countries, typically starting from a lower baseline. Limited declines occurred mainly in China and Europe.

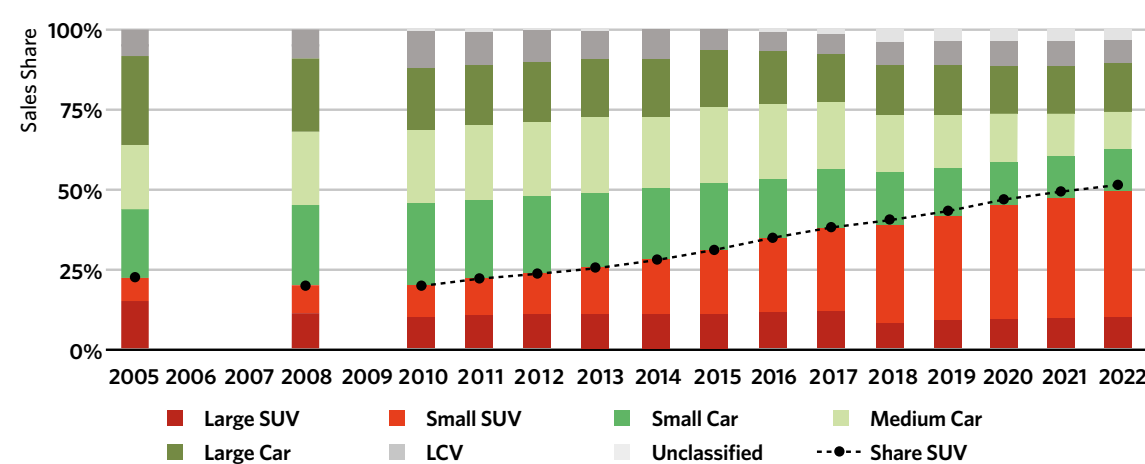
**FIGURE ES2:** Global LDV sales shares by powertrain



**Note:** ICE stands for internal combustion engine.

**Sources:** this assessment (details in the Annex) based on IEA, 2019a; IEA, 2021a; EEA, 2023a; EEA, 2023b and Marklines data.

**FIGURE ES3:** Global LDV sales by segment



**Sources:** this assessment (details in the Annex) based on IEA, 2019a; IEA, 2021a; EEA, 2023a; EEA, 2023b and Marklines data.



The two main trends underpinning developments in the global car market – a market shift towards SUVs and the transition toward EVs – have far-reaching implications for the automotive industry, as well as on the environment and society.

Shifts to larger and heavier vehicles led to increased oil consumption, direct CO<sub>2</sub> emissions and vehicle weight, size and power. Without the shift towards SUVs, energy use per km for combustion engine vehicles could have fallen at an average annual rate that is 30% higher than it did from 2010 to 2022. In the absence of the SUV shift, vehicle weight increases for these same vehicles could also have been more than halved.

Impacts of the SUV shift on energy use and direct emissions of CO<sub>2</sub> per km are being offset by increased electrification, thanks to markedly lower specific energy consumption versus combustion vehicles.

Electric vehicles however tend to weigh more than combustion vehicles, and their rise has added to the weight increases coming from the shift from small and medium cars to SUVs.

Despite increases in disposable income of households worldwide, the SUV shift was instrumental for an increase in original equipment manufacturers (OEM) profitability that remained in place even after the contraction observed in the global LDV market. This, however, also resulted in relevant affordability and equity challenges within and across countries. Higher investment costs needed for EVs exacerbated these challenges, even if savings from lower energy and maintenance costs for EVs help to mitigate this effect on a total cost of ownership basis.

Legacy OEMs have been slow to enter the EV market, especially in smaller segments, despite the risk of exposure to long-term losses of market shares to Chinese competitors. Reasons include the near-term focus on higher profitability, the cost of the batteries for BEVs and complex powertrains for PHEVs, challenges in the development of new battery supply chains and large capital outlays for investment in new industrial facilities.

Equity-related challenges and greater exposure of low-income households and businesses to the combined market transformation towards EVs and SUVs point towards the possibility of a growing global divide, not only within different income groups within countries, but also between major developed economies and other countries.

## POLICY OPTIONS

Managing these developments requires a broad range of policy actions.

- The adoption and continued development of fundamental pre-requisites: technical standards, increased low-carbon electricity availability, and removal of fossil fuel subsidies.
- A coherent policy framework is also needed beyond tailpipe emissions, taking a holistic approach to address impacts of LDV production and operations from a lifecycle perspective.

Novel regulatory mechanisms can address issues related to increased vehicle size and weight.

- The introduction of a cap on vehicle footprint, in absolute terms and as a sales-weighted average, paired with net declines going forward, to limit and then reverse the SUV shift.
- Corporate-average regulatory requirements, similar to those in place for fuel economy or CO<sub>2</sub> emissions, having battery capacity (kWh/vehicle) as the regulated parameter. These could be especially effective to complement the footprint regulations to reverse the SUV shift, addressing critical mineral issues from the demand side and equity issues specifically related with EVs through product diversification, while leaving room for innovation in battery chemistries and providing flexibility in compliance strategies for automakers.
- The use of vehicle footprint, rather than weight, is also suggested as the best choice as a modulating parameter in existing regulations on specific energy consumption or direct CO<sub>2</sub> emissions, alongside tightened requirements for larger vehicles (including both ICEVs and EVs). This is because regulating based on footprint can incentivize lightweighting as an energy consumption reduction strategy, whereas weight-based regulations fail to do this.

This report proposes also to target more stringent environmental and safety regulations on highly utilized vehicles such as company cars, taxis, government fleets, and ride- and carsharing services. Measures requiring higher EV market shares and incentivizing electric vkm in these use cases can enhance efficiency in the use of minerals for EV batteries and may also generate positive spillovers in terms of equity.



Adapting existing policy and regulatory instruments can also help address these issues.

- Vehicle taxation reforms – including the integration of weight and prices as modulating parameters for vehicles taxes and charges, at the national and at the local levels – can help steer vehicle markets away from SUVs and encourage EV adoption without reducing government budgets.
- Fossil fuel taxes and carbon pricing mechanisms offer important opportunities to provide economic incentives for EVs. Incentives need to be targeted on more vulnerable households and businesses, facilitating a more equitable and inclusive transition. They can be financed from revenues from fossil fuel taxes and carbon pricing.
- Regulatory and fiscal measures supporting universal access to EV charging infrastructure are needed to enable consumers to gain more confidence to undertake a larger share of their trips even with a shorter range, thereby also addressing weight-related challenges for EVs.

- Sustainable finance frameworks, important to help achieve a better alignment between the decisions taken by investors, corporations and other entities, can benefit from updates in their taxonomies regarding weight-related attributes of vehicles.
- Financial instruments designed to facilitate access to EVs for capital-constrained households and small businesses, as well as initiatives favouring access to capital at lower cost, are crucial to help favouring an equitable transition, domestically and internationally.

While it is also technically feasible to make progress by reforming trade rules and tariffs applied to critical minerals, EV battery, and vehicles, progress on this depends upon the effectiveness of the dialogue and negotiations taking place at the intergovernmental level. Possible improvements to trade-related policies on vehicles include differentiated tariffs based on powertrain, battery size, energy efficiency, GHG emissions, vehicle weight and footprint. They are feasible as long as the differentiation aligns with rules of origin, environment- and national security-related exceptions foreseen by the World Trade Organization (WTO).



# 1 INTRODUCTION

This report is the latest update and sixth instalment of the Global Fuel Economy Initiative's biannual benchmarking report on light-duty vehicle sales, extending the analysis from 2019 through 2022.

Previous reports tracked the technical, market, and policy drivers of fuel economy and CO<sub>2</sub> emissions performance of new light-duty vehicles (LDVs) at a country, regional, and global level (Cuenot and Fulton, 2011, Cuenot and Körner, 2013, IEA, 2019a, and IEA, 2021a). These reports, together with other GFEI analyses (Cuenot, 2017), have documented the rising market shares of Sport Utility Vehicles (SUVs), and more generally, of larger and heavier vehicles, and analysed the impact of these trends on energy efficiency and CO<sub>2</sub> emissions in major LDV markets.

This report tracks this continuing trend, highlighting key implications, including reduced energy and resource efficiency, increased vehicle production costs and reduced affordability for vehicle owners – exacerbating inequalities within and among countries – as well as heightened injury and mortality risks to pedestrians, cyclists, and car drivers alike. Examining vehicle sales trends in low- and medium-income countries, this work also extends themes developed in the UC Davis report commissioned by the FIA Foundation for the ZEV Transition Council, “Facilitating a Transition to Zero-Emission Vehicles in the Global South” (Cazzola and Santos Alfageme, 2023).

Chapter 2 illustrates that the tendency towards larger market shares for vehicles in larger heavier vehicle segments is persistent and widespread. The same analysis also shows a rapid increase in vehicle electrification, with strong EV adoption in

China, Europe, Korea, Japan and North America,<sup>1</sup> resulting in substantial energy intensity and GHG emission reductions.

Chapter 3 analyses key determinants of the observed market developments, with a specific focus on the shift towards SUVs and the increase in EV shares. It examines the broader impacts of these dynamics, focusing on vehicle size, weight, and price increases, and considers aspects related with energy, emissions of CO<sub>2</sub> and local air pollutants, road safety, demand for minerals resources, and equity.

The following analysis, in Chapter 4, reviews policies already developed by governments to address the impacts of recent market developments, identifies best practices, and recommends changes and new regulatory instruments that are best suited to address the challenges discussed in Chapter 3, placing a greater emphasis on solutions that help bridge the risk of a global divide.

The methodological approach of this update differs from previous GFEI benchmarking reports. Rather than relying on a database with detailed model-level and in some cases trim-level data and including an extensive list of vehicle technical parameters (e.g., weight, footprint, engine capacity, number of doors, presence of efficiency technologies such as continuously variable transmissions, turbochargers, etc.), this data update relies on lower resolution data (still at the model level) from Marklines. The Methodological Annex outlines the methods used to ensure as close as possible consistency with previous reports, and to verify the accuracy and validity of this assessment.

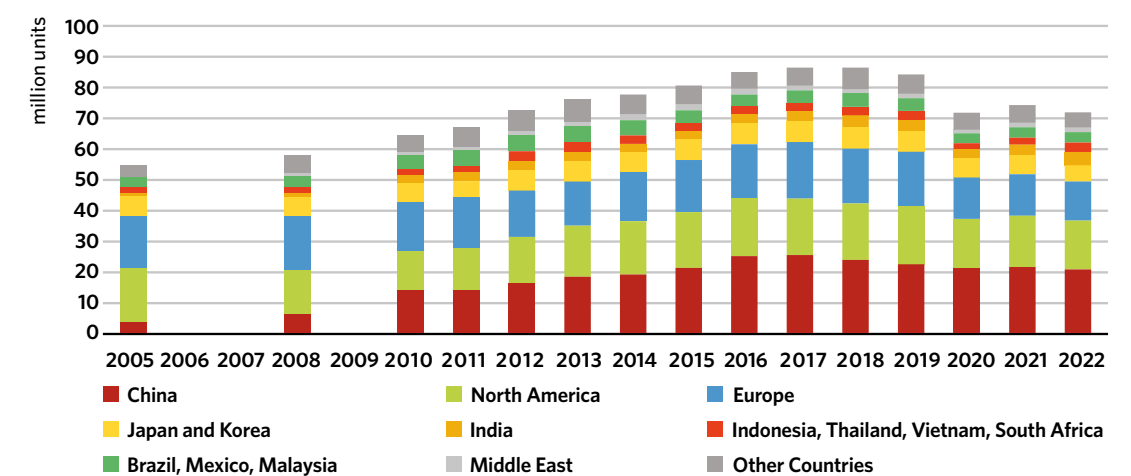


# 2 KEY DEVELOPMENTS IN LIGHT DUTY VEHICLE MARKETS

## 2.1 NEW SALES OF PASSENGER CARS AND LIGHT COMMERCIAL VEHICLES

Worldwide, the sales of light-duty vehicles (LDVs) – including passenger cars and light commercial vehicles<sup>2</sup> – steadily increased through 2017, and then slowed down through 2019 (Figure 1). Long term-trends were disrupted by the Covid-19 pandemic in 2020, which resulted in a rapid drop of sales across all regions: globally, 15% fewer LDVs were sold in 2020 than in 2019. Following 2020, sales rebounded, but are still around 10% lower than they were before the pandemic.

FIGURE 1: Global LDV sales by region 2005-2022



**Note:** LDV sales included in this analysis and in this graph are those for the countries listed in annex Table A6. Europe includes all member countries of the European Economic Area (EEA) plus Switzerland and the United Kingdom. North America includes the United States and Canada but excludes Mexico, included in the same group as Brazil and Malaysia, as they have similar characteristics with respect to GDP per capita, while still having a comparable population density, the presence of an automotive manufacturing capacity and not being a net importer of oil and petroleum products. Total sales for this set of countries are equivalent to roughly 85% of the total vehicle sales accounted by OICA – including commercial vehicles (OICA, 2023), meaning that they represent the vast majority of light duty vehicle sales globally.

**Sources:** this assessment (details in the Annex) based on IEA, 2019a; IEA, 2021a; EEA, 2023a; EEA, 2023b and Marklines data.

The rebound in sales has been slowed down by a stretched supply chain – especially due to a shortage of microchips – that has struggled to keep up with swings in demand (JP Morgan, 2023; Brinley, 2023; Straughan, 2023; Burkacky et al., 2021; Burkacky et al., 2022). Shifts in the market structure, as discussed below, accompanied by changes in vehicle prices as larger vehicles are above those of smaller ones, discussed in Chapter 3, are also influencing consumer choices regarding the acquisition of a new vehicle, including through postponement of purchases (GfK, 2023; Shmuel, 2022; Romei, 2022) or an increased consideration of second-hand options, where they are available (Roch Baranowski et al., 2023; Manheim, 2023).

The Chinese LDV market has undergone a very rapid rise since the beginning of the century. China became the world's largest LDV market in 2009 and from 2020 through 2022, with annual sales of 21 million vehicles, it has become by far and away the world's largest automotive market, accounting for 29% of global LDV sales in 2022. All the same, China's sales peaked in 2017 and have since been slowly declining. Several factors, often limiting growth in car ownership, help explain why the stabilization of car sales occurred when the number of cars per capita in China is still well below the levels observed in economies with higher per capita income. These reasons include, in addition to recent supply-chain challenges:

- the early phase of a transition from a growth market where most vehicles were sold to first-time owners to a mature “replacement” market;
- significant investments in public transport, including urban and intercity rail services (Xinhua, 2020; IEA, 2019b; and Ou et al., 2022);
- the frequent use of policies managing access to personal vehicles in cities, also in light of the transition to vehicle electrification (Feiqi et al., 2020; Liu et al., 2022; Jin et al., 2023; and He et al., 2018); and
- a pro-active deployment of digitally-enabled shared mobility services (Yin et al., 2022).<sup>3</sup>

The 2020 pandemic also had a much smaller impact in the Chinese market than in all other markets, with sales only declining around 5% year on year. Sales in China have subsequently remained fairly constant.

Sales in mature markets such as North America, Korea, Japan and Europe<sup>4</sup> remained mostly stagnant through 2019. With sales increasing in China by nearly seven-fold in 2020, relative to 2005 (and despite the decrease in sales from 2017 onwards) and with other countries, such as India, Indonesia, and Brazil, the

combined share of these mature markets out of the global market has declined from over 70% in 2005 to under 50% in 2022.

LDV sales in North America declined 14% in 2020 from their 2019 level, and have dropped a further 5% since then, to 13.9 million vehicles in 2022. Global supply chain constraints and rapid inflation, with the prices of new cars and trucks rising even higher than other consumer goods (Bureau of Labor Statistics, 2023), justify this reduction.<sup>5</sup>

In Japan, sales of LDVs declined by more than 10% since the pandemic and remained roughly constant thereafter.

In Korea the pandemic did not lead to any reduction in sales, but there has been a small decline since 2020. In 2022, Korea and Japan accounted for 8% of global LDV sales, the same share they accounted for pre-pandemic.

The European market has been slower than others to recover from the impacts of the pandemic due to regional shortages of vehicle components that were aggravated by Russia's invasion of Ukraine (VDA, 2022). This has led Europe's share of the global market to decline from 21% in 2019 to 18% in 2022.

Vehicle sales in emerging markets such as India, Indonesia, and Brazil grew substantially between 2005 and 2010, but their growth has slowed down since. In 2022, these markets accounted for 22% of global sales. The pandemic and the ensuing economic difficulties have also taken a toll on car sales in these countries, with a decline of 20% in 2020. Sales have since regained 7%, but they are still below pre-pandemic levels. Among these markets, the Indian market has been particularly dynamic, as it declined by a staggering 30% in 2020 but has since regained all the losses and sales volumes in 2022 exceeding pre-pandemic levels.



## 2.2 ENERGY EFFICIENCY OF NEW VEHICLES

The specific energy consumption of new vehicles has decreased since the beginning of this benchmarking exercise. The global sales-weighted average fuel consumption for LDVs sold in 2022 was 6.9 Lge/100km (0.64 kWh/km)<sup>6</sup>, nearly 30% less energy than the value in 2005. In 2020, GFEI partners reaffirmed their target to double the energy efficiency of new LDV sales by 2030 from a 2005 baseline. If it can be sustained through 2030, the global average annual rate of energy intensity reduction in the period from 2020 to 2022 (4.2%) would bring LDVs very close to meeting the GFEI target.

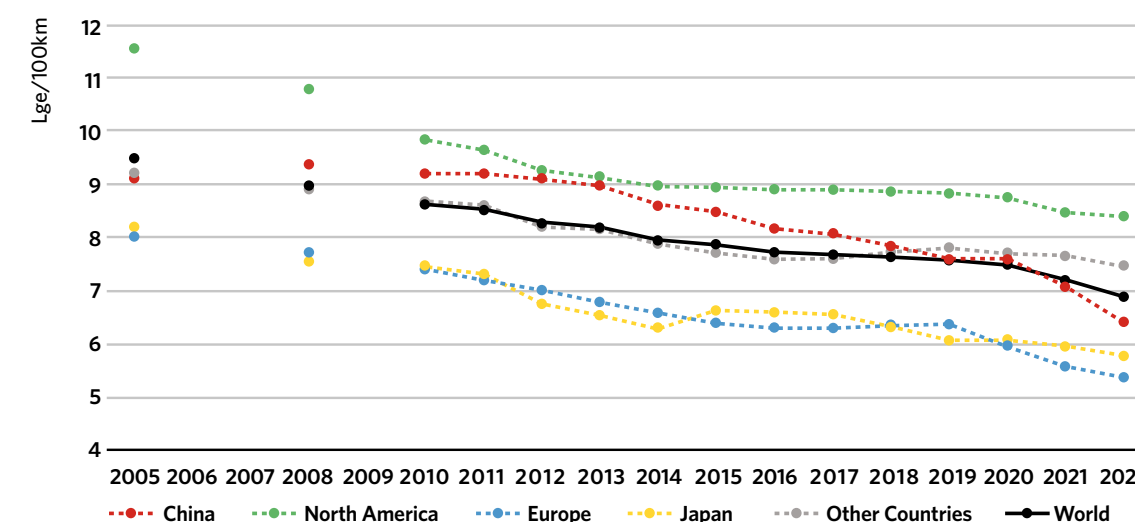
Worldwide, the pace of annual reduction in energy consumption per km declined over the 2010s, but marked improvements can be seen from 2019 onwards, as sales shares of electric vehicles have begun to ramp up substantially (Figure 2). The rapid acceleration in energy efficiency improvements seen in recent years is mainly due to the uptake of EVs, which include both BEVs

and PHEVs, reflecting the fact that electric powertrains consume three to six times less energy to cover a unit of distance in comparison with powertrains reliant on internal combustion engines (ICEs) and their sales share reached 15% in 2022.

The yearly rate of energy efficiency improvement between 2019 and 2022 was more pronounced in markets where EV sales increased the most, namely China (5.9%) and Europe (5.8%). In North America, lower uptake of EVs and a continued trend in sales of larger and heavier vehicles has resulted in a yearly improvement rate of 1.6%. In countries where EVs are not widely deployed, annual improvement rates are close to 1.5%.

Fuel prices and income levels remain key determinants of vehicle energy use per km, leading to systemic differences across national and regional markets, as already identified in earlier analyses (IEA, 2019a, IEA, 2021a) and shown in Figure 3. The Figure shows specific energy consumption plotted against gasoline prices and GDP per capita, both corrected based on purchasing power parities. Results show that higher fuel prices (and taxes)<sup>7</sup> tend to be paired with lower energy consumption per km and also that specific energy consumption is higher in countries with lower levels of fuel taxation, across different levels of average income.<sup>8</sup>

**FIGURE 2:** Trends in the specific energy consumption of new vehicles in major car markets

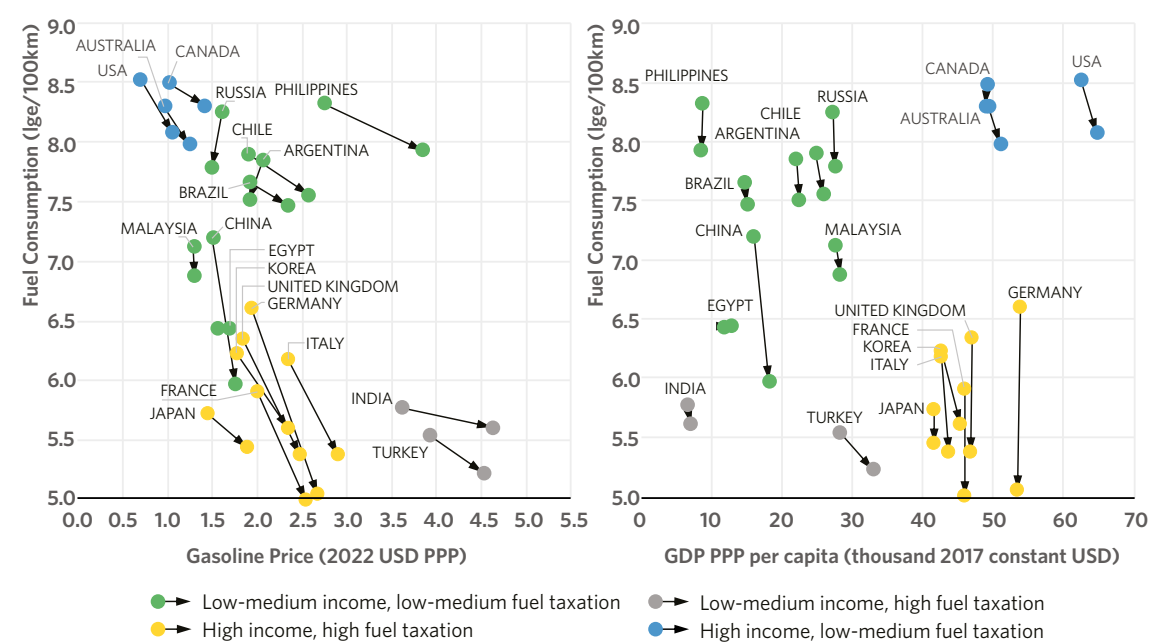


**Notes:** Data from 2005 to 2017 is based on Fuel Economy in Major Car Markets 2005-2017 (IEA, 2019a), while from 2019 onwards data follows the new methodology outlined in the annex. The year 2018 is shown as the average in values between 2017 and 2019.

**Sources:** this assessment (details in the Annex) based on IEA, 2019a; IEA, 2021a; EEA, 2023a; EEA, 2023b and Marklines data.



**FIGURE 3:** Evolution of specific energy consumption and gasoline price (left) and GDP per capita (right), using purchasing power parities, 2019-2022



**Notes:** Arrows show the change from 2019 to 2022.

**Sources:** Specific energy consumption from this data assessment (see the Annex for sources and methods)

Gasoline prices from the IEA energy prices database (IEA, 2023a) GDP per capita PPP and PPP conversions are from the World Bank Open Data (World Bank, 2023).

The trends in the specific energy consumption of new vehicles shown in Figure 2 can be analysed looking at three phases. The first spans the years between 2005 and 2017, the second runs from 2017 to 2020 and the third (also having important implications for Figure 3) follows the year 2020. Figure 4 summarizes key developments characterizing each of these phases, considering the development of key driving factors and their evolution over the years.

Between 2005 and 2017, average fuel consumption declined at a yearly rate of 1.8%, with most improvements having occurred in the earlier part of this period. These improvements were driven by regulations in major car markets aiming to reduce fuel consumption and CO<sub>2</sub> emissions, setting the pace of technology deployment in a way that also influenced other markets. Carmakers largely delivered these improvements through improved internal combustion engine (ICE) and vehicle technologies. These included turbochargers and improved transmissions, engine downsizing, material substitution and light-weighting technologies, an increased use of diesel powertrains (especially in

Europe, India and Korea) and hybrid powertrains (IEA, 2019a).

Between 2017 and 2020, improvements in rated specific energy intensity have mostly stagnated at a global level, with average specific energy consumption hovering 7.5 lge/100 km (0.7 kWh/km). This period of stagnating improvements can be largely explained by two counteracting drivers.

- On the one hand, new vehicles became larger, heavier, and more powerful, with a shift in market segments (the SUV share increased from 38% to 46%) driving fuel consumption upward.
- On the other hand, the beginning of growing market shares of electric vehicles (EVs), substantially lowering sales-weighted average fuel consumption and tailpipe emissions.

Electric vehicle sales increased from 1.5% in 2017 to 4% in 2020, on the back of supportive government policies and market- and technology-driven cost declines (IEA, 2018; 2019b; 2020).

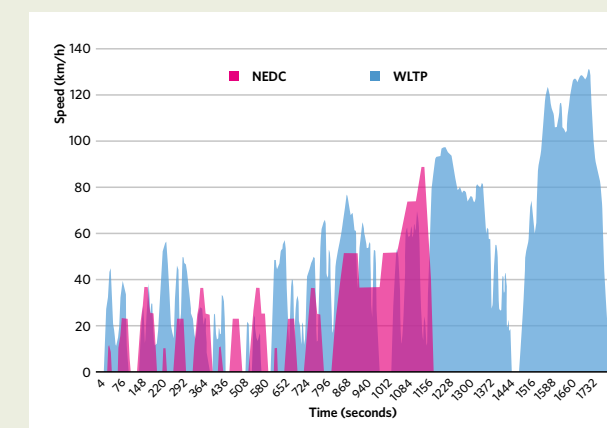
BOX 1:

## REVISED BENCHMARKING OF NEDC TO WLTC CONVERSION

To enable global comparisons across countries and major markets, fuel consumption and CO<sub>2</sub> emissions data are converted from regional or national test cycles to a single globally harmonized test cycle, the Worldwide harmonized Light-duty Test Cycle (WLTC).

In earlier reports (from 2016 to 2021), conversion factors were taken from powertrain-specific (i.e. gasoline and diesel ICE) zero intercept regressions developed by the ICCT (Kühlwein et al., 2014).<sup>10</sup> This approach is revised here, using regressions based on actual type approval data providing CO<sub>2</sub> emissions based on both the NEDC and WLTC test cycles, as reported by the European Environmental Agency (EEA) for light-duty vehicles registered across Europe between 2019 and 2022.<sup>11</sup> This led to a revision of the gap between NEDC and WLTC, meaning that it is now larger than it had been initially assessed in 2014, in line with other literature (Pavlovic et al, 2018, JRC, 2023).

Table 1 highlights the main differences in the assessment of specific fuel consumption due to this update. These results, based on EEA data and compared with those of the 2014 assessment (Kühlwein et al., 2014), indicate that the earlier NEDC to WLTC conversion factors were lower by a factor of 1.05 for gasoline- and 1.20 for diesel-powered LDVs, in comparison with updated values.



As inter-cycle conversion factors for test cycles used in different regions (e.g., between CAFE and JC08 and NEDC) assessed in 2014 remain accurate, the factors summarized in Table 1 have been used to rebase results assessed in earlier editions of this work, while maintaining inter-cycle conversion factors unchanged.

It is also worth highlighting that a gap remains between the WLTC factors and real-world fuel consumption, as has been established by a number of recent assessments (Tietge et al., 2017; Craglia and Cullen, 2019; IEA, 2019a; Dornoff et al., 2020; Komnos et al., 2022).

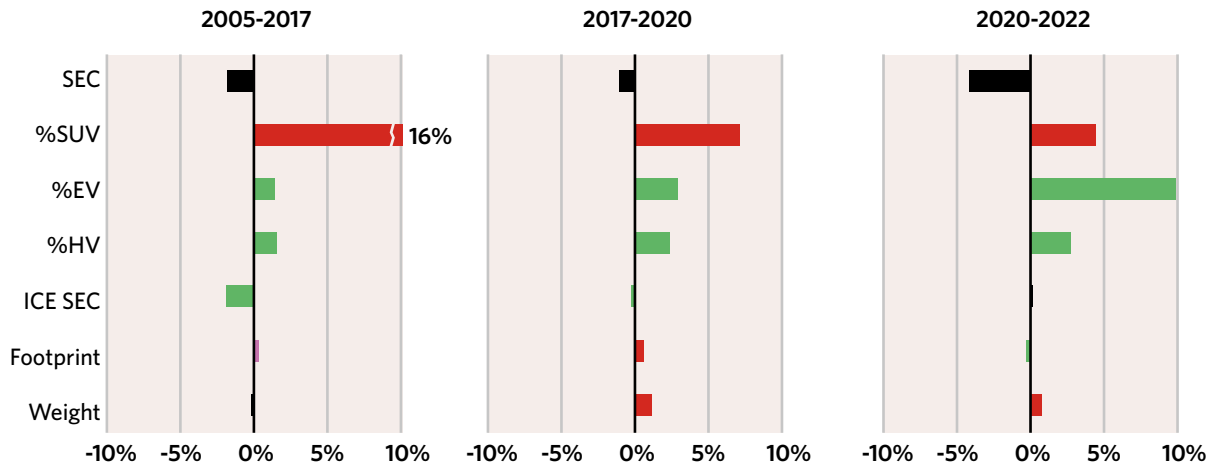
**TABLE 1:** Regression results for gasoline and diesel conversion between NEDC and WLTC

| Powertrain | NEDC to WLTC ratio ICCT 2014 | NEDC to WLTC ratio update EEA data 2019-22 | Ratio between 2014 and updated factor |
|------------|------------------------------|--------------------------------------------|---------------------------------------|
| Gasoline   | 1.128                        | 1.185*                                     | 1.05                                  |
| Diesel     | 1.029                        | 1.235*                                     | 1.20                                  |

\* The values reported here are for the ratio between NEDC and WLTC emissions performance (g CO<sub>2</sub>/km) for passenger cars. These ratios were determined also separately for passenger vehicles and light commercial vehicles for all basic powertrain-fuel combinations in the EEA dataset (gasoline, diesel, natural gas, LPG, gasoline-electric, diesel-electric, e85). Since direct CO<sub>2</sub> emissions for battery-electric and fuel-cell electric vehicles are 0 g CO<sub>2</sub>/km, ratios for specific energy consumption are unaffected for these powertrains. Full regression results are provided in the Appendix.



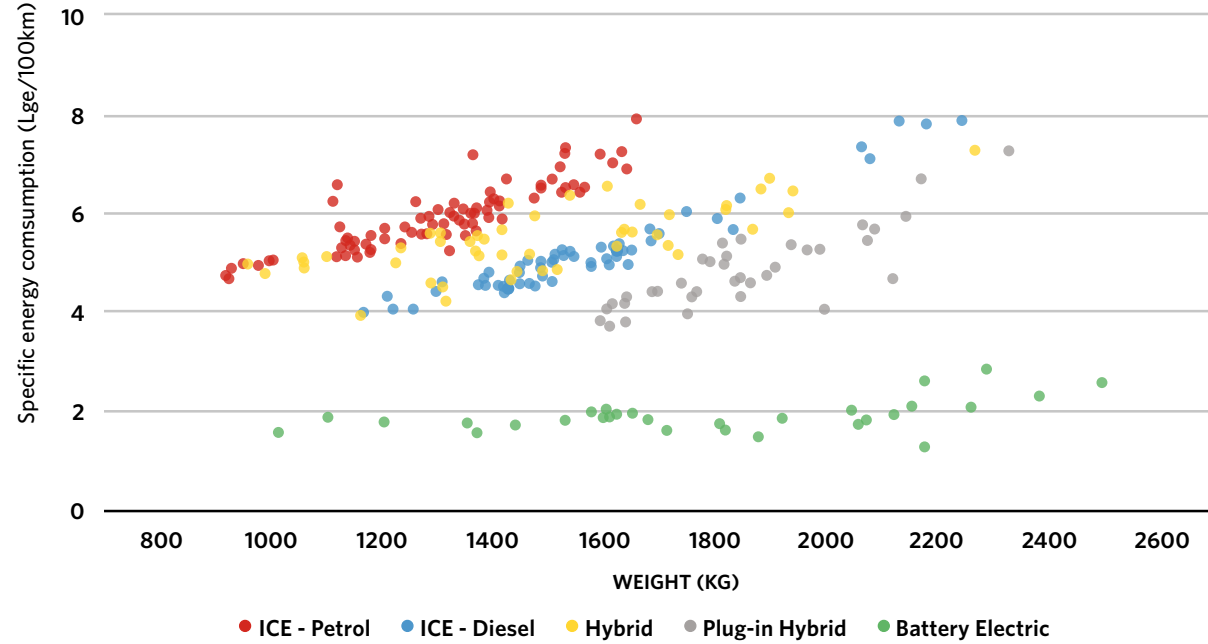
FIGURE 4: Changes in LDV specific fuel consumption and its principal drivers



**Notes:** SEC stands for specific energy consumption, calculated as the compound annual rate of increase/decrease. ICE SEC stands for the specific energy consumption of ICE vehicles, calculated as compound annual rate of change. Footprint stands for the average vehicle footprint, calculated as compound annual rate of change. Weight stands for the average vehicle mass, calculated as compound annual rate of change. % EV refers to the change in the market share of electric vehicles over the period. % HV refers to the change in the market share of hybrid vehicles over the period. % SUV refers to the change in the market share of SUVs over the period. Green indicates a contribution that decreases specific energy consumption. Red indicates a contribution that increases specific energy consumption.

**Sources:** this assessment (details in the Annex) based on IEA, 2019a; IEA, 2021a; EEA, 2023a; EEA, 2023b and Marklines data.

FIGURE 5: Specific energy consumption plotted against vehicle mass, by powertrain, for top selling light-duty vehicles in Europe



**Source:** based on 2021 European registration data from EEA, 2023a; EEA, 2023b. Specific energy consumption for PHEVs was calculated using a utility factor derived from the all-electric range reported in the EEA database using a function reflective of real-world usage (Fraunhofer ISI, 2021), specific energy consumption of electricity for driving phased in all-electric mode and specific fuel consumption for other driving phases.

Between 2020 and 2022, the global average of the specific energy consumption of new vehicle sales decreased 8%. This equates roughly to a 4.2% year-on-year decrease, double what has been observed in any year previously over the entire GFEI database period that started in 2005 (as covered by this series of benchmarking reports). This suggests that, starting in 2020, trends in specific energy consumption have entered a new period, heavily influenced by the rise of EV market shares across all major LDV markets.

Indeed, China saw EV sales share start to grow very rapidly in 2019. Europe followed in 2020. Since 2022, a remarkable growth is starting to occur also in North America. With EV sales accounting for 15% of the global market in 2022, and limited changes in the energy use per km of new ICEVs, the impact of EVs on the specific energy consumption of light-duty vehicles is now significant, even at the global scale.

The surge in EV market shares that occurred after 2020 is paired with stronger changes in the patterns show in Figure 3, since markets with high increases in EV sales shares are those characterized by the most relevant drops in the specific fuel

consumption of new vehicles. The cases of European countries and China are particularly visible, as they have undergone the fastest change. In China, the change was so pronounced that it now fits well within the cluster of developed countries with high fuel prices, while still having a relatively low level for fuel taxation.

## 2.2.1 TECHNICAL DETERMINANTS OF THE ENERGY EFFICIENCY OF VEHICLES

The specific energy consumption of vehicles depends primarily on two physical characteristics: it is proportional to the weight and size of the vehicle, and it is inversely proportional to the efficiency of the powertrain.

Figure 5 shows results relative to vehicles sold in 2022 in the European market and reflects differences taking place across both weight and powertrains.

Weight-related trends by powertrain show that heavier vehicles (which are generally also larger, and tend to be Sport Utility Vehicles, or SUVs) require

more motive energy per unit distance. For example, a large SUV (such as a Ford F150) powered by a gasoline engine consumes around 11 Lge/100 km (1 kWh/km), while a medium car (such as a VW Golf) consumes 6.4 Lge/100km (0.6 kWh/km). Conversely, powertrains that more efficiently convert input energy into motion consume less energy to drive the same distance.

Differences in specific energy consumption across powertrains reflect differences in the capacity of different powertrains to convert energy into motion (IEA, 2021a).

- Gasoline-powered ICEs convert roughly 20%-25% of the energy available in the fuel into motion.
- Diesel powertrains are generally more energy efficient than gasoline ICEs with similar performance, requiring roughly 15% to 20% less energy than gasoline ICEs to perform the same service, despite a weight penalty.
- Hybrid vehicles convert around 35% of the fuel's energy into motion, cutting liquid

fuel requirements by roughly 20% vs. ICE powertrains, thanks to the use of electric propulsion in driving phases where the ICE is particularly inefficient, which more than offsets higher energy demand (to recharge the batteries) in driving conditions with better ICE energy efficiency.

- Battery electric vehicles (BEVs) convert around 75% of the energy they receive into motion.
- Plug-in hybrids combine the benefits of BEVs and hybrids in a way that depends on the extent to which they are driven in charge-depleting mode (in which case their energy efficiency performance is close to a BEVs) or in charge-sustaining mode (in which case they behave in a way that is similar to a conventional hybrid vehicle).

Hybrids, plug-in hybrids, and battery electric vehicles also recover, with limited losses, the kinetic energy of vehicles during braking, with larger energy efficiency advantages vs. ICEs for heavier vehicles. Further variability depends on driving speeds and the use of auxiliaries (e.g., air conditioning).<sup>9</sup>

2.2.2 TAILPIPE CO<sub>2</sub> EMISSIONS OF NEW LIGHT DUTY VEHICLES

The tailpipe carbon dioxide emissions from new sales have evolved in a very similar way to the specific energy consumption, as shown in Figure 6. The two quantities are proportional and closely related.

For vehicles powered by fossil fuels, declines in tailpipe CO<sub>2</sub> emissions are directly proportional to the declines in specific energy consumption. The key difference in trends between the two parameters is driven by the presence of EVs, and in particular of BEVs: their specific energy consumption is around 70% lower than that of ICEs, while their CO<sub>2</sub> emissions are 100% lower, as they emit no CO<sub>2</sub> tailpipe emissions.

Until 2019, 95% of all vehicles sold globally were powered by traditional internal combustion engine powertrains. A major driver for improvements in fuel economy through 2019 was the introduction, growth and eventual decline of diesel powertrains in Europe and India. Diesel engines proved to be a good solution to reduce CO<sub>2</sub> emissions, but improvements came at the expense of increased air pollutant emissions.<sup>12</sup> The discovery of these increased emissions in 2015 has marked the beginning of the decline for this powertrain in both Europe and India.

This means that the electrification trend is stronger than the SUVs shift, when looking at this parameter. Therefore, unlike specific energy consumption, CO<sub>2</sub> emissions have continuously declined at a global level. The decline was 1.6%, on average, per year,

from 2005-2019, and 4.6% between 2019 and 2022 – faster than the decline in specific energy consumption. Similarly, we observe that all markets where electrification has advanced CO<sub>2</sub> emissions have declined faster than specific energy consumption.

2.3 VEHICLE SALES BY POWERTRAIN

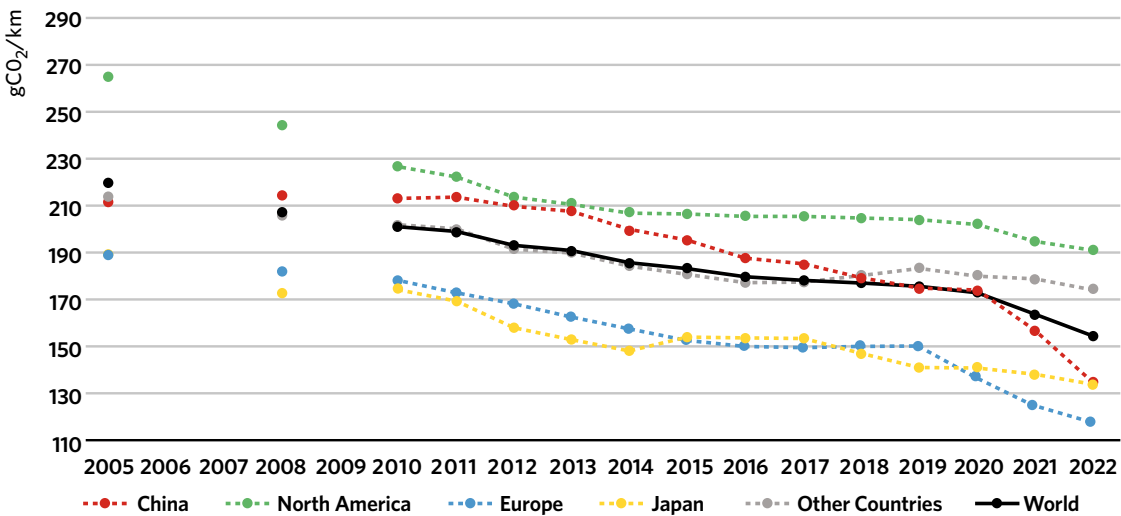
Figure 7 summarizes the dynamics the LDV market has evolved in terms of vehicle powertrains. It considers both global developments (across the whole period analysed here) and specific cases, represented by selected years and targeted markets.

Until 2019, 95% of all vehicles sold globally were powered by traditional internal combustion engine powertrains. A major driver for improvements in fuel economy through 2019 was the introduction, growth and eventual decline of diesel powertrains in Europe and India. Diesel engines proved to be a good solution to reduce CO<sub>2</sub> emissions, but improvements came at the expense of increased air pollutant emissions.<sup>12</sup> The discovery of these increased emissions in 2015 has marked the beginning of the decline for this powertrain in both Europe and India. In 2022, diesel powertrains accounted for 23% of sales in Europe and 25% in India.

As shown in Figure 5, hybrid vehicles offer energy savings relative to gasoline-fuelled vehicles. They also offer reduced air pollutant emissions relative to diesel-fuelled vehicles. This technology was pioneered in Japan, where hybrid vehicles account now for about one-quarter of sales. Worldwide, hybrid sales shares remained constant from 2013 to 2019, accounting for roughly 3% of all vehicles entering the market. Over this period, relatively low oil prices and limited availability of hybrid models have limited market penetration, mostly to Japan and Korea, where hybrid sales shares reached 20% and 6% of the total,

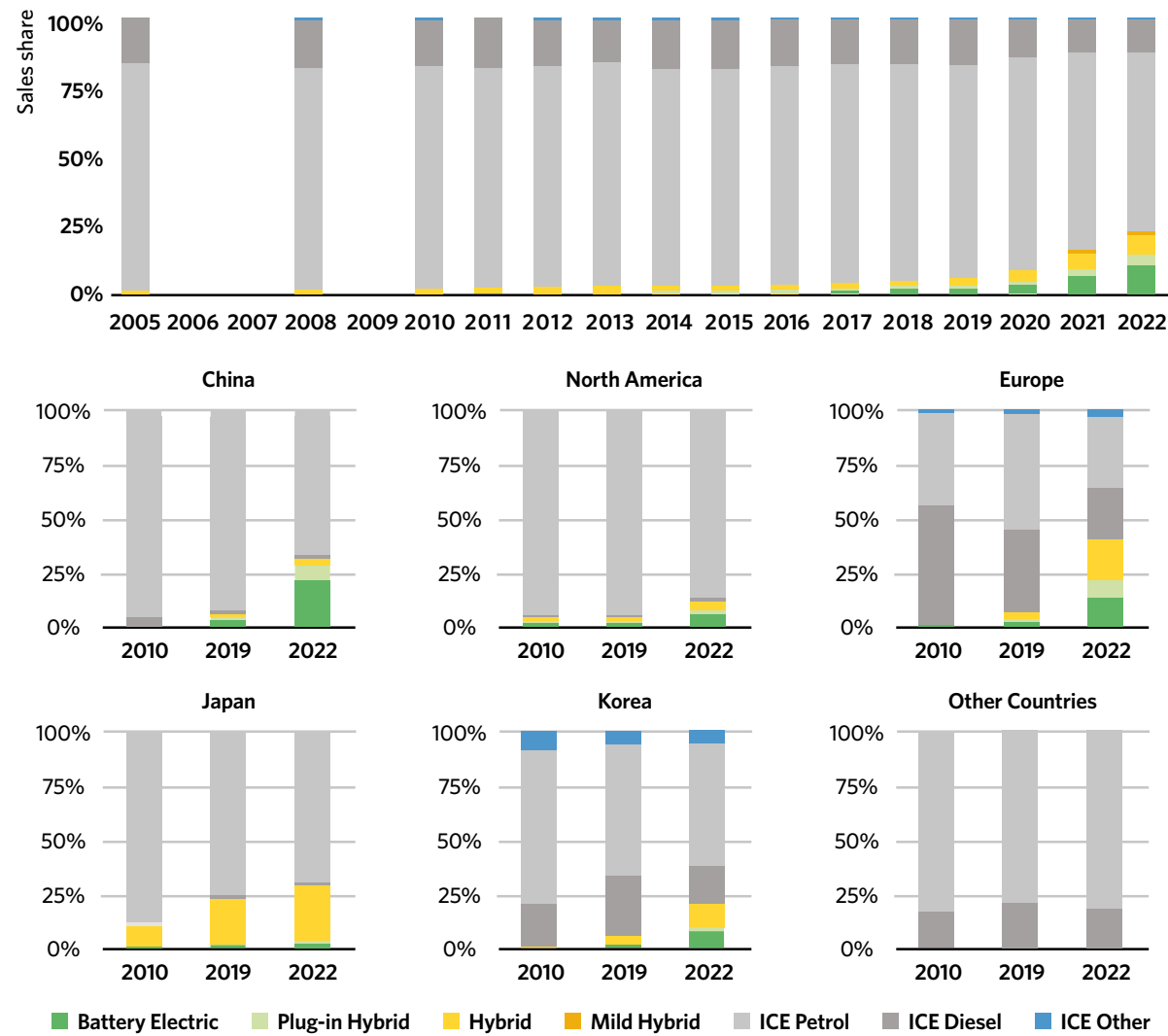
respectively, in 2019. Since then, hybrid sales have further increased in Korea, reaching a 12% market share in 2022. From 2019 onwards, hybrids have also made inroads in the European market, mostly driven by regulatory pressures to reduce fuel consumption and reflecting increased model availability. Hybrid sales increased in Europe from 4% in 2019 to 19% in 2022. Hybrids also grew in market relevance in North America, with sales shares reaching 5% in 2022. Despite a growing trend, hybrid vehicles have small market share in China, reflecting a strong policy focus on BEVs.

FIGURE 6: Trends in the tailpipe CO<sub>2</sub> emissions of new vehicles in major car markets



Sources: this assessment (details in the Annex) based on IEA, 2019a; IEA, 2021a; EEA, 2023a; EEA, 2023b and Marklines data.

FIGURE 7: LDV sales shares by powertrain: global and in selected markets



Notes: ICE stands for internal combustion engine - Other includes compressed natural gas (CNG) and liquefied petroleum gases (LPG) powered vehicles.

Sources: this assessment (details in the Annex) based on IEA, 2019a; IEA, 2021a; EEA, 2023a; EEA, 2023b and Marklines data.

PHEVs and BEVs, accounted for limited shares at the global level until 2016, at which point sales surpassed two million units (IEA, 2017). By 2019, EVs reached 2% of global sales. Norway was an early adopter, with shares well above global average already before 2019. By 2019, EV sales accounted for 56% of the market in Norway, more than ten times the 5% share of China and the 3.5% share for the European market as a whole (IEA, 2020 and this assessment). EV sales shares increased sharply in 2020 in Europe, with OEMs selling more EVs to comply with the more stringent CO<sub>2</sub> emission standards, as they integrated EV-specific incentives mechanisms.<sup>13</sup> In that year Europe was the largest EV market. Its EV sales share tripled and reached 10% (IEA, 2021b and this assessment). In 2021, the same trend occurred in China, where the EV sales share tripled over the previous year, reaching 15% (IEA, 2022 and this assessment). EV sales accelerated significantly in 2022 also in North America and Korea, with EVs reaching 7% and 10% of the market, respectively. In other developing and emerging economies, EV sales shares are still below 2%. Despite this, EVs accounted for 14% of all new LDV sales globally. Of these, two-thirds are pure battery electric vehicles while the rest are PHEVs (IEA, 2023b and this assessment).

## 2.4 VEHICLE SALES BY SEGMENT

International regulations define passenger cars as power-driven vehicles with four or more wheels destined primarily for the carriage of people (UN, 2005, UN, 2023). The passenger car market is divided into different segments, based on vehicle size and shape. Conventional cars typically include sedans, hatchbacks, or multipurpose vehicles. Larger forms of passenger

cars, with higher ground clearance and height and that may have initially been designed to be able to drive off-road, include the so-called Sport Utility Vehicles (SUVs) and, in specific markets (mainly in North America) also pick-up trucks.

For the purposes of this report, the passenger car market is divided into five categories: small, medium, and large conventional cars and small and large SUVs. Efforts were made to harmonize segment definitions across all vehicle markets.

All else held equal, SUVs tend to have a higher specific energy consumption than cars, due to a larger cross-sectional area (which increases air drag) and larger weight (which increases the energy needed for acceleration, i.e. to overcome inertia). Light commercial vehicles (LCVs) are primarily intended for the carriage of goods. They tend to be larger than cars and have more space for freight than for passengers, but they also share many of the technology characteristics (especially in terms of powertrains) of cars and, for this reason, are often subject to similar regulatory requirements. Table 2 shows popular vehicles of these categories in each of the main car markets.

All else held equal, SUVs tend to have a higher specific energy consumption than cars, due to a larger cross-sectional area (which increases air drag) and larger weight (which increases the energy needed for acceleration, i.e. to overcome inertia). Light commercial vehicles (LCVs) are primarily intended for the carriage of goods. They tend to be larger than cars and have more space for freight than for passengers, but they also share many of the technology characteristics (especially in terms of powertrains) of cars and, for this reason, are often subject to similar regulatory requirements. Table 2 shows popular vehicles of these categories in each of the main car markets.

TABLE 2: Top selling vehicle models by segment in key markets

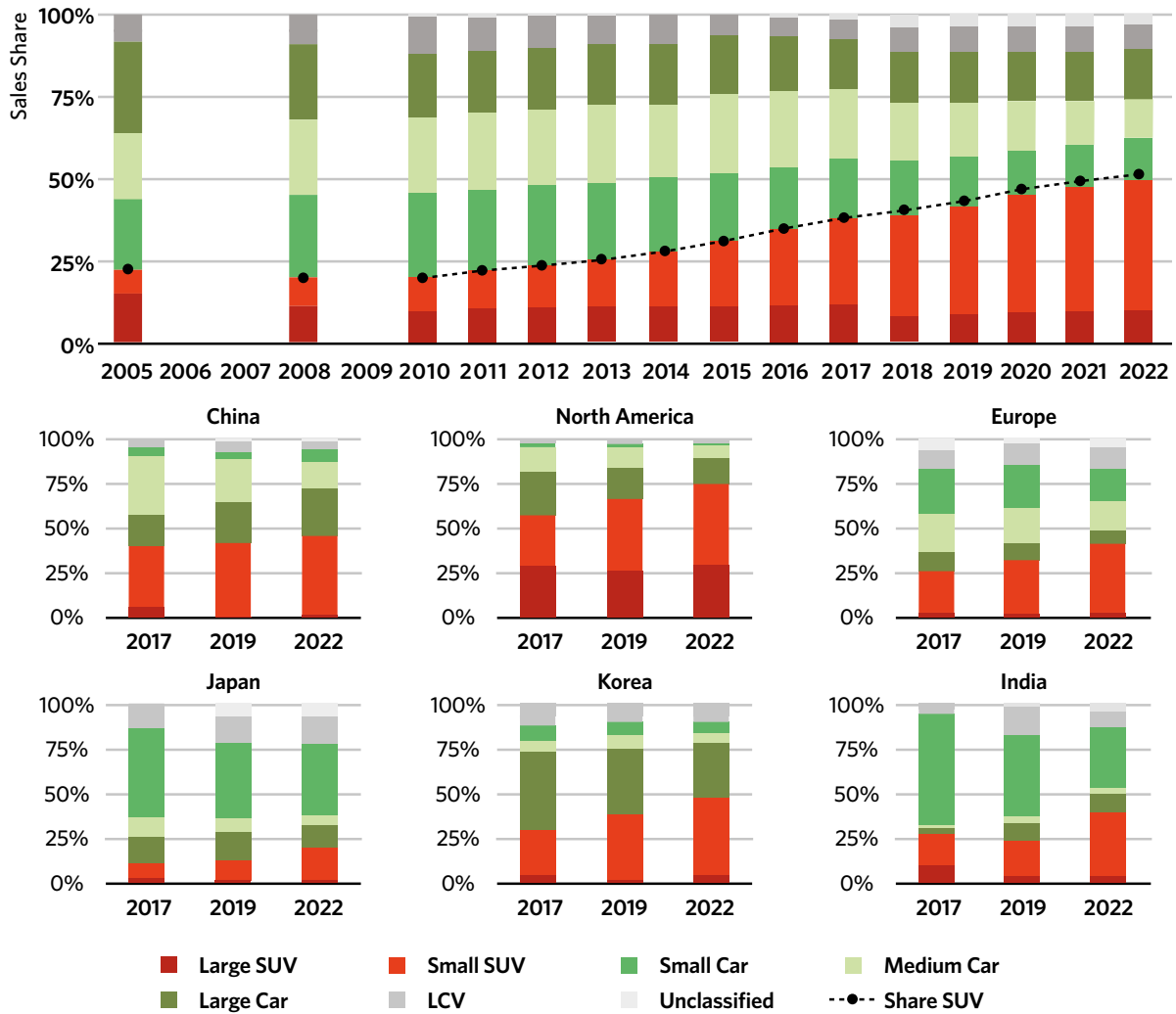
| Market        | Small car               | Medium car     | Large car     | Small SUV         | Large SUV  | LCV                 |
|---------------|-------------------------|----------------|---------------|-------------------|------------|---------------------|
| China         | Wuling Hongguang Miniev | VW Lavida      | Toyota Camry  | Haval H6          | Li L9      | Foton Xian-gling M1 |
| Europe        | Fiat 500                | VW Golf        | Audi A4       | WV T-Roc          | BMW X5     | Renault Trafic      |
| United States | Kia Rio                 | Toyota Corolla | Tesla Model 3 | Chevrolet Equinox | Ford F-150 | Ford Transit        |

Figure 8 shows global LDV sales by market segment, clearly illustrating that the main development observed over the period covered by this analysis (2019-2022) has been an increase in the share of SUVs and a corresponding decrease in the sales of cars (especially small and medium cars). On the global scale, SUVs saw their market share rise from 22% in 2005 to roughly half of the LDV market (including cars, SUVs, and LCVs) in 2022.

In addition to an increase across all major markets in the market share of SUV, Figure 8 – which includes details for the main global automotive markets – also shows significant differences in market segmentation across countries.



FIGURE 8: LDV sales by segment: global and in selected markets



Sources: this assessment (details in the Annex) based on IEA, 2019a; IEA, 2021a; EEA, 2023a; EEA, 2023b and Marklines data.



The United States is the country where SUVs account for the largest share of the market (75% in 2022); Canada and Australia have similarly high SUV shares (79% and 76% in 2022, respectively) (not shown in Figure 8). The North American vehicle market is also characterized by the highest share of Large SUVs, which include vehicles that are locally defined as “full sized SUVs” and “pick-ups,” and are not common in other parts of the world. Large SUVs accounted for one quarter of all vehicle sales in 2022. Growth in these segments has remained strong, with the overall SUV market share increasing by 9 percentage points from 2019 to 2022.

In China, SUVs accounted for 45% of the market in 2022, a share that increased by 4 percentage points from 2019. Nearly all SUVs sold fall in the small SUV category, as is the case in most other global markets. Large cars also account for a significant share of the market (26%) in 2022, up by 3% since 2019. China has witnessed, over the past decades, not only a surge in vehicle demand, but also a fast transition from smaller vehicles to larger ones, as the disposable income of its citizens rose.

Europe’s share of SUVs is the lowest among the three largest global markets, accounting for 41% of all sales. However, SUV sales in Europe have also consistently grown since 2017. Conventional cars still account for the majority of vehicles sold, however the share of medium cars has been shrinking fast, while small SUV sales increased.



The Korean market has shown similar recent trends in segmentation as Europe, with the exception of the relative shares of conventional cars; large cars have larger market shares in Korea, and shares of small and medium cars are smaller.

Japan has similar market segmentation characteristics to Europe, but the share of small cars is even greater, and that of SUVs even smaller. Europe and Japan share a high reliance on oil imports. The significant resilience of small cars also points to a strong peculiarity of the Japanese market.<sup>14</sup>

India also has high shares of small car sales, following a long-standing tradition of high fuel taxes and

domestic manufacture of small vehicles. Recent market developments, however, show an erosion of market shares of small vehicles, in favour of large cars and small SUVs.

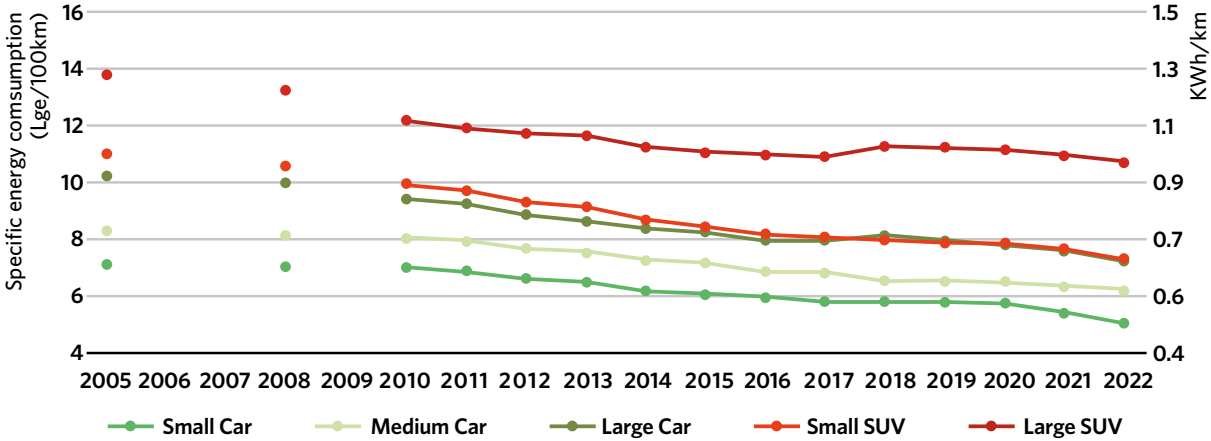
Specific energy consumption varies significantly by vehicle segment: large SUVs are the most energy intensive type of vehicle, while small cars are the most efficient (Figure 9). Small SUVs and large cars are roughly equivalent since the former tend to have higher weight and larger cross-sectional area, while the latter tend to have higher power ratings. When looking at trends, it becomes clear that not all segments have improved at the same rate. In the period 2010 to 2019, small SUVs have undergone the fastest efficiency improvements, as this segment transitioned and evolved from a niche composed mostly of smaller 4x4 vehicles to the world’s most popular segment. The specific energy consumption of small SUVs improved by 3% per year, while all other segments improved at rates between 1% and 2.5% per year. In the period between 2019 and 2022, the strongest efficiency improvements have been observed in small cars, with specific energy consumption declining at a staggering 4.3% per year in the case of small cars, driven mostly by rapid adoption of electric cars, in particular in China.

As explained in Section 2.3, electric powertrains significantly reduce energy consumption. However, their market penetration is not equally distributed

across segments, nor across geographies. In China, EVs accounted for three-quarters of small car sales in 2022 (Figure 10), with the Hongguang mini EV, a sedan with a top speed of around 100 km/h that sold from around USD 6,500 to up to USD 15,000, being the top-selling model both in 2021 and 2022 (van Vyk, 2023). Chinese automakers have been competing intensely for market share in the small electric car segment, and have been willing to sustain tight margins; Wuling further cut the starting price of the Hongguang mini EV to around 4,300 USD in May 2023 (Reuters, 2023). EVs sold in other segments are often sold at far higher price points, either by established EV leaders such as BYD and Tesla or by new market entrants such as Nio, Li Auto, and XPeng, who have yet to post profits (Leplâtre, 2023).

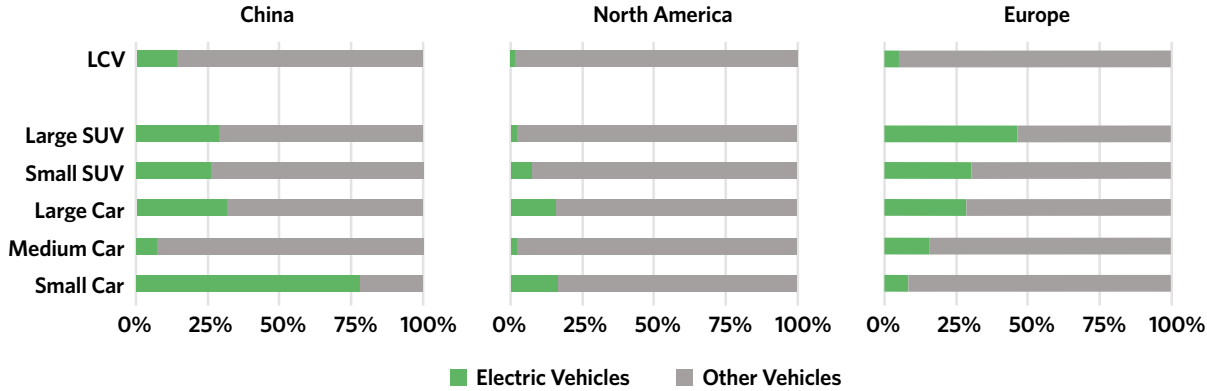
In Europe and the United States, the share of electric sales in the small car segment is far lower than in China (Figure 10). In Europe, large SUVs are the most heavily electrified segment, with nearly half of all sales being electric, followed by the much larger segment – in terms of sales volumes – of small SUVs; with European automakers apparently seeking to replicate the possibility to lock-in higher margins by selling more SUVs even in the rapidly electrifying market. North America sees a different dynamic, where EVs are mostly found in small and large cars (with Tesla leading in the large car segment). Across all three markets, the medium car segment has relatively low levels of EV penetration.

FIGURE 9: Global specific energy consumption by vehicle segment



Sources: this assessment (details in the Annex) based on IEA, 2019a; IEA, 2021a; EEA, 2023a; EEA, 2023b and Marklines data.

FIGURE 10: Electric vehicle sales share by vehicle segment in key automotive markets, 2022



Note: Electric vehicles include plug-in hybrid and battery electric vehicles.

Source: this assessment (details in the Annex) based on IEA, 2019a; IEA, 2021a; EEA, 2023a; EEA, 2023b and Marklines



## 2.5 VEHICLE SIZE AND WEIGHT

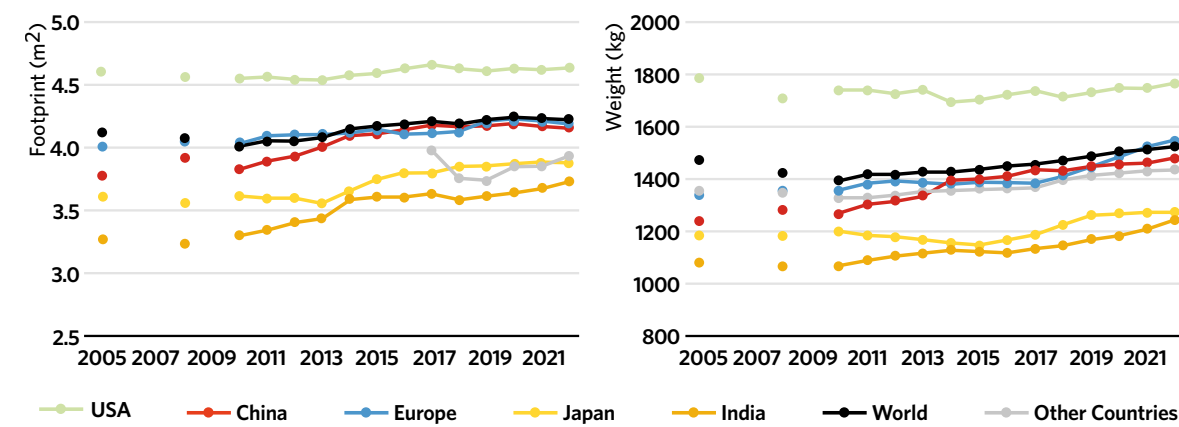
Two major global trends are affecting the average vehicle size (best represented by the attribute of footprint)<sup>15</sup> and weight<sup>16</sup> are the shift of market segments towards SUVs and electrification.

Both weight and footprint have been on the rise since 2010 (Figure 11), the year that also marks a change in pace in the transition across market segments globally (Figure 7). The shift from (especially small and medium) cars to SUVs has been a key driver of larger average footprint and

greater weight.<sup>17</sup> As shown in Table 3 and Figure 5, for ICEVs this shift is also associated with systematic differences in specific fuel consumption across segments, pointing to a key role of the shift in market segmentation in limiting energy efficiency improvements for LDVs.

Recent developments, however, following the year 2020, also suggest that the increasing trend for vehicle footprint has slowed down, and vehicle size even experienced a slight decline in 2022 (Figure 12). Vehicle weight, on the other hand, continued to increase. A major determinant of this development is the adoption of EVs. The reason is that EVs tend to have similar dimensions (and footprint) to ICEVs, but greater weight, largely due to the heavy battery that they carry (as further detailed in Chapter 3).

FIGURE 11: Footprint and weight trends across major LDV markets



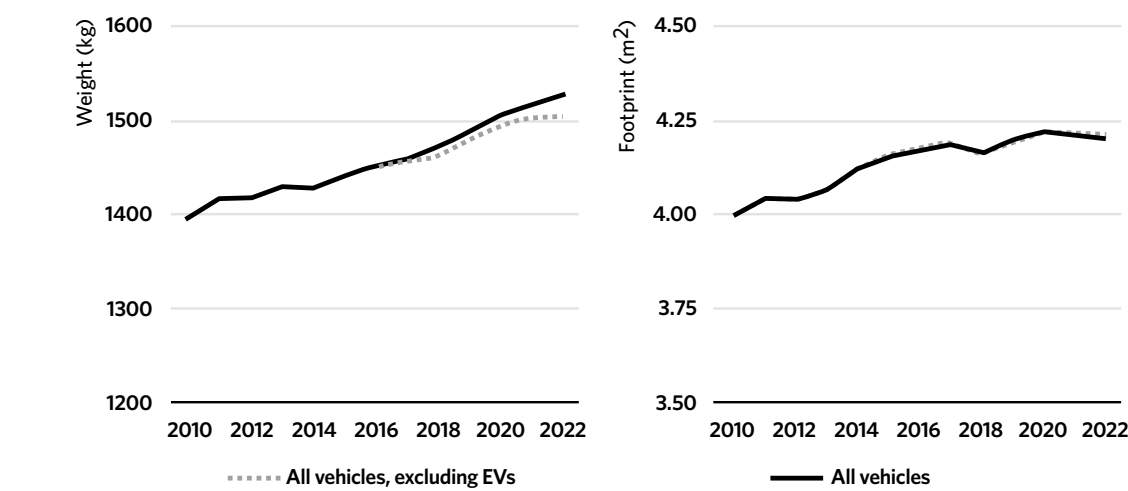
Sources: this assessment (details in the Annex) based on IEA, 2019a; IEA, 2021a; EEA, 2023a; EEA, 2023b and Marklines data.

TABLE 3: Average vehicle characteristics by segment (left) and change in sales share by segment (right)

| World      | Average footprint | Average weight | Specific Energy Consumption |        | Market share change |           |
|------------|-------------------|----------------|-----------------------------|--------|---------------------|-----------|
|            | m²                | kg             | Lge/100km                   | kWh/km | 2010-2017           | 2017-2022 |
| Small car  | 3.5               | 1050           | 4.9                         | 0.46   | -9%                 | -3%       |
| Medium car | 4.0               | 1350           | 6                           | 0.56   | -3%                 | -8%       |
| Large Car  | 4.5               | 1660           | 6.5                         | 0.60   | -3%                 | -1%       |
| Small SUV  | 4.1               | 1520           | 6.6                         | 0.61   | 19%                 | 10%       |
| Large SUV  | 5.2               | 2140           | 10.5                        | 0.98   | -2%                 | 1%        |
| LCV        | 4.4               | 1670           | 7.6                         | 0.71   | 18%                 | 11%       |

Source: this assessment (details in the Annex) based on EEA, 2023a; EEA, 2023b and Marklines data.

FIGURE 12: Global vehicle weight (left-hand side) and footprint (right-hand side) trends, including and excluding EVs



Sources: this assessment (details in the Annex) based on IEA, 2019a; IEA, 2021a; EEA, 2023a; EEA, 2023b and Marklines data.



# 3 ANALYSIS OF THE VEHICLE MARKET DEVELOPMENTS AND IMPLICATIONS FOR POLICY ACTION

This Chapter focuses on the two major trends identified in Chapter 2: a shift in market segments towards SUVs and a recent rapid development of vehicle electrification. The analysis considers the impact of both these developments on energy use per km, direct CO<sub>2</sub> emissions, road safety, and equity. Specific sections cover the implications that the EV transition had on the SUV shift, and makes the case that the combined shift to SUVs and the EV transition are leading to increased risks of a global divide. The last section lays out reasons that justify the policy interventions elaborated in Chapter 4.

## 3.1 IMPACTS OF THE SHIFT TOWARDS SUVs

This section outlines impacts that the shift towards SUVs had on energy, direct CO<sub>2</sub> emissions per km<sup>18</sup> and vehicle weight, also considering related implications for road safety and equity.

### 3.1.1 ENERGY AND CO<sub>2</sub> EMISSIONS

Figure 13 shows historical evolutions in specific energy consumption for the main automotive markets globally, comparing developments in cases that include or exclude a shift in market segmentation, taking the year 2010 as the baseline. The data indicate that energy use per km for ICE vehicles without the shift towards SUVs (and the subsequent increases in vehicle size, weight and power) could have improved

at an average annual rate that is 30% higher than it actually did.<sup>19</sup> The gap is larger in China (around 50%) and narrower in Europe (around 20%), as the first focused on EVs while the other focused on improved technologies for ICEs (as discussed in Section 3.3.).

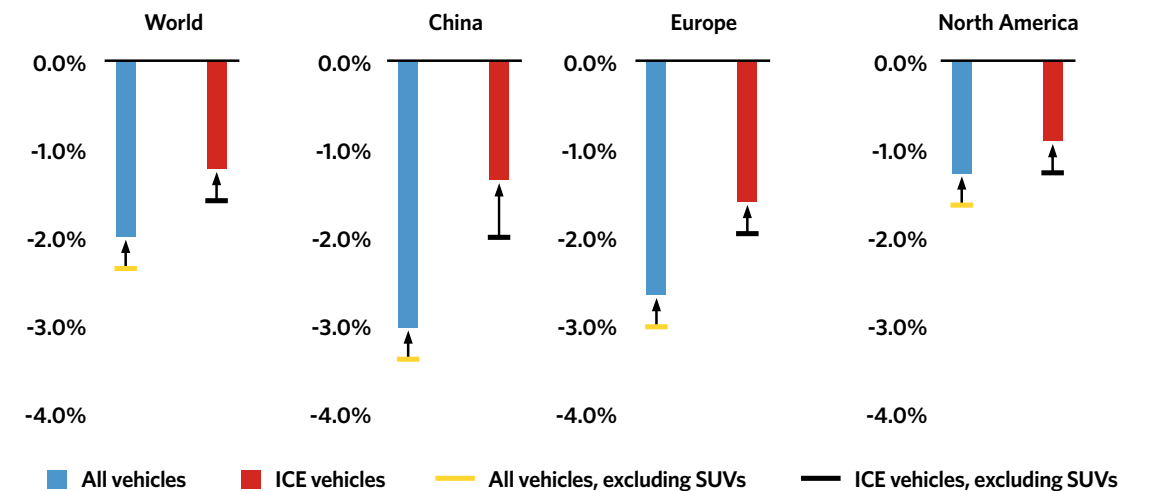
Gaps in terms of direct emissions of CO<sub>2</sub> are even larger, as CO<sub>2</sub> emissions are almost directly proportional to fuel use for ICEVs,<sup>20</sup> and EVs do not emit CO<sub>2</sub> at the tailpipe. Gaps are slightly narrower with lifecycle accounting of greenhouse gas emissions, as:

- Light-duty EVs have significantly lower lifecycle emissions, over their lifetime, with respect to ICEVs (Bieker, 2021), but the lifecycle emission gap, especially in places with carbon-intensive grid mixes, is not as wide as the energy efficiency differential.
- The variation of specific energy consumption for EVs across vehicle segments is small (as shown in Figure 5 for the case of Europe for 2022, and as also shown in IEA, 2019a, with data from different geographies).

### 3.1.2 VEHICLE WEIGHT

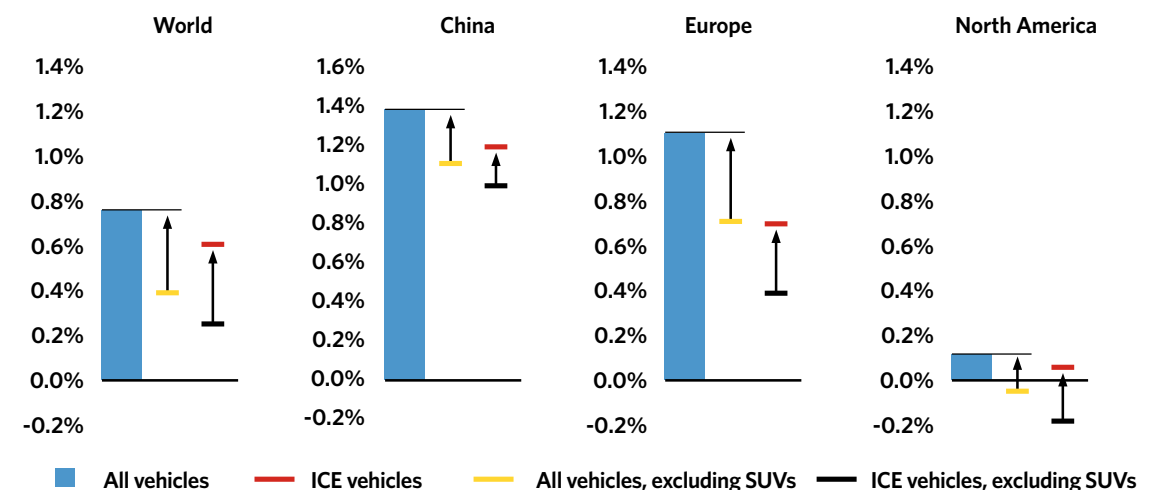
Figure 14 illustrates trends in vehicle weight, globally and in the main markets, excluding the effect of the EV transition (discussed in Section 3.3.2), but including the impacts of the SUV shift. As SUVs are heavier than small and medium cars (Table 3), and as the main shifts in market segmentation consist of a decline in sales share of small and medium cars and an increase in small SUV sales shares, the data in Figure 14 indicate

**FIGURE 13:** Global yearly rate of change in specific energy consumption, with a focus on the impact of the SUV shift, 2010-2022



**Note:** Observed rate is the yearly rate of improvement in SEC. Without EV, with SUV: is the rate of improvement that would have been achieved without EV (BEV and PHEV) sales. Without SUV, with EVs: is the rate that would have been achieved if LDV segment share had remained the same as it was in 2010. Without SUV, without EVs: is the rate that would have been achieved with the same LDV segment sales share as 2010 and without EV sales.  
**Sources:** this assessment (details in the Annex) based on IEA, 2019a; IEA, 2021a; EEA, 2023a; EEA, 2023b and Marklines data.

**FIGURE 14:** Rate of change in vehicle weight, with a focus on the impact of the SUV shift, 2010-2022



**Sources:** this assessment (details in the Annex) based on IEA, 2019a; IEA, 2021a; EEA, 2023a; EEA, 2023b and Marklines data.

that, in the absence of the SUV shift, vehicle weight increases could have been more than halved relative to the increase that actually occurred (when excluding impacts of the EV transition) between 2010 and 2022.

Region-specific results shown in Figure 14 indicate that net savings in weight (and related material demand)

could have been stronger, in percentage terms, in Europe and China than in the United States. They also indicate that weight increases have been more pronounced, over time, outside of the United States, even if average LDV weight in the North American market is still well above all others in absolute terms (by about 15-20%).

3.1.3 ROAD SAFETY

The shift to SUVs also had implications for road traffic injuries. Worldwide, road traffic injuries are the leading cause of death for children and young adults aged 5-29 years, and the cost of road traffic crashes is estimated at around 3% of GDP across most countries (WHO, 2022).

Studies analysing the impact of increases in vehicle weight and size on motorist, passenger, and pedestrian safety show that collisions with larger, heavier vehicles are more likely to result in more severe injuries (including brain damage) or death, both to drivers of smaller vehicles and to cyclists and pedestrians (Ossiander et al., 2014; Van den Berghe, 2021; Edwards and Leonard, 2022; Nuyttens and Ben Messaoud, 2023). Such studies primarily focus on the impacts of larger and heavier cars in North America (and especially in the United States – where car crashes are among the leading causes of death) and Europe.

Recent analyses conducted in the United States find that large trucks, minivans and SUVs do not necessarily make the roads more dangerous, in aggregated terms, for drivers or passengers. However, risks are distributed unevenly. Increased injury and mortality rates for occupants of smaller vehicles are generally offset by lower rates for occupants of larger vehicles (Ossiander et al., 2014).

In addition to their greater weight and size, pickup and SUV designs diverge somewhat across key parameters that influence crash safety (for instance

ride height) from cars. In the United States, this design incompatibility has decreased following a 2009 voluntary commitment among automakers to standardize the height of energy-absorbing structures across all vehicles. Nevertheless, weight differences, together with some degree of continuing incompatibility, increase mortality risks for drivers of cars in crashes between pick-ups or SUVs and cars by around 25% (Monfort and Nolan, 2019).

Evidence also shows that the severity of injuries and the risk of mortality is substantially higher for pedestrians that are hit by minivans, pickups, and SUVs, due to factors such as greater impact force, higher front-end designs, and larger driver blind spots (Tyndall, 2023, Nuyttens and Ben Messaoud, 2023). In the United States, pedestrians hit by a pickup truck are roughly 70% more likely to die than those hit by a car, and those hit by an SUV are twice as likely (Tyndall, 2023). If all light trucks (minivans, pickup trucks and SUVs) sold from 2000-2019 had been cars, pedestrian deaths in 2019 could have been reduced by 30% (Tyndall, 2021).

3.1.4 EQUITY

The analysis developed by the IEA and the ICCT in 2017 (as summarized in Figure 15) shows that vehicle prices tend to be higher, across all main automotive markets, for small SUVs – the segment that keeps experiencing significant increases in market shares – than for small and medium cars – the segments that, globally, experienced the most relevant contractions.

Taking central estimates, for all regions, the gap between a medium car and a small SUV price is on the order of 10% to 20%, and 25% to 60% between a small car and a small SUV, with the largest gap in developed economies with low fuel taxes (IEA, 2019a).<sup>21</sup> Similar gaps emerge from a recent comparison between small/medium cars and small SUVs for different European brands and models, which found that small SUVs carry a price premium of 8% to 30% with respect to comparable small and medium cars (Krajinska, 2023).

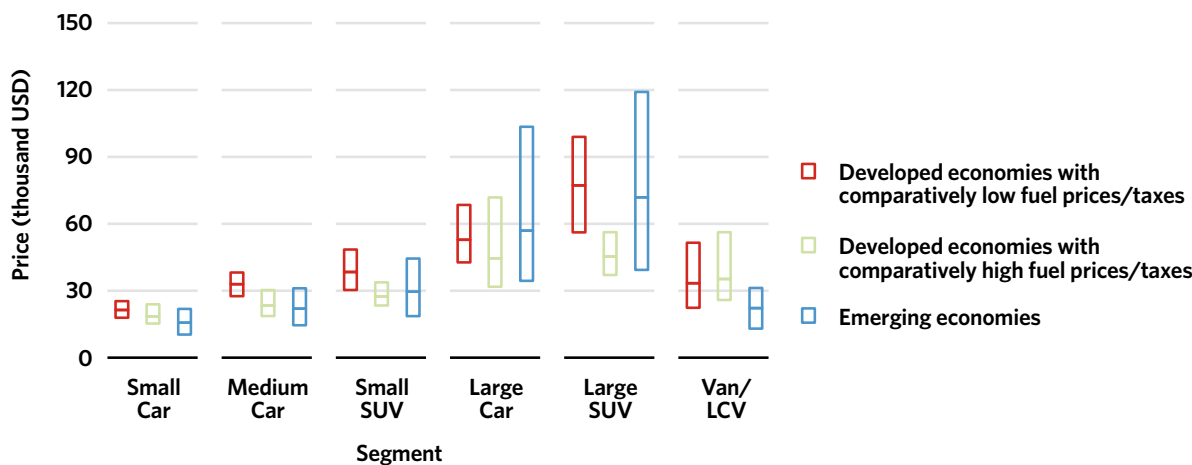
Figure 16 indicates also that ICE powertrain costs make up lower shares of the total vehicle price for small SUVs with respect to small and medium cars. This suggests that a shift in market segmentation towards SUVs, without major changes in powertrain technology, is not only likely to lead towards increases in turnover, but also towards larger profit margins, for manufacturers. Such a development is confirmed also by analyses pointing to larger margins available for larger, premium ICEVs (Sussams et al., 2018; Slowik et al., 2022). This is also consistent with reports showing increases in OEM profits, even with declining sales (Welch and Naughton, 2023 and Hersh, 2023).

Combining these estimates with the decade-long tendency of a global shift towards SUVs shows clearly that the resulting impact led to significant increases in OEM revenues with respect to a counterfactual without the shift. Drawbacks related to potential market growth higher than what has been observed

are possible and are also consistent with the increases in average vehicle age in replacement markets like the EU and North America (European Environment Agency, 2023, for Europe and Parekh and Campau, 2022, for the United States),<sup>22</sup> even despite increases of average income levels, which provided households with a larger budget for vehicle purchases). The significant price gaps shown in Figure 15, combined with a continued expansion in SUV sales shares, are also consistent with the increased profitability registered by the automotive industry after 2020, taking place even with a decline in sales volumes (Stricker and Correa, 2023), and notwithstanding a contextual effect due to increased inflation.

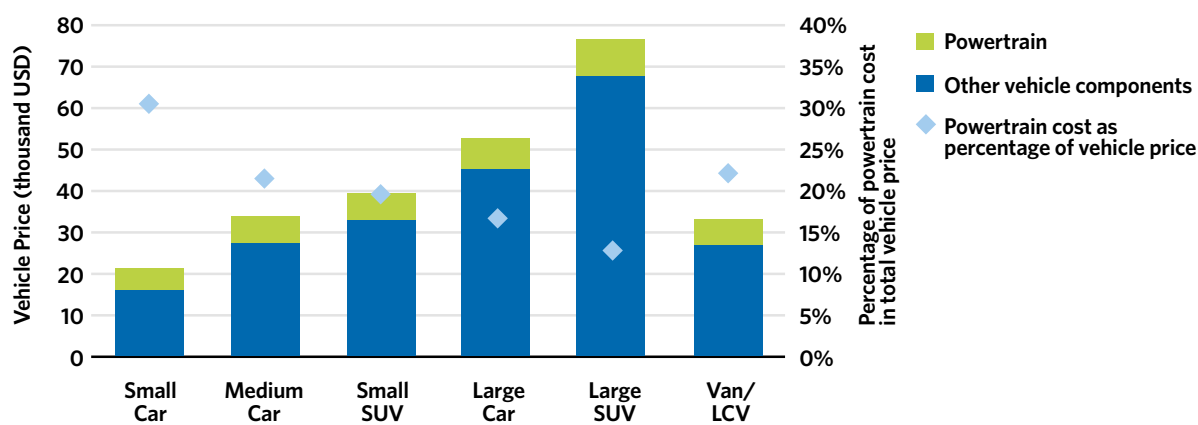
This also resulted in relevant affordability and equity challenges, within and across countries. Since 2019, average new car sales prices have risen faster than inflation in most regions. For example, the average price of new cars in the United States in early 2023 was 30% higher than in 2019 (this compares prices of the same cars, and hence is not a result of the shift to SUVs) (Bureau of Labor Statistics, 2023). New car buyers tend to be higher-income households (Krisher, 2022) that can afford larger and more expensive vehicles. However, the choices made by this segment of the population affect the choices and affordability of car sales for the second-hand market (see, for instance, Krisher, 2022).<sup>23</sup> The lower-income segment of the population that relies on the second-hand market is also likely to be affected by the recent average price increase of vehicles, which was compounded by a shift towards SUVs.

FIGURE 15: Evolution of vehicle prices, by segment and economic cluster, for the year 2017



Source: adapted from IEA, 2019a, with revision of labels used for vehicle segments to match names used in this report.

FIGURE 16: Share of powertrain costs in internal combustion engine vehicle price for different vehicle segments



Source: adapted from ITF, 2020a, with revision of labels used for vehicle segments to match names used in this report.



This effect is stronger in high-income countries, where there is a higher share of SUV sales. However, data shows that the move towards larger market segments is a global phenomenon. Data on vehicle prices by segment and global region, available from IEA, 2019a (and shown in Figure 15) show a clear price gap between cars (especially small and medium cars) and small SUVs. As sales shares of small and medium cars shrink and shares of small SUVs rise, equity impacts are also likely to emerge.

The dynamics of segment shifts in low- and medium-income countries are the combination of different factors that vary country by country:

- New car buyers in low-income countries tend to represent a small and very high-income segment of the population, therefore their high budget availability and preferences lead them to purchase increasingly large vehicles. In such countries, lower income segments of the population do not have the financial ability to enter the new car market, therefore the demand for smaller, more affordable new cars is weak.
- In medium-income countries, where vehicle ownership is on the rise and demand growth is strong, small and medium cars are retaining market share as first-time new car buyers in these countries are more likely to be able to afford smaller vehicles. The rapid growth dynamics also mean that OEMs can retain sufficient profit margins. Both justify lower SUV market shares, in comparison with high-income countries.

Equity impacts due to increases in new vehicle prices in developed countries may also impact second-hand vehicles sales in low- and medium-income countries, where second-hand vehicle purchases are a more

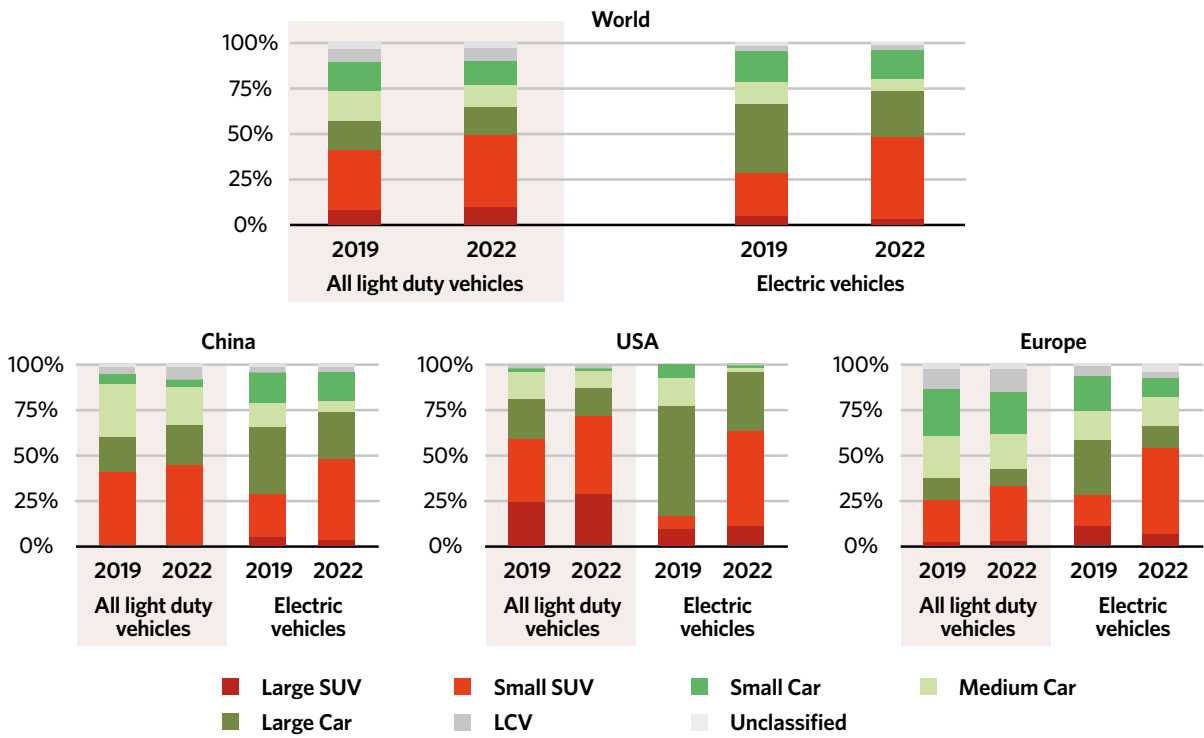
common path to access motorization. Therefore, a higher average price of imports driven by an increased availability of larger cars exports can lead to greater challenges in gaining access to motorized mobility in countries strongly reliant on second-hand vehicle imports. Due to greater constraints in the range of mobility choices, equity impacts due to vehicle price increases are also more relevant in countries with limited affordable, accessible, and reliable alternatives to personal vehicles (such as public transport).

### 3.2 THE ROLE OF EVS IN THE SHIFT TOWARDS SUVs

Figure 17 provides additional insights across the main global markets compared to the information already shown in Figure 10.<sup>24</sup> The figure illustrates the evolution of market segmentation across all powertrains (left-hand bars) and for EVs (right-hand bars), between 2019 and 2022. The figure shows that EVs are not exempt from the shift towards SUVs: the market share of electric SUVs (especially small electric SUVs) has grown substantially between 2019 and 2022, in all markets. This marks an increase in product diversification, as EVs also gained overall market shares, moving beyond earlier market deployment strategies, more focused on large, premium car models.

EV shares declined in the small car segment between 2019 and 2022, across all markets. This is primarily

FIGURE 17: Powertrain shares globally and in major EV markets globally, with EVs singled out, 2019 and 2022



Sources: this assessment (details in the Annex) based on IEA, 2019a; IEA, 2021a; EEA, 2023a; EEA, 2023b and Marklines data.

due to shifts in Europe and the United States (where this was further exacerbated, in 2023, by discontinuation of the only electric small car by a US OEM). As shown also in Figure 6, EVs in the small car segment maintained significant market shares in China. Globally, EVs also have limited market share within the large SUV segment. This is consistent with sizable market shares of large SUVs limited to North America, where EVs also had – to date – lower market penetration, in comparison with China and Europe (despite recent increases).

### 3.3 IMPACTS OF THE EV TRANSITION

Similar to the case of the SUV shift covered in Section 3.1, this section assesses impacts on the EV transition on energy and CO<sub>2</sub> emissions, weight and material needs, road safety, and equity in different sub-sections.<sup>25</sup>

#### 3.3.1 ENERGY AND CO<sub>2</sub> EMISSIONS

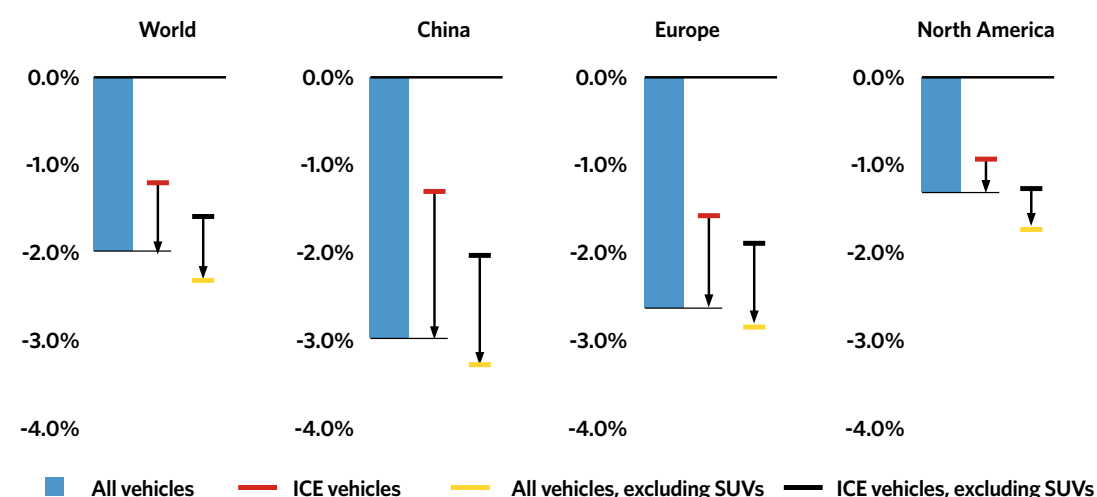
Chapter 2 highlights the key role EVs have played in reducing the specific energy consumption of vehicles after 2020. Section 3.1.1 discusses impacts of the shift towards SUVs on energy efficiency and CO<sub>2</sub> emission trends, excluding the effect of electrification, pointing out that the SUV shift led to significant reductions in the rate of improvement of energy efficiency compared to what could have materialized without this shift, and resulting in upward pressure on energy demand and CO<sub>2</sub> emissions.

This section analyses the specific effect of increased EV deployment on the gap in energy use per km (outlined in Section 3.1.1), considering the impacts on specific energy consumption of the shift to SUVs in EVs. Like Figure 14, Figure 18 shows historical evolutions in specific energy consumption for the main automotive markets globally, comparing developments that actually occurred with a counterfactual that excludes the shift in market segmentation (on the top of the results already included in Figure 14).





**FIGURE 18:** Global yearly rate of change in specific energy consumption, with a focus on the impact of the EV transition, 2010-2022



**Sources:** this assessment (details in the Annex) based on IEA, 2019a; IEA, 2021a; EEA, 2023a; EEA, 2023b and Marklines data.

Overall, results shown in Figure 18 point toward net increases in energy savings from EVs, across all markets. Without EVs, savings would have been 40% lower at the global level.

The role of EVs is the result of two effects. On one hand, EVs have markedly lower specific energy consumption versus competing technologies (see also Figure 5, showing this clearly for the case of the European market). On the other hand, like all vehicles, specific energy consumption for EVs also increases with increasing vehicle weight (and therefore also with the segment shift towards SUVs), even though these increases are less pronounced than for other powertrains.

Energy savings due to EVs are stronger in recent years and in markets that saw a larger EV market penetration. In China and Europe, electrification had a very strong role in the decrease of average specific energy consumption of new vehicles. In the United States, impacts of the EV transition on trends of specific energy consumption are less pronounced, due to lower EV market shares as compared to China and Europe. From 2020 to 2022, electrification led to reductions in specific energy consumption that were roughly offset by the detrimental impact of SUVs.

### 3.3.2 VEHICLE WEIGHT

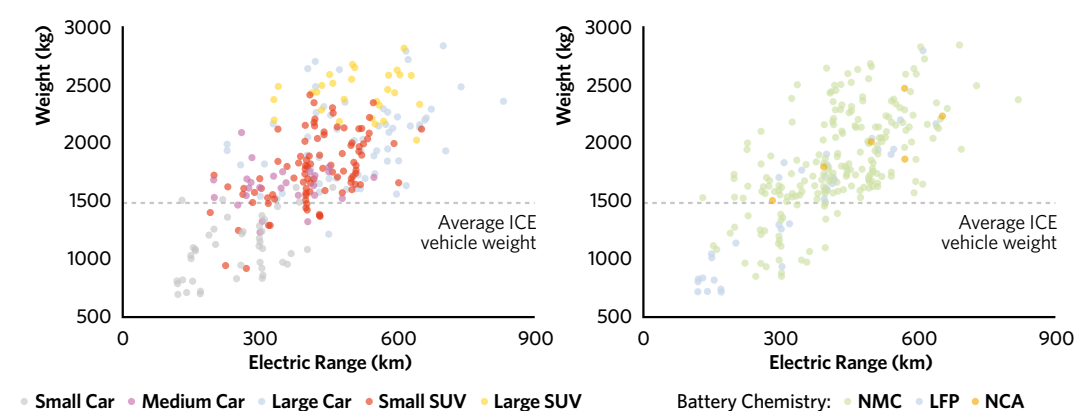
EVs are on average 13% heavier than equivalent ICEs. The differential in weight for EVs comes primarily from the weight of the battery, which in turn depends on

three factors: specific energy consumption, battery technology, and range.

Despite lower impacts on EVs, due to the possibility to recover energy in regenerative braking, specific energy consumption for EVs still varies across market segments. European data (Figure 5) show that small BEVs consume less energy, on average (14-15 Wh/km), than large all-electric SUVs (18-20 Wh/km). Small EVs also have lower vehicle weights than large EVs, as they need smaller batteries for the same range (Figure 19). Motor technology can also contribute to weight savings, since higher efficiency motors (usually using rare-earth rich permanent magnets) can deliver better specific energy consumption.

Battery technology (including chemistry and pack architecture) matters for vehicle weight because it determines the energy density of the battery (Wh/kg). Better technologies deliver more energy per unit weight and tend to be used more frequently on larger vehicles, with longer ranges (Figure 19). High nickel content chemistries tend to have higher cell-level energy densities that range from 240 to 340 Wh/kg, while lithium iron phosphate (LFP) chemistries range between 150 and 190 Wh/kg (Hasselwander et al., 2023, Battery Design, 2022, Frith et al., 2023). Pack technology is also very important, as there can be significant differences across chemistries, with LFP performing better than other chemistries, as also shown by BYD, with the blade battery (Frith et al., 2023). This opens up opportunities for its use on vehicles with larger batteries and longer ranges.

**FIGURE 19:** Weight as a function of electric range for battery electric vehicles

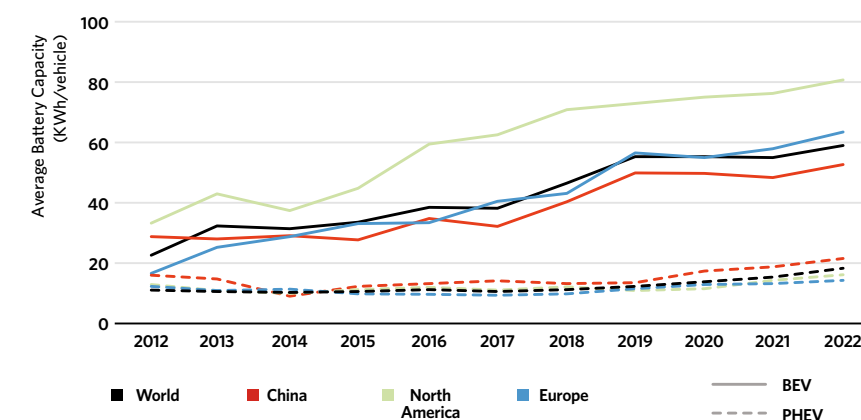


**Source:** analysis based on data from EV Volumes (EV Volumes, 2023).

The electric range of a vehicle is determined by battery capacity and weight (Figure 19), as well as by the vehicle aerodynamics and powertrain efficiency. All else being equal, range is directly proportional to battery capacity, and thus also vehicle weight. Figure 19 shows that, on average, adding 100 km of range adds 330 kg to vehicle weight for a BEV (less additional weight is needed for smaller BEVs, given their lower energy intensity). EVs with ranges below 400 km have a weight that is roughly similar to average ICE vehicles, while for longer range vehicles, weight rapidly increases.

The relevance of range as a key determinant of battery size is also important considering PHEVs and BEVs independently, since PHEVs are meant to rely on all-electric ranges mainly for trips with shorter distances – and therefore have smaller battery packs (Figure 20) – while they still rely on the HEV powertrain in charge-sustaining mode for longer distances.<sup>26</sup> As such, they come with the advantage of lower requirements in terms of battery materials, with respect to BEVs, and the disadvantage of having a weight penalty due to the ICE.<sup>27</sup>

**FIGURE 20:** Average battery capacity for PHEVs and BEVs globally and in the main LDV markets



**Source:** this assessment (details in the Annex) based on EV Volumes (EV Volumes, 2023).

# REDUCING CRITICAL MATERIAL REQUIREMENTS FOR EV BATTERIES BY REDUCING BATTERY SIZES

EV battery cathodes require high purity “critical materials” including lithium, cobalt, manganese, and nickel. Magnets that are in most EV motors (except for AC induction motors) require rare earth elements (mainly neodymium, and often also dysprosium, terbium, and praseodymium).

A massive scale-up of critical material mining, processing, and EV cell production will be required over the coming decade to enable the rapid growth of EVs required to meet global climate targets (IEA, 2023c). Scaling up to levels where supply can match demand growth will require closing gaps between global supply (based on expansion announcements) and EV battery demand, as well as ensuring that each step of the EV battery supply chain — mines, material processing, cathode and anode production and cell production — ramps up to full capacity at speeds equivalent to or better than what has been achieved to date. The supply gap for lithium is particularly acute – IEA assessed the gap between EV battery requirements in the Net Zero Scenario and announced production plans to 2030 to be just under 40% for lithium mining and processing (IEA, 2023c).

Rapid acceleration in EV demand, bolstered by ambitious EV deployment and industrial policies and

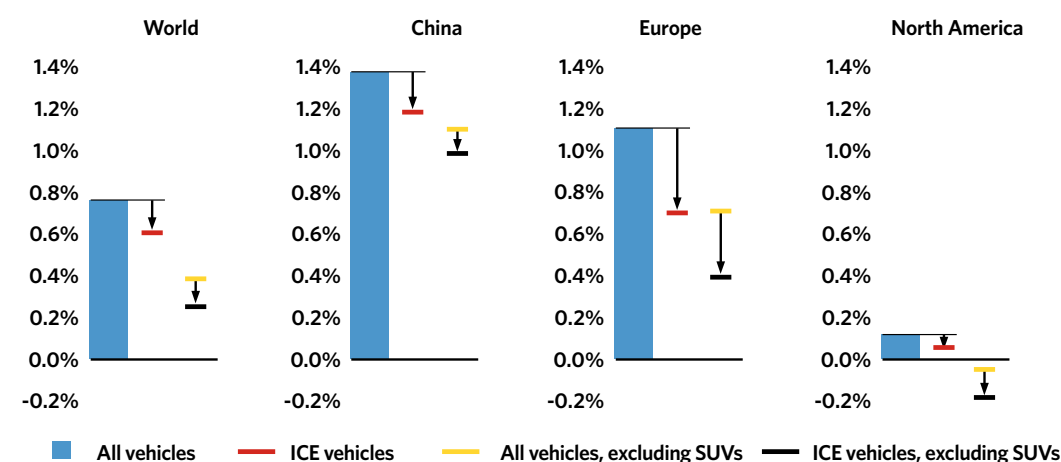
targets, has already begun to guide investment for new facilities, as well as development of innovative chemistries such as sodium-ion batteries for vehicle applications (Tapia-Ruiz et al., 2021). These are being explored by several Chinese battery makers, and are most viable in small EVs (as well as in electric two-wheelers due to lower energy density and lower cost).

For a given battery chemistry, mineral intensity scales linearly to battery capacity at the cell level. For example, 0.1 kg of lithium are needed per each kWh of capacity for NCA and NMC 811 cell chemistries (the intensities are similar for LMO, at 0.106 kg/kWh, and for LFP, at 0.095 kg/kWh).

Demand-side opportunities for right-sizing batteries could also help to close the material supply gap, as well as decrease risks posed by regional concentration of lithium (and other metal) mining and processing. For instance, returning to average battery capacities of around 40 kWh/vehicle (the global average in 2017), rather than 60 kWh/vehicle (the average in 2022 – as shown in Figure 20), would reduce lithium demand by around one-third. Other demand-side measures, such as reducing reliance on car ownership, together with EV battery recycling, could further reduce exposure to critical mineral risks (Riofrancos et al., 2023).



**FIGURE 21:** Rate of change in vehicle weight, with a focus on the impact of the EV transition, 2010-2022



Source: this assessment (details in the Annex) based on EEA, 2023a; EEA, 2023b and Marklines data.

Figure 21 shows weight trends, globally and in the main light-duty vehicle markets, considering both the SUV shift and the EV transition, similar to Figure 18 for specific fuel consumption. The indications emerging from Figure 21 are consistent with the considerations outlined in Chapter 2 and above, since they indicate that the EV transition led to net increases in weight trends, adding to the effect of the shift from small and medium cars to SUVs.

The effect is remarkable in the case of Europe, characterized by rapid growth both in EV shares and by higher EV penetration in the SUV segments. China exhibits a lower weight increase due to its EV transition, reflecting the fact that the majority of EV sales are in the small segment (Figure 10). In the case of North America, impacts of the EV transition are larger when the SUV segment shift is not taken into consideration, since EVs have mostly penetrated in small and large car segments to date.

## 3.3.3 ROAD SAFETY

Chapter 2 – in particular Section 2.5 – shows that vehicle electrification is having a significant effects on vehicle weight, contributing to the continuation of an upward trend, despite a flattening of the evolution of vehicle footprints. This contribution means that EVs are clearly not exempt from implications related to road safety. Available data on road safety point to a likelihood of passengers being killed in a collision with another vehicle

that increases by 12% for every 500 kg difference between vehicles (Shaffer et al, 2021). This is also what explains increased injury and mortality rates for occupants of smaller vehicles in crashes with larger vehicles, as flagged in Section 3.1.3 and as also reported in Nuytens and Ben Messaoud (2023) for the case of Belgian roads.

A 2018 study by the Insurance Institute for Highway Safety, focused on the United States, found that hybrid vehicles were subject to a 10% higher likelihood to injure a pedestrian than ICE equivalents (Highway Loss Data Institute, 2018). Extrapolating this result on the basis of characteristics like faster acceleration and lower noise, Zipper (2023) claims that similar impacts could also end up being observable for EVs. Lower noise is effectively identified as a reasonable cause of higher frequency of crashes between EVs and pedestrians, in the case of Norway (Nuytens and Ben Messaoud, 2023).

While acknowledging that most countries are still in an early phase of EV deployment, analyses that have reviewed available evidence from road safety analyses regarding EVs in Europe (including Norway) do not point towards indicators of negative impacts from vehicle electrification on road crashes with other vehicles (Nuytens and Ben Messaoud, 2023). A possible reason for this is the possibility that EVs are more frequently equipped with effective driver assistance features, capable of protecting both occupants of the vehicle and other road users.

Overall, it is therefore important that a transition towards greater shares of EVs can effectively integrate strategies that limits their impact on weight increases (Shaffer et al, 2021), while still delivering the sizable energy security, energy diversification, and GHG emission mitigation benefits that EVs are capable of.

### 3.3.4 EQUITY

Available data on vehicle purchase prices – such as those outlined in IEA, 2019a and in following techno-economic analyses, including Slowik, 2022, for the United States<sup>28</sup> – point to a significant purchase price premium still characterizing sales of both PHEVs and BEVs. This premium is grounded in a combination of technical and economic factors, including:

- The cost of the batteries, for BEVs, which currently still exceeds the cost of ICE powertrains, and major efforts (including the possibility to develop new joint ventures between battery manufacturers and automotive OEMs) needed to develop new supply chains.
- In the case of PHEVs, the cost of complex powertrains, which combine ICEs with systems meant to pair engines with electric motors and batteries, anyway larger than on hybrids and ICEVs.
- Other cost components, related to research, development and – above all – investment in new industrial facilities, as these come with large capital outlays that need to be recovered over time.
- Especially for legacy OEMs, costs potentially associated (as this varies on a case-by-case basis) with the need for early dismissal of existing industrial facilities, or part of them (e.g., engine production lines), even if other capital costs are likely to be already amortized (contrary to the case of new market entrants focusing exclusively on electric vehicles).

These factors, combined with a near-term focus on higher profitability, also explain the greater reluctance of legacy OEMs to enter the EV market, especially in smaller segments. This is the case despite exposure to long-term losses of market shares to Chinese competitors (already selling EVs at affordable prices, and across several different segments) and prospects for shrinking relevance as automotive technology providers going forward.

The economic benefits of EVs – which consist of lower running costs and a decreased exposure to

oil product market price – are benefitting those consumers and small businesses that can afford the higher upfront cost. These tend to be in very high-income segments of the population, meaning that lower income segments of the population are not able to reap the economic benefits of electrification. Therefore, vehicle electrification is not exempt from equity challenges, at least until such a time when EVs no longer come with higher upfront costs.

EV sales are concentrated in China and high-income countries, as higher upfront costs (especially in countries other than China) and lack of charging infrastructure make EV deployment slow in low- and middle-income countries. The same equity issue that exists within individual economies – as low-income groups are not yet able to reap the savings that come with more efficient electric vehicles – also exists at the global level, across countries with different levels of income.

## 3.4 ARE SUVs AND EVs INCREASING THE RISK OF A GLOBAL DIVIDE?

Equity-related challenges and greater exposure of low-income households and businesses to the combined market transformation towards EVs and SUVs point towards the possibility of a growing global divide, not only within different population groups within countries, but also between major developed economies and other countries.

A number of global dynamics may exacerbate this potential trend:

- Increases in fossil energy prices, already accelerating the transition to EVs, as they tend to be paired with greater exposure to high energy prices on non-EV drivers.<sup>29</sup> resulting in greater challenges to access EVs for households and businesses exposed to higher costs of borrowing, and often reliant on second-hand vehicle purchases.
- Faster depreciation of ICEVs, including SUVs (which are still likely to remain more expensive than conventional cars), with respect to EVs,<sup>30</sup> resulting in greater challenges to access EVs for households and businesses exposed to higher costs of borrowing, and often reliant on second-hand vehicle purchases.

- Growing interest in batteries for stationary applications, as well as regulatory requirements related with materials circularity and a progressive transition towards net-zero emissions, insofar as these policies exert upward pressure on the value of EV batteries and the materials they contain, as these could also slow down EV depreciation, with net advantages for people and businesses having easier access to capital at lower costs.<sup>31</sup>

The impacts of dynamics affecting vehicle prices (via depreciation and/or structural determinants of battery costs) are not only limited to single countries or markets, but they also have transnational relevance, through international trade of new and second-hand vehicles. The latter is especially important for many low- and medium-income countries in Africa, Asia, the Middle East and Latin America, as they receive significant flows of used cars and vans (contributing to ensure a more affordable access to enhanced mobility options)<sup>32</sup> from high-income countries (UNEP, 2021).

In the absence of strong efforts to accelerate the shift to electric mobility in the Global South, at affordable costs, there is an increased risk of a growing divide between vehicle markets in the Global North – more focused on new EV purchases and having greater capital availability to retain second-hand EVs, and other markets – more exposed to EV deployment and increased flows of cheap and unsafe ICE vehicles, including through second-hand vehicle trade.

Rapid declines in new battery costs and/or energy prices (with greater environmental benefits if these declines are faster for renewable energies and/or other forms of low-carbon electricity, in comparison with fossil fuels) could mitigate these effects.

## 3.5 NEED FOR POLICY ACTION TO ADDRESS EXISTING CHALLENGES

Chapter 2 described key features of recent developments of the light duty vehicle market, providing a global overview that covers vehicle sales trends, powertrain technologies, market segments, specific energy consumption, CO<sub>2</sub> emissions, vehicle weight and footprint. Chapter 3 analysed further specific implications of two major trends identified in Chapter 2: a shift in market segments towards SUVs and a recent rapid development of vehicle electrification.



The analysis developed in Chapter 3 considered key elements that underpinned an increase in market shares of SUVs. It looked at the impact of this development on energy consumption, CO<sub>2</sub> emissions road safety and equity. It overlaid these considerations with transformations due to increased rates of electrification in the global LDV market, pointing out cases where EVs could mitigate or exacerbate challenges arising from the SUV shift.

Overall, this analysis flagged the following key issues, also summarized graphically in Table 4:

- While the shift towards SUVs in the LDV market could be important to support longer-term investments for stakeholders in the automotive sector, especially in cases where the need to invest in electrification has not been properly anticipated (or it has been deliberately delayed)<sup>33</sup>, it is effectively reducing the offer of affordable vehicles on the market.
- The shift towards SUVs has therefore detrimentally impacted equity, with stronger negative consequences on part of the society subject to greater barriers to access capital, both domestically and internationally. Due to its upward pressure in new vehicle prices, and despite increases in average income that took place over the years across different geographies, this shift may also have contributed to a stagnation of the global market for new vehicles.
- The SUV shift has clear negative implications for energy efficiency improvements and CO<sub>2</sub> emission mitigation, as it led to sizable reduction in energy efficiency improvement in comparison with a counterfactual without this shift.
- The SUV shift is also clearly paired with increased vehicle weight and demand for materials, beyond what can become available from end-of-life management of vehicles,<sup>34</sup> even in replacement markets.



- Increased market shares of SUVs are also paired with negative implications for road safety, including for the most vulnerable users, exacerbating equity impacts.
- The net benefits for energy efficiency improvements and CO<sub>2</sub> emission mitigation from EVs.
- The EV transition will continue to require increasing extraction and processing of materials for EV batteries. Over the coming decades, material demand will not only exceed supplies that may become available from vehicle and EV battery recycling, but growing sales of electric vehicles will require rapid expansion of material demand and processing (IEA, 2023c). Electric SUVs are paired with higher energy use per km and larger battery packs, exacerbating these challenges.
- Existing evidence suggests that EV impacts on road safety are not yet clear. At the same time, key characteristics like greater weight and less noise are likely to require risk mitigation strategies to avoid negative impacts, especially but not only for vulnerable road users.
- High upfront costs of EVs also expose the EV transition to equity-related challenges, similar to the case of the SUV shift, since low-income households are subject to greater capital availability constraints and higher costs of borrowing. This is relevant both domestically and internationally, with greater exposure for low-income countries.

Contrary to the SUV shift, though, the EV transition enables access to much lower operational costs, and lower total cost of ownership, especially for highly utilized vehicles. This has positive implications for equity, as long as hurdles in overcoming higher upfront costs are addressed by policy.

Effectively addressing these key issues, while pursuing improvements across all indicators considered, requires continued policy focus on the transition towards vehicle electrification, paired with targeted policies to mitigate, and if possible, reverse, the size shift towards SUVs.

This transition is achievable with the combination of forward-looking policy and alignment of industry strategy aligned with longer term viability. Challenges related to the demand of materials and minerals for battery supplies deserve specific attention, due to their wide-ranging implications for industrial development, trade, and geopolitics. These challenges are linked with stresses regarding the availability, pace of extraction and processing of battery materials (stronger with larger EV batteries) and the need for greater diversification of the battery value chain, also for reasons related with security of supply.<sup>35</sup>

Policy is crucial to de-risk transformative investment choices and direct them towards a product mix capable of mitigating the negative impacts on equity, environment and road safety highlighted in this chapter. A re-envisioning of industrial priorities is needed to steer capital toward investments that provide longer term prospects for market growth and value creation.

Policy is also crucial to handle challenges related with tensions regarding material demand and supply. In addition to scaling up supply and investing in alternative battery chemistries, demand-side measures can play an important role (Riofrancos et al., 2023). These are not limited to aspects related with the type of materials needed in EV batteries, but they also cover the effects associated with the evolution of vehicle and battery sizes. Importantly, policy measures aiming to manage the development of EV battery materials can also have positive implications for equity, especially if they are paired with other policies that enhance access to charging infrastructure.

If not paired with investments in the technology transition towards EVs by legacy OEMs, the EV transition also risks coming with a weakening of existing industrial clusters. Unless compensated by new market entrants, this can lead to overall deindustrialization. Due to impacts on jobs and their geographical location (ILO, 2021), this can also have destabilizing effects on social and economic resilience, especially for countries that currently have a strong stake in the automotive industry.<sup>36</sup> Policies and strategic choices for industrial development should address these deindustrialization risks (or, in countries that do not have strong automotive industry clusters, seize industrialization opportunities), while not losing focus on the need to maintain economic competitiveness.

Challenges of making affordable vehicles available on national markets could become opportunities for countries that have retained higher sales shares in the smaller market segments, as they have the possibility to leverage production already existing for the domestic market, turning it towards exports. China is particularly well positioned to gain market shares through exports for its EVs, thanks to its already strong EV production capacity – including smaller market segments – and the pervasive role that it has acquired across all stages of the battery supply chain.<sup>37</sup>

Due to their domestic market structure, other major global manufacturers with stronger presence in the small vehicle segments can also benefit from policy action capable of rebalancing opportunities for value creation away from SUVs and vehicles with comparatively high energy demand and emissions, as long as they continue to invest in domestic production capacities for EVs and batteries. On this basis, OEMs that are active in parts of Europe, India, Korea, Japan, and part of Latin America – all characterized by shares of smaller vehicles that remain significant – are well positioned to exploit opportunities.

Further opportunities can also arise for other emerging economies, as they could kickstart and/or strengthen nascent manufacturing industries, especially if they are supported in this effort by development or clean finance. These opportunities are not limited to LDVs, but include product diversification, e.g., with two-wheelers, and improved/strengthened informal and/or structured public transport services, due to their high rate of use and higher likelihood to lead to net savings, on a total cost of ownership basis.

Other arguments supporting the case for a reversal of the shift to SUVs come from the longer-term risk for OEMs to remain relevant with the new generation of vehicle owners. Continuing to pursue a strategy of focusing on SUVs could have important drawbacks, as young vehicle owners are often subject to capital availability constraints.<sup>38</sup> Maintaining a continued presence of OEMs in the smaller vehicle segments is also crucial, in high-income countries, to reduce social tensions, as it helps addressing equity-related pressures also involving dynamics that touch the second-hand vehicle market.

Industry and governments that already produce small vehicles can also seize opportunities from policy actions that redistribute value creation away from large vehicles with high energy use, emissions, and material demand profiles, to continue to compete for a role as a technology provider for the likely growing middle class in emerging markets. Competitors can leverage these same opportunities to enter in these market segments, with net overall savings for material and energy demand, emissions, and road safety. Such a strategy would leverage increases in market size for smaller cars.

Policy mechanisms specifically affecting finance – such as those started with the definition of taxonomies of activities mapping sustainability-aligned investments – are also important to contain risks related with the prioritization of near-term profits as the primary driver for investment choices. In the case of shifting to SUVs, such risks include the socialization of losses, especially relevant in the presence of climate policies that require rapid CO<sub>2</sub> emission reductions. These instruments are also important to support investment choices – including electrification – that are aligned with scientific evidence regarding climate- and environment-related imperatives and are therefore more likely to be aligned with sustained profitability over time and lower risk to socialize costs (with net benefits for social stability, especially in democratic political systems).

TABLE 4: Key issues arising from the analysis of the impacts of the SUV shift and the EV transition

|                               | CO <sub>2</sub> emissions | Road safety | Equity | Critical mineral demand |
|-------------------------------|---------------------------|-------------|--------|-------------------------|
| Electrification               |                           |             |        |                         |
| SUV shift                     |                           |             |        |                         |
| Electrification and SUV shift |                           |             |        |                         |

**Note:** green indicates that the impacts are minimal, or that the trend can promote better outcomes on a given metric. Yellow indicates that issues do exist, and policy makers should be aware of this, and there might be a case for regulation. Red indicates that issues should be addressed by policy, in the interest of society, the economy, and the environment.

Source: this assessment.

# 4 POLICY OPTIONS

Chapters 2 and 3 documented the relevance of the SUV shift for increases in energy use, CO<sub>2</sub> emissions, weight, road safety risks and vehicle prices, as well as opportunities from the EV transition to address many of these challenges, with the important exceptions of increases in weight (and demand for battery materials) and an upward pressure on vehicle prices (with equity implications, domestically and internationally).

This Chapter builds upon the trends (Chapter 2) and their implications (Chapter 3), to develop recommendations on policy actions that can support continued efforts to transition to EVs, while also managing material- and equity-related challenges. The recommendations developed draw from policy instruments already adopted or under consideration that attempt to steer the automotive market towards enhanced sustainability, while enabling economic development and preserving or enhancing equity.

This Chapter aims to offer suggestions on measures that can enable both consumers and OEMs to find added value in sustainability-aligned vehicle features, rather than in options that are detrimental to health and the environment. The focus is on instruments that orient consumer and industry choices towards technologies offering improvements in energy and resource efficiency, emission reductions, and road safety. Complementary recommendations also account for the need to ensure that this transition is inclusive and socially fair, both domestically and internationally.

These recommendations build on work developed in earlier assessments (in particular IEA, 2018, ITF, 2021b, GFEI, 2021, Khan et al., 2022, Cazzola and Santos Alfageme, 2023), integrating specific insights regarding the challenges associated with the SUV shift and the EV transition discussed in Chapters 2 and 3. Novel recommendations included here focus on policy instruments targeting vehicle weight, battery materials, and equity considerations. By addressing weight, they also aim to improve road safety.

Table 5 summarizes the policies outlined in this chapter, the actions recommended with respect to each of them, and the issues that they have the potential to address.

The importance of establishing a vision regarding the EV transition, of setting clear targets (also regarding access to charging infrastructure) and of broadening understanding of the benefits of EVs (including through pilot projects) are not discussed in detail here, as they

are pre-requisites for the discussion developed in this document. The same applies to:

- Safety-related technical standards, regulations, and test procedures, to enable the proper operation, safe repair, and end-of life handling of vehicle equipment and parts (including batteries and electric motors, and also covering durability aspects), as well as charging infrastructure (including sockets and connectors).
- Energy and environment-related technical standards, regulations, and test procedures, such as those regarding the measurements of energy consumption, CO<sub>2</sub> and air pollutants emissions, or the assessment of their lifecycle characteristics, underpinning possibilities to develop other policies.
- Communication protocols and payment instruments allowing to perform charging operation and related economic transactions, especially important for the vehicle to infrastructure interaction.
- Technical guidelines for first respondents, necessary for new technologies to ensure safety in case of crashes.
- Workforce support needed to ensure availability of skilled labour across all the steps of the automotive, energy/electricity and battery value chains.

Alternative decarbonization options to EVs using batteries (PHEVs and BEVs), such as hydrogen (fuel cell or ICE) vehicles, biofuels and e-fuels, or offsets, are not the focus of this analysis. The reasons for this are:

- limited availability of sustainably produced biofuels, limited market deployment and high investment risks associated with options using hydrogen as energy carrier (both for vehicles and refuelling infrastructure);
- far lower energy efficiency, for all hydrogen-based options (including e-fuels), with implications on costs, making them less competitive than EVs;<sup>39</sup> and
- the sheer size of fossil energy demand that needs to be replaced to decarbonize road transport, requiring extremely large deployment of carbon dioxide removals, in contrast with what is deemed feasible in IPCC scenarios (IPCC, 2022).<sup>40</sup>

**TABLE 5:** Policy options, recommended actions, and the potential to address key issues

| Policy                                                                                                                       | Recommendations                                                                                                                                                                                                              | Potential to address      |                     |                                |             |                       |
|------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|---------------------|--------------------------------|-------------|-----------------------|
|                                                                                                                              |                                                                                                                                                                                                                              | CO <sub>2</sub> abatement | Pollutant emissions | Battery materials, circularity | Road safety | Affordability, equity |
| Energy efficiency/CO <sub>2</sub> /GHG standards (with footprint as modulating parameter)                                    | Ramp up stringency; adopt footprint as modulating parameter. Implement new standards; tighten standards on higher footprint vehicles                                                                                         |                           |                     |                                |             |                       |
| Pollutant emissions standards                                                                                                | Ensure alignment with real-world, ramp-up stringency in countries/regions lagging behind, maintain or increase stringency in leading markets                                                                                 |                           |                     |                                |             |                       |
| Complementary policies on renewable fuels, vehicle manufacturing and end-of-life                                             | Adopt a comprehensive and coherent portfolio of policies, each targeting a clearly defined regulated entity, to ensure a life-cycle coverage                                                                                 |                           |                     |                                |             |                       |
| Specific safety-related regulations for EVs and batteries                                                                    | Adopt legal requirements that have been developed by the UNECE WP.29                                                                                                                                                         |                           |                     |                                |             |                       |
| Vehicle trade regulations based on environmental performance                                                                 | Differentiate import conditions based on vehicle powertrain/characteristics (e.g., for EVs, based on emissions, etc.)                                                                                                        |                           |                     |                                |             |                       |
| Urban access restrictions based on environmental performance                                                                 | Differentiate access based on vehicle environmental performance                                                                                                                                                              |                           |                     |                                |             |                       |
| Regulations specifically targeting highly utilised vehicles, based on environmental performance                              | More ambitious EV sales requirements, incentivising or mandating all-electric vkm                                                                                                                                            |                           |                     |                                |             |                       |
| Regulations on vehicle footprint                                                                                             | Apply a maximum LDV footprint, as well as a CAFE regulation at a smaller footprint to stimulate product diversification                                                                                                      |                           |                     |                                |             |                       |
| Regulations on EV battery capacity                                                                                           | Apply a CAFE regulation mandating a maximum battery capacity in kWh                                                                                                                                                          |                           |                     |                                |             |                       |
| Additional road safety requirements on heavy vehicles                                                                        | Require additional passive and active safety equipment on vehicles exceeding a given weight threshold                                                                                                                        |                           |                     |                                |             |                       |
| Differentiated purchase/registration taxes (including VAT) based on vehicle characteristics (including footprint and weight) | Modulate taxes factoring in weight differences (e.g., excluding larger and heavier vehicles from rebates)                                                                                                                    |                           |                     |                                |             |                       |
| Differentiated annual taxation on vehicle ownership                                                                          | Increase stringency (and taxation levels) for older vehicles, with poorer environmental performance. Differentiate local taxes/charges based on vehicle powertrain/characteristics (e.g., for EVs, based on emissions, etc.) |                           |                     |                                |             |                       |
| Differentiated import duties                                                                                                 | Differentiate local taxes/charges based on vehicle powertrain/characteristics (e.g., for EVs, based on emissions, etc.)                                                                                                      |                           |                     |                                |             |                       |
| Differentiate local vehicle taxes and charges                                                                                | Differentiate local taxes/charges based on vehicle powertrain/characteristics (e.g., for EVs, based on emissions, etc.)                                                                                                      |                           |                     |                                |             |                       |
| Fuel taxation and carbon prices                                                                                              | Increase fuel taxes to levels commensurate with the externalities of fuel consumption, the same applies more broadly to economy-wide emissions                                                                               |                           |                     |                                |             |                       |
| Road user charges                                                                                                            | Gradually adopt road user charges to complement fuel taxes to fund transport infrastructure and cover externalities                                                                                                          |                           |                     |                                |             |                       |
| Redistributive measures enabled by revenue generation from carbon pricing and road user charges                              | Use of revenues from taxation reforms to promote public transport and target incentives and support to low-income households and businesses                                                                                  |                           |                     |                                |             |                       |
| EV charger deployment and other regulations to scale up charging availability                                                | Mandate or incentivise the provision of a charging network sufficient to ensure autonomy on all trips without excessive battery capacity                                                                                     |                           |                     |                                |             |                       |
| Sustainable finance framework for sustainable activities (including EVs and related infrastructure)                          | Adopt a taxonomy similar to the one put in place in the European Union to orient investments towards sustainable activities, including EVs                                                                                   |                           |                     |                                |             |                       |
| Scale up development aid for sustainable activities (including EVs and related infrastructure)                               | Scale up multilateral funding to support an inclusive EV transition globally                                                                                                                                                 |                           |                     |                                |             |                       |

**Notes:** dark green indicates that the policy can be designed to directly impact or target a given issue. Light green demotes positive indirect impacts. Yellow indicates neutral effects, or that effects depend on specific circumstances. Orange stands for adverse indirect impacts. Red indicates adverse impacts.

**Source:** dark green indicates that the policy can be designed to directly impact, or target a given issue. Light green demotes positive indirect impacts. Yellow indicates neutral effects, or dependent on specific circumstances. Orange stands for adverse indirect impacts. Red indicates adverse impacts.



# 4.I REGULATORY POLICY FRAMEWORKS ON ENERGY, ENVIRONMENT AND SAFETY

## 4.1.I ENVIRONMENTAL REGULATIONS

Stabilising global temperatures and mitigating the impacts of climate change requires swift action on the reduction of greenhouse gas emissions. Addressing the health impacts of poor air quality in urban areas, across the globe, also requires swift action to reduce local pollutant emissions.

Regulations limiting emissions of greenhouse gases and local pollutants are key policy instruments aiming to achieve these goals. Regulations requiring reductions of direct emissions of CO<sub>2</sub> and local pollutants, with a specific focus on LDVs, have already been deployed in several countries. This is not only the case in high-income countries or groups of countries, like the European Union or the United States, but also, in low- and medium-income countries, including major economies like China and India (as summarized in Table 6).

Regulations generally tend to be technology-neutral, to enable and spur innovations available at the lowest possible cost — an exception is tailpipe air pollutant emissions standards, which are developed based on techno-economic assessments of powertrain — and fuel-specific emissions control technologies. Over the past decade, based on the very dynamic technology and market developments of EVs, many of these regulatory instruments already integrate provisions — such as incentives or targeted sales share requirements — that address the specific case of EVs. Key reasons for this lie in the effectiveness of EVs in mitigating emissions, improving energy efficiency, and enabling cost-effective access to a more diversified energy mix (including scalable forms of renewable energy) in road transport, as well as in the significant implications for industrial transformations and development.<sup>41</sup>

Stabilising global temperatures would require ratcheting up the ambition of regulatory requirements, and not only reaching zero direct emissions from vehicle use, but also effectively abating GHG emissions associated with the production of fuels, as well as the manufacture

and maintenance of vehicles and of their support infrastructure. Given the higher weight of EVs, with repercussions on tyre wear, it is also important to ensure that pollutant emission regulations effectively account for non-exhaust emissions. However, it is important to acknowledge the possibility of net benefits on non-exhaust emissions for EVs, due to reduced particle emissions from regenerative braking. Work recently finalized by the United Nations World Forum for Harmonization of Vehicle Regulations, focused on the development of related measurement methodologies, provides a solid foundation for further policy developments in this area (UNECE, 2023a).

Adopting a holistic approach is important not only to trigger an economy-wide response to the challenge of climate change (rather than a sectorial one, which would anyway be insufficient to bring GHG emissions to net zero), but also to reduce the likelihood for regulations to lead to unintended consequences.<sup>42</sup> The European regulatory policy portfolio — summarized in Table 7 — provides a clear example of regulatory approaches that target discrete parts of the vehicle lifecycle, each with a clearly defined set of regulated entities, in order to ensure that the overall approach is effectively holistic.

Internationally, the UNECE World Forum for Harmonization of Vehicle Regulations established, in 2022, an informal working group on Automotive Life Cycle Assessment (UNECE, 2023b), with the aim to develop a harmonized methodology to measure GHG emissions incurred by vehicles across their lifecycles.<sup>43</sup> This can offer an objective, scientific and multilaterally developed basis to OEMs and parts suppliers to document performance related with GHG emissions embodied in materials and components. The harmonized approach would also ensure that consumers can take decisions accounting for the use of low-carbon options and could thereby offer a complementary set of incentives beyond national or regional policy approaches.



TABLE 6: Regulations requiring reductions in energy intensity, direct CO<sub>2</sub> and local pollutant emissions for new vehicles in selected markets

| Country or region | Fuel economy / CO <sub>2</sub> / GHG and pollutant emissions standards                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Argentina         | Current pollutant standards are Euro 5a.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Australia         | Australia's pollutant emissions standards are currently at Euro 5 equivalence, are harmonised with the European standards, and differ based on gross vehicle mass.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Brazil            | Pollutant standards are PROCONVE L8 (passenger cars), and PROCONVE L7 (LCVs).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Canada            | Fleet average GHG limits for passenger cars and light trucks currently mandate a 5% improvement per year through 2025 and are closely aligned with US standards.<br><br>Since 2015, Canada's pollutant emissions standards have been aligned with the US Federal standards.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Chile             | A new CAFE fuel economy standard will come into effect in 2024, mandating limits of 18.8 km/Lge (for PLDVs) and 18.3 km/Lge (for LCVs).<br><br>Newly registered new LDV models must meet either Euro 6b or U.S. EPA Tier 3 Bin 125 standards from September 2022, while newly registered used LDVs must comply by February 2023. By September 2024, new registrations of both new and used vehicles must comply with either Euro 6c or U.S. EPA Tier 3 Bin 70.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| China             | Phase V standards set a fleet average target of 4.0 L/100 km (NEDC) by 2025, and include both a per-model standard and a CAFC standard.<br><br>China 6 (similar to Euro 6) across 16 regions; China 5 (similar to Euro 5) nationwide.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| European Union    | The 2023 CO <sub>2</sub> emission performance standards for cars and vans require achieving CO <sub>2</sub> emissions reductions relative to 2021 of: 15% by 2025; 55% (cars) / 50% vans by 2030; and 100% by 2035.<br><br>The EU's current pollutant emissions standards are at Euro 6d (from January 2021). A proposal for Euro 7 emissions standards is currently under negotiation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| India             | India's current CAFE target is 113 g CO <sub>2</sub> /km in April 2022 for new cars.<br><br>BS VI standards (based on Euro 6) apply to all LDVs from April 2020.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Indonesia         | Current pollutant emissions standards for gasoline and diesel light-duty vehicles are Euro 4 equivalent.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Japan             | The current Top Runner program began in 2022 and runs through 2030 – targeting a 32.4% improvement in fuel consumption by 2030 compared with the 2016 fleet average.<br><br>Japan's pollutant emissions standards are equivalent in stringency to Euro 6, with testing since 2018 conducted on the Worldwide Harmonized Light Vehicles Test Procedure (WLTP).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Korea             | Adopted 2030 GHG targets require reductions of 27.8% for cars and 12% for light trucks when compared to a 2020 baseline, while 2030 fuel economy standards are 37.3% more stringent for cars and 22.7% for light trucks. Manufacturers may choose to comply with either greenhouse gas or fuel economy standards.<br><br>For pollutant emissions standards, for gasoline-fuelled vehicles, Korea adopts California's Non-Methane Organic Gases fleet average system, while diesel vehicles are subject to Euro 6 regulations.                                                                                                                                                                                                                                                                                                                                                                          |
| Mexico            | Current CO <sub>2</sub> and fuel economy standards are based on footprint-based US standards from 2012-2016 but have not increased in stringency since that time.<br><br>A mix of U.S. Tier 1 to 2 emissions limits and Euro 3 and 4 standards has been in effect since 2004.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| New Zealand       | From 2022, the Clean Vehicle Standard applies GHG emissions standards. In 2023, the standard is 145g CO <sub>2</sub> /km for PLDVs, and 218 g CO <sub>2</sub> /km for LCVs. These increase in stringency to 63.3 g CO <sub>2</sub> /km and 87.2 g CO <sub>2</sub> /km in 2027 for passenger light duty vehicles and LCVs, respectively.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Russia            | From 2016, Euro 5 standards apply to all LDVs (imports and domestic alike).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Peru              | For pollutant emissions, from 2016, light-duty vehicles must meet either the Euro 4 or the US Tier 2 standards. In 2021, Peru established standards that require light-duty vehicles to comply with Euro 6b or U.S. Tier 3/EPA 2010 emissions limits by October 2024.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Thailand          | LDV pollutant emissions standards since 2012 have been at Euro 4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| United States     | The December 2021 greenhouse gas (GHG) standards for light-duty vehicles revises CAFE standards to be more stringent in model years 2023-2026, with targeted temporary flexibilities to address production lead times and incentivize production of near-zero and zero-emission vehicles. These are aligned with the CAFE standards for model years 2024-2026 for cars and light trucks. Proposed multipollutant standards for light- and medium-duty vehicles for 2027-2030 are under discussion. These would regulate GHGs as well as criteria air pollutants (PM, ozone, nitrogen oxides, and carbon monoxide).<br><br>In California, Low Emission Vehicle (LEV III) standards, which apply both GHG and particulate standards become gradually stricter from 2015-2025.<br><br>Air pollutant (criteria pollutants) are currently regulated under U.S. Tier 3 standards (which apply through 2025). |
| Vietnam           | As of 2022, light-duty vehicles are regulated under the Euro 5 standard.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

Notes: Text in italics refers to emissions of local pollutants. Other text refers to energy efficiency or direct emissions of CO<sub>2</sub>.

Sources: TransportPolicy.net (n.d.), Australian Government, n.d., SAC, 2021, European Commission, n.d., True, 2021, ICCT, 2019, ICCT, 2013, NHTSA, 2022, ARB, n.d., EPA, 2023.

TABLE 7: Complementary EU regulations aiming for a holistic approach on GHG emission reductions

| Life-cycle emission phases                                                                            | Processes                                                                                                          | Regulatory requirements                                                                                        | Other policy tools                                                                                                                                     |
|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Vehicle design, manufacture, including material extraction and processing, and end-of-life management | Vehicle design, manufacture, including material extraction and processing, and end-of-life management              | Regulation on circularity requirements for vehicle design and on management of end-of-life vehicles (proposed) | Carbon pricing (Emission Trading Scheme)<br><br>Carbon Border Adjustment Mechanism<br><br>Energy Efficiency Directive<br><br>Effort Sharing Regulation |
|                                                                                                       |                                                                                                                    | Battery durability requirements (UN Global Technical Regulation 22, recently introduced)                       |                                                                                                                                                        |
|                                                                                                       | Vehicle component design and manufacture, including material extraction and processing, and end-of-life management | EU battery regulation (recently updated)                                                                       |                                                                                                                                                        |
| Energy production                                                                                     | Primary energy extraction                                                                                          | Regulation on methane emissions in the energy sector (proposed, being negotiated)                              | Policies targeting economy-wide decarbonisation, including from the industry sector (e.g., steel, aluminium manufacture and recycling)                 |
|                                                                                                       | Energy conversion                                                                                                  | Renewable energy directive (proposed update, close to be finalized)                                            |                                                                                                                                                        |
|                                                                                                       |                                                                                                                    | Electricity market design (proposed update, being negotiated)                                                  |                                                                                                                                                        |
| Vehicle and fuel use                                                                                  | Energy use during operations                                                                                       | Regulation on tailpipe CO <sub>2</sub> emissions                                                               | Vehicle taxation<br>Fuel taxation<br><br>Targeted carbon pricing for road transport                                                                    |

Sources: this analysis based on legal and negotiating texts in UN, 2022; European Union, 2023a; European Union, 2023b; European Commission, n.d.; European Commission, 2021, European Parliament, 2023a; European Commission, 2019, European Council, 2022, European Parliament, 2023b; and European Union, 2023c.

4.1.2 ROAD SAFETY REGULATIONS

Regulations are also applied to road vehicles to improve road safety. These span a variety of topics, including active safety (brakes, steering, tyres, electronic stability controls), passive safety (to minimize the risk and severity of injury to vehicle occupants or to other road users in case of collisions, safety belts) and other general safety-related aspects (e.g., glazing, lighting). New technical provisions and are also being developed to address the specificities of vehicle connectivity and automation (UN, 2021).

The adoption of these requirements is rooted in the need to improve the behaviour, handling, and

equipment of vehicles to reduce the chance and severity of crashes. The requirements also facilitate trade by reducing divergence across markets and providing a clear regime governing liability (Pernice and Debyser, 2023).

Specific safety-related regulations address the case of EVs and battery technologies. These require continuous monitoring and updates. Key examples include the case of requirements related to thermal runaway, thermal propagation, electrolyte leakage, and safety requirements in the event of a crash. These issues are being addressed by the UN World Forum for the Harmonization of vehicle regulations (UNECE, 2023c; UNECE, 2023d; ITF, 2020b).<sup>44</sup>

4.1.3 USE OF REGULATIONS IN VEHICLE TRADE

A number of regulatory instruments are already used to regulate vehicle trade flows. Current practices range from full trade restrictions (e.g., for used vehicles in major manufacturing countries or markets like Brazil and India) to the absence of any restrictions whatsoever (e.g., within free-trade areas like the European Union and the North American Free Trade Agreement). The diversity of regulations was one of the key reasons behind international efforts aiming to harmonize regulatory texts (UN, 2021).

Parameters used to regulate international used vehicle trade flows typically include age and pollutant emission limits and necessitate compliance with key roadworthiness requirements, leveraging UN regulations for technical considerations.

Very few trade-related regulations integrate aspects directly linked with energy efficiency and CO<sub>2</sub> emissions, and particular powertrain types (including EVs). New Zealand’s Clean Car Standard, which came into effect in 2023, is the first regulatory instrument that requires importers to reduce the CO<sub>2</sub> emissions of the vehicles entering the country (Waka Kotahi, n.d.) and it represents a best practice case globally. Vehicles are collectively required to meet a set of targets, currently set until 2027, with a growing level of stringency over time (Te Manatū Waka, n.d.). Non-compliance is subject to the payment of penalties, per vehicle and g CO<sub>2</sub>/km, similar to regulatory requirements in place in the European Union (only applicable to new vehicles). The standard is also paired with differentiated vehicle taxation (the Clean Car Discount), as discussed in section 4.3.

4.1.4 URBAN ACCESS RESTRICTIONS

Regulatory measures exist not only at the national or supra-national level, but also at regional and municipal levels, especially in Europe (Urban Access Regulations, n.d.). Low Emission Zones (LEZs) and Zero Emission Zones (ZEZ) are the most common type of local environmental regulation applied to road vehicles. They generally restrict access to sub-categories of vehicles based on environmental performance (in some jurisdictions limiting access to EVs and other technologies with zero tailpipe CO<sub>2</sub> and local pollutant emissions). In some cases, they complement urban access fees, discussed in Section 4.3.4, on vehicle taxation.

4.1.5 TARGETED REGULATORY REQUIREMENTS FOR SPECIFIC USAGE PROFILES

Environmental regulations promoting energy efficiency improvements, CO<sub>2</sub> and local pollutant emission savings (including via the EV transition) have the strongest merit for highly utilized vehicles, given that these are the ones where upfront costs (and also emissions resulting from battery manufacturing, for EVs) can be most rapidly offset, thanks to lower operational costs, lower energy requirements per km, and (in terms of societal and environmental costs) lower GHG and pollutant emissions.<sup>45</sup>

Like environmental regulations, there is also a case for higher stringency on safety requirements for highly utilized vehicles, due to their more frequent presence in active traffic — which increases the likelihood of crashes.

Public procurement policies are well suited to require greater regulatory stringency by incentivizing or requiring disproportionate procurement of EVs and adoption of enhanced road safety features. This applies both in cases where public authorities subsidize the acquisition of vehicles used for shared transport services and where vehicles are directly owned by the public administration.<sup>46</sup>

4.2 REGULATORY CHANGES TO ADDRESS VEHICLE WEIGHT INCREASES AND EQUITY-RELATED CHALLENGES

Evidence available from Chapters 2 and 3 shows the importance of introducing or adding elements accounting for weight- and equity-related issues to existing regulatory frameworks. Doing so can effectively mitigate the negative effects of the SUV shift on energy efficiency, GHG emissions (especially for ICEVs) and material demand (especially for EVs).



## 4.2.1 REGULATIONS ON VEHICLE FOOTPRINT

The introduction of a cap on vehicle footprint, in absolute terms, could effectively limit vehicle size increases. A corporate-average regulatory requirement, similar to those in place for fuel economy or CO<sub>2</sub> emissions but having footprint as the regulated parameter, would also help reverse the SUV shift observed since 2010 and could complement a cap.

Footprint-based regulations could be better than weight-based ones, as the latter would need differentiated treatment for different powertrains (namely for EVs, due to battery weight), subject to uncertainties due to varying energy density across different battery technologies.

The cap would come with strict limitations, without flexibility mechanisms, but it would only be applicable to the largest vehicles. Sales-weighted regulatory approaches are better suited to induce fleet-wide changes, integrating flexibilities to enable compliance and leave room for product diversification.

Regulations on footprint could have positive implications for equity, as they would reduce the scope for continued size increases, thereby addressing challenges arising from the transformations occurring in automotive markets.

## 4.2.2 REGULATIONS ON BATTERY CAPACITY

A second new regulatory instrument, cutting across environmental and safety aspects, could be particularly well suited to ensure effective and efficient utilization of battery materials. This could also be based on a corporate-average regulatory approach, solely applied to EVs and having battery capacity as the regulated parameter. The requirement can be set to prevent or even reverse the continued tendency towards an increase in battery sizes shown in Figure 20.

Using weight as the regulated parameter could also be possible but it risks leading to limitations in the way innovation can help address material availability criticalities. This is due to the fact that some of the technologies already used to handle material availability constraints rely on battery chemistries that have lower energy densities (such as LFP or sodium-ion, rather than NMC or NCA), which is partly compensated by improved cell-to-pack architectures (as discussed in Section 3.3.2).

Importantly, this approach can also effectively integrate flexibility mechanisms (including OEM pooling), enabling continued diversification of products and strategies for different OEMs (including the possibility to meet the needs of highly utilized vehicles, such as taxis and shared cars, for which larger battery packs are justifiably required).

Equity aspects could also be indirectly targeted by this approach, as growth in battery capacities tends to be paired with greater deployment of EVs in larger vehicle segments and a cap on the fleet-average capacity can effectively promote a differentiation of the offer as well as greater diversity of different battery sizes available for any given model.

This novel regulatory approach can further offer important opportunities to introduce demand-based policies to address challenges specifically related with the surge in demand for EV battery materials accompanying the EV transition, also helping to moderate eventual supply constraints. If based on battery capacity, rather than weight, it could leave greater room for changes in chemistries to help in achieving this goal. If based on weight, it could limit the relevance of technologies that have lower gravimetric energy densities than those already in use.

Due to competition among major economies for the acquisition of battery materials,<sup>42</sup> this policy is likely to require international coordination to be maximally effective and viable. For this reason, international fora with specific mandates to monitor the availability and price of critical materials and to ensure continued availability at the global level, as in the case of the IEA, can play a crucial enabling role in this context.

## 4.2.3 OTHER REGULATORY REQUIREMENTS APPLYING SPECIFICALLY TO BATTERIES

Specific regulatory tools can also be applied to batteries, as they are key components of EVs, with major relevance for vehicle weight and evolutions in material demand. Regulatory requirements regarding extended producer responsibility can be integrated into existing legislation. These can address:

- Material traceability, solutions facilitating re-use, repurposing and recycling (including an electronic “battery passport” — a digital record on battery packs that provides data on battery characteristics, such carbon footprint, state of health, procedures for dismantling, and composition of the battery).

- End-of-life requirements (including collection targets and obligations targets for the recovery of materials) — such as those already integrated in the EU Battery Regulation (European Union, 2023b). These are particularly relevant in addressing challenges related with EV battery material demand. This is especially important for the next generation of EV batteries, as these regulatory obligations can ensure that the necessary investments to enable the recycling of battery materials can be made on time, facilitating greater reliance on recycled materials as EVs introduced now and in the near future approach the end of their useful life.

Due diligence reporting requirements — also integrated in the EU Battery Regulation — aim to address social (including protection of human rights, human health, community life, including that of indigenous peoples, the protection of children, and gender equality) and environmental (protection of the natural environment and biological diversity) consequences of industries involved in the extraction, processing, and trade of certain raw materials and secondary raw materials used for battery manufacturing. These are important for managing risks associated with EV battery supply chains, and are also being used to avoid de-industrialization (a choice that needs to be accompanied by a strong focus on the need to ensure effective industrial competitiveness and the avoidance of protectionism, for reasons of economic sustainability).

These provisions are additional to other requirements on battery durability (important for the optimal use of minerals, in addition to consumer protection), which saw a major milestone being finalized in 2022, in the context of the World Forum for the Harmonization of Vehicle Regulations (UNECE, 2022). Battery durability requirements for LDVs require that EVs retain at least 80% (and 70%) of their charge for at least 5 (and 8) years or 100,000 km (160,000 km), whichever comes first, and outline how to account for “virtual range” in cases where EVs are used to provide power to electricity grids. Similar requirements are now being developed also for heavy-duty vehicles (UNECE, 2023e) and – like other UN Global Technical Regulations – offer an opportunity for a common basis for country-specific transposition.

## 4.2.4 CHANGES IN EXISTING ENVIRONMENTAL REGULATIONS

The use of vehicle footprint as a modulating parameter of existing regulations on specific energy consumption or direct CO<sub>2</sub> emissions, in combination

with increasing stringency of the standards as vehicle footprint increases, offers the opportunity to effectively tighten the requirements applicable to larger vehicles (including both ICEVs and EVs).

Most regions have adopted regulations using weight (and not footprint) as a modulating parameter. Under such a framework, CO<sub>2</sub> emissions standards are more stringent for lighter vehicles. Vehicle light-weighting is an effective means to reduce fuel consumption, but weight-based standards fail to incentivize energy saving technologies based on weight reduction, as lower weight vehicles are subject to more stringent CO<sub>2</sub> emissions limits. Hence, whenever possible, switching from weight-based to footprint-based standards can help to effectively incentivize light-weighting.

Alternative approaches based on weight as the modulating parameter are possible, but they have the risk losing effectiveness in promoting the use of material substitution and light-weighting solutions as energy-saving technologies for ICEVs.

Regardless of which modulating parameter is applied, tightening requirements for larger (in the case of footprint) or heavier (weight) light-duty vehicles would have positive implications for energy and CO<sub>2</sub> savings, without negative equity implications (as larger vehicles tend to be sold at higher prices purchased by wealthier customers, and are therefore those with greater margins available for EV deployment, resulting in a higher share of the EV deployment cost falling on premium vehicle models).

Regulatory requirements that are focused on CO<sub>2</sub> emissions rather than being specifically designed for EVs can also benefit significantly from legal frameworks enabling the development of strategies based on lifecycle accounting. In Europe, a recent proposal develops harmonized rules for accounting GHG emissions of transport services (European Commission, 2023a). This can help establishing a level playing field between transport modes, which can help to more effectively allocate material demand occurring from systemic responses, not limited to shifts across light-duty vehicle segments and powertrains. Equity implications depend on the nature of the systemic response. A systemic response to emission reduction for transport services can consist of an increased reliance on smaller EVs, providing opportunities to lower electricity demand, charging infrastructure needs and battery materials requirements (ITF, 2023). Such a shift could also help address equity challenges, since smaller electric vehicles (including quadricycles, discussed in Box 3, and two- or three-wheelers) are more likely to be available at lower prices.



## THE CASE OF QUADRICYCLES

Electrification has been accompanied, especially in Asia and also to some degree in Europe, by increasing interest in quadricycles, four-wheeled vehicles subject to limitations on maximum weight and speed. Reasons for this interest include affordability challenges for conventional LDVs, stemming in part from the SUV shift and EV transition, recent increases in fuel prices, and opportunities for OEMs to deploy these models at lower price points compared to conventional cars. Increased reliance on quadricycles can also be part of a systemic response to the decarbonization and electrification of transport services (ITF, 2023).

The specific regulatory developments in place for lighter EVs (including quadricycles) could be an enabler of market growth: the separate (and less strict<sup>71</sup>) regulatory framework to which quadricycles are subject<sup>72</sup> has been an important feature making quadricycles attractive to OEMs, as this allowed for faster design processes, minimization of components and – for successful models – has also been paired

with manufacturing cost savings, enabling quicker market deployment and shortened time to market (Robert, 2020).

Other reasons that spurred OEM interest also include opportunities to attract younger customers,<sup>73</sup> paired with positive repercussions related with brand loyalty (Adolf, 2022), and limited risks for these vehicles to jeopardize their main markets (as they also compete as possible alternatives to two-wheelers), also linked with restrictions in terms of segment substitution potential.<sup>74</sup>

To ensure that it can effectively lead to net benefits, including in terms of safety, a shift in focus from cars towards quadricycles – including electric ones – in urban areas, needs to be accompanied by adequate safety provisions (ITF, 2023). Key examples include changes in current provisions regarding the use of airbags, crash tests and other safety features (NCAP, 2016).



### 4.2.5 CHANGES IN EXISTING ROAD SAFETY REGULATIONS

Given their impact on weight, documented in Chapters 2 and 3, and their growing market shares, EVs — like SUVs (which also have additional changes in ground clearance) — also need stringent road safety requirements.

New Car Assessment Programmes (NCAPs) have been promoted by consumer protection organisations to enhance vehicle safety features, to integrate best practices in existing regulatory texts related with active and passive safety (Euro NCAP, 2022). They also have a track record of being an important driver of enhancements of international test procedures underpinning technical regulations on road safety (Global NCAP, 2018; Perl, 2020). The work already developed in these frameworks is particularly relevant to offering solutions to improve and expand the scope of safety regulations.

Due to its specific relevance for road safety, weight can also be considered as a criterion for the introduction of additional safety regulations and/or requirements to integrate active safety features. Considering the correlation between vehicle size, weight and price, documented in Chapter 3 and in IEA (2019a), differentiated safety requirements based on weight could also bring affordability benefits, as they could increase affordability and consumer demand for lighter vehicles", while focusing prices increases on heavy (and anyway less affordable) market segments.

### 4.2.6 CHANGES IN TARGETED REGULATORY REQUIREMENTS FOR SPECIFIC USAGE PROFILES

More stringent environmental regulations (i.e., vehicle efficiency or CO<sub>2</sub> standards, and local pollutant emissions standards, as well as specific requirements to transition vehicles towards EVs) for highly utilized vehicles can promote efficient use of minerals for EV batteries and may also generate positive spillovers in terms of equity.

In the case of minerals, the advantage comes from the fact that EVs that are more intensively used displace more GHG emissions and oil demand each year per unit battery capacity. Examples include taxis and shared mobility services as well as municipal service and postal fleets, which are driven higher cumulative lifetime distances than private cars (Morfeldt and Johansson, 2022).<sup>48</sup> In

the case of equity, positive spillovers are especially important in emerging economies (due to greater difficulties to overcome higher upfront costs). The reason is that a targeted policy approach, e.g., mandating accelerated EV adoption for ridesharing and taxi services or government fleets (all of which face lower cost of access to capital than low-income households and businesses) can bring more EVs to emerging economies, also making EVs more broadly available locally in the second-hand vehicle market.

Good practice examples exist in developed and emerging economies. In California, the Clean Miles Standard (Government of California, 2018) requires a progressive reduction of GHG emissions per passenger km by ridesourcing services, encouraging a faster EV transition for the highly utilized vehicles providing them.<sup>49</sup> In London, a mandate requiring all newly registered taxis to be zero-emission capable as of 2018 was followed shortly afterwards by a voluntary commitment from Uber to transition every car on the app in the British capital to be fully electric by 2025 (ITF, 2020a; TfL, 2016; Mayor of London, 2019; Uber, 2018).<sup>50</sup> In the Balkans, Tirana (Albania) gave priority to EVs, HEVs and Euro 6 vehicles to enable access to additional taxi licenses. This has led to investments by several operators to deploy EVs and to invest in charging infrastructure, starting as early as 2016, with continuously increasing EV and charging station deployment over time (EnerGNETMob, 2021).

Specific regulatory requirements, raising the level of ambition for fleet electrification – including leasing companies and other fleet managers, also align well with better capacity for organizational fleet planning decisions and greater relevance of total cost of ownership and lifecycle emissions, as well as growing consideration placed on environmental, social and governance (ESG) goals, as the basis for investment decisions by fleet operators (Daina, 2023).

The differentiation of environmental regulatory requirements based on footprint as a modulating parameter (as discussed in Section 4.2.3) or safety regulations based on weight (as discussed in section 4.2.4) is also applicable, in principle, to the case of highly utilized vehicles. The rational basis for this choice lies in the faster return on the capital investment (price premium) for electric or otherwise more fuel-efficient vehicles that require greater amounts of energy for their operations and that are more frequently in traffic. More stringent regulatory requirements for larger and heavier vehicles could also make smaller and lighter vehicles comparatively more affordable, thereby reorienting consumer choices towards them.

Differentiated regulations based on weight and footprint are likely easier to implement at the local level. One example is given by footprint-specific access or parking restrictions in selected urban areas, such as central districts (ITF, 2023). This is also justified by constraints related with the limited availability of street space.<sup>51</sup>

## 4.3 VEHICLE TAXATION

### 4.3.1 COUNTRY-LEVEL TAXATION FRAMEWORKS

Vehicles are subject to different types of taxes and fees (or a combination of fees and subsidies, in feebates or bonus/malus schemes) applicable at the country level, generally applied at the time of purchase of vehicles (e.g., as registration or value added taxes) and/or during vehicle life (in the form of annual circulation/ownership charges or recurrent fees, possibly including parking and emissions certifications).

Vehicle taxation can be differentiated based on different possible criteria. The parameters currently used by governments as discriminants for differentiated taxation include energy efficiency, diversification, security, GHG and pollutant emissions.<sup>52</sup> Other discriminating parameters include engine capacity (most commonly for frameworks set up before the EV transition and the adoption of downsizing as an energy efficiency measure), power, and price<sup>53</sup> (Carpenter and Antich, 2022).

For ICEVs, all these discriminating criteria can have impacts on both weight and equity, as energy use, CO<sub>2</sub> emissions and power all tend to be correlated with weight and prices (IEA, 2019a). For EVs, the decoupling between GHG emissions and prices can lead to equity-related challenges,<sup>54</sup> requiring corrective redistributive measures.

Ensuring that differentiated taxation is effective in fostering progress on energy efficiency and CO<sub>2</sub> emissions requires that these parameters become key determinants of what defines the differentiated taxation.<sup>55</sup> As in the case of regulations, it is also critical that differentiated taxation takes into consideration lifecycle performance.<sup>56</sup>

As a general rule, registration taxes are substantially higher than circulation/ownership taxes, also because the latter have a recurrent nature. Company cars also tend to be subject to lower taxation rates than private vehicles (Harding, 2014;

Carpenter and Antich, 2022).<sup>57</sup> This has adverse equity implications, as corporations are more able to withstand a higher tax burden on their balance sheet compared to many private households, especially in lower-income countries (Carpenter and Antich, 2022).

Vehicle registration taxes also tend to be higher in countries that do not have a vehicle manufacturing industry, generating larger revenue streams for governments than in cases of countries that are major vehicle producers (Carpenter and Antich, 2022).

The design of vehicle taxation schemes also has implications for government revenues. Revenue-neutral feebates or bonus/malus schemes are better suited, from an equity perspective, for countries with higher incomes and strong car dependency (since lower income households have fewer alternatives to car ownership to access mobility). Revenue-generating frameworks are more likely to have lower equity challenges in emerging economies,<sup>58</sup> especially if universal access to mobility is ensured with greater investments in public transport.

Vehicle circulation/ownership taxes are used in some countries to encourage more frequent vehicle renewal, especially when they are designed such that charges increase over time. This can be beneficial from an environmental and safety perspective, as long as vehicle performance on these metrics is improving. An important limitation of this approach, particularly in car-centric high-income countries, is that circulation taxes come with equity challenges for capital-constrained households and businesses, who often rely on second-hand cars. Similar considerations also apply for low- and medium-income countries, where car buyers also rely, to a large degree, on second-hand vehicle imports.

### 4.3.2 KEY EXAMPLES OF COUNTRY-WIDE DIFFERENTIATED VEHICLE REGISTRATION TAXES

The use of differentiated taxes on vehicle acquisition is currently common in most countries. This is the case for taxes applied to households (summarized for selected countries and regions in Table 8) and, increasingly, also for taxation frameworks applied to businesses (Harding, 2014; Carpenter and Antich, 2022 and European Environment Agency, 2022).

Registration taxes are most frequently applied to new vehicles or used vehicle imports. In specific cases, including France and New Zealand, they also apply to

TABLE 8: Vehicle taxation frameworks in selected countries and regions

| Country or region | Fuel economy / CO <sub>2</sub> / GHG and pollutant emissions standards                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ASEAN             | In the Association of Southeast Asian Nations (ASEAN), Singapore adopted differentiated taxation, based on the environmental performance of vehicles, starting 2012. Differentiated vehicle taxes based on CO <sub>2</sub> emissions/km are also in place in Indonesia (in the form of a luxury tax that uses engine size as a discriminating parameter) and Thailand. Malaysia applies differentiated vehicle excise taxes based on engine size. The Philippines differentiates vehicle taxes based on vehicle price.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| China             | China applies vehicle purchase taxes, allowing reductions for qualified energy-saving vehicles and exempting EVs and fuel cell electric vehicles (FCEVs).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Europe            | Taxes are differentiated based on engine power (Austria, Bulgaria, Croatia, Italy – also differentiating by powertrain type – and Spain) capacity (Belgium, Czech Republic, Hungary, Romania), CO <sub>2</sub> emissions/km (Cyprus, Luxembourg, and Sweden – also differentiating by powertrain type). Denmark, Finland, the Netherlands combine weight and CO <sub>2</sub> emissions/km as modulating parameters for vehicle taxes. France combines CO <sub>2</sub> emissions/km, weight (from 2022), and power. From 2023, France will also mandate a ceiling on EV manufacturing emissions for EVs to qualify for subsidies. Germany, Greece, Ireland, and Portugal combine CO <sub>2</sub> emissions/km and engine capacity. Latvia uses weight, engine capacity, and power. EVs and FCEVs are often exempted from or subject to taxation advantages: e.g., in Austria, Belgium, Cyprus, Czech Republic, Denmark, France, Germany, Ireland, Italy, Latvia, Luxembourg, Poland, Romania, Slovakia, Slovenia, Spain, and Sweden. |
| India             | India applies lower tax rates for EVs and FCEVs and also differentiates tax rates between cars and SUVs, penalizing the latter.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Japan             | Taxation favoured the adoption of smaller cars for a long time in Japan, where “Kei-cars” benefited from tax exemptions since their designation as the smallest vehicle segment in Japan, resulting in major contributors to the consistently high market shares of these vehicles in the country. Additionally, local policies exempt Kei-cars from the requirement that applies to all other private cars to own a “garage certificate” – a dedicated parking spot permit. However, like all cars, they are not allowed to use on-street parking overnight.                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Latin America     | Brazil applies vehicle registration taxes, including exemptions for EVs. Colombia has differentiated taxation based on LDV categories, with higher tax rates for more expensive vehicles and incentives for EVs. El Salvador has tax incentives for EVs (BEVs and PHEVs). Mexico applies tax rates based on vehicle prices with incentives or exemptions at the Federal and State level for EVs. Peru and Uruguay also apply tax exemptions for electric and hybrid vehicles.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| United States     | Vehicle registration taxes are applied at the Federal level, and so are tax credits for EVs and FCEVs. Complementary measures, including taxes and exemptions for energy saving vehicles, EVs and FCEVs are applied at the State level – e.g., via the Clean Vehicle Rebate Program in California.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

Sources: NEA Singapore, 2022; ITF, 2022; PWC, 2022; electrive, 2023; ACEA, 2022; Lipsy and Schipper, 2013; Parking Reform Atlas, 2021; UNEP et al., 2020; OECD, 2020; IRS, 2023; California Sales Tax Handbook, n.d.; California ARB, n.d..

second-hand used vehicles. In New Zealand, where second hand imports are the vast majority of the newly registered vehicles, the Clean Car Discount expanded earlier rebates for BEVs and PHEVs into a revenue-neutral feebate or bonus/malus scheme (New Zealand Transport Agency, 2023). The program has unique features globally, as it applies different rebate and fee curves for new versus used vehicles (with rebates and fees for used vehicles being about half those applied to new vehicles). The pairing of this differentiated vehicle taxation with New Zealand’s Clean Car Standard (discussed in Section 4.1.3) is especially interesting, as it is the only case of coherently developed regulatory and taxation mechanisms applicable to both new and second-hand imports aiming to address both CO<sub>2</sub> emissions and the EV transition.

### 4.3.3 VEHICLE TAXATION RELATED WITH INTERNATIONAL TRADE

Trade-related taxation policies, in particular duties applied to imports, can, like production incentives, contribute to the orientation of consumers’ choices and industry investments, insofar as they effectively alter product prices. Trade policies are also closely related with international taxation regimes including, in particular, rules and instruments that were developed under the framework of the World Trade Organization.<sup>59</sup>

The WTO framework attempts to promote open trade and avoid protectionism, while allowing for special provisions and flexibility for developing countries. It allows for the application of duties,



following specific procedures. Relevant agreements include one on Subsidies and Countervailing Measures (SCM) (WTO, n.d.a) and the General Agreement on Tariffs and Trade (GATT) (WTO, n.d.b). These place constraints on the use of subsidies but do not ban them outright, except if they are contingent upon export performance or local-content requirements (Wu and Salzman, 2014). Otherwise, subsidies are permissible under WTO law as long as they do not negatively harm the trade interests of other countries, meaning that a government may take unilateral actions in domestic administrative courts against another government's subsidy if it finds that the subsidy causes or threatens material injury to an established domestic industry (Wu and Salzman, 2014).

The WTO agreements also allow for other exceptions to GATT, including the need not to discriminate between “like” products and domestic and foreign products (WTO, n.d.c and WTO, n.d.d). The most relevant in the context of vehicle trade relate with Article XX of the GATT (WTO, n.d.e). This recognizes that the protection of the environment including natural resources is a legitimate object of governments.

Automobile emission standards aiming to protect air quality and reduce GHG emissions are well suited to comply with the Article XX exception to national treatment. Precedent for this exists: in the specific case of gas guzzler taxes applied in the United States, differentiated taxation for vehicles with higher GHG emissions was also deemed in line with WTO rules (WTO, 1994). A key aspect of the alignment is the requirement that the application of conditions not differ based on the country of origin.

Trade duties regarding cars and other transport vehicles are currently applied internationally on the basis of different frameworks. These span from full exemptions from any duty, as in the case of free-trade agreements, to the application of a range of different duty rates, in other cases. Import levies differentiated based on environmental reasons also exist – e.g., South Africa (PWC, 2022) – and there are cases where specific exemptions (sometimes conditional to prices) or reductions have been applied for EVs (e.g., Argentina, Armenia, Colombia, Ecuador, Indonesia, Paraguay, Philippines, Rwanda and Thailand) (PWC, 2022; IEA, 2020; Global Trade Alert, 2022; GEF 2021; Randall, 2022; TrendsInAfrica, 2023; UNEP et al., 2020).

Recent developments regarding trade and tariffs of critical materials, batteries, and EVs are leading to

significant trade-related tensions across the world. Domestic subsidies and tariffs are being formulated in consideration of prospects for continued EV market growth and also in light of the scale of the industrial transition needed to decarbonise transport and energy. Tensions are driven, above all, by the extensive use by different market players of measures supporting the scale up of EVs, automotive batteries, and related supply chains – including support schemes based on domestic content (CSIS, 2022), as these are not aligned with WTO rules. These may have strong implications on the way duties applicable to cars and other transport vehicles will develop. Key examples of controversial measures include the case of the New Energy Vehicle Subsidy Programme, which came to an end in China in 2022 but may still be complemented by supportive policies at the local level — leading to a move by the European Union to investigate further (Aizhu and Blenkinsop, 2023; European Union, 2023d) and the Inflation Reduction Act in the United States, which includes country-specific provisions (US Congress, 2022; US Treasury, 2023).

#### 4.3.4 LOCAL VEHICLE TAXES AND CHARGES

The application of charges and taxes is also possible at the local level, and it is common practice in some cities. Measures in this category include parking and access fees (i.e., congestion or cordon pricing), limited to specific urban districts or applicable across larger urban areas. These policies often have systemic impacts capable of enhancing energy efficiency and reducing environmental impacts — e.g., by stimulating shifts in modal mixes towards non-motorized or public transport (and more recently also to shared mobility services).

In some cases, they already integrate additional incentives to support the same goals through technology shifts, as in the case of targeted exemptions or differentiated charges based on pollutant and/or CO<sub>2</sub> emission levels. The most iconic are probably the cases of urban access charges in place in selected cities globally, including London, Milan, Stockholm and Singapore, also intended to manage efficiently the use of scarce road space (ITF, 2021a).

Differentiated local taxes and charges based on vehicle weight and footprint are not common but pioneering initiatives are starting to arise. These are discussed in section 4.4.3.

## 4.4 CHANGES IN VEHICLE TAXES TO ADDRESS VEHICLE WEIGHT INCREASES AND EQUITY-RELATED CHALLENGES

### 4.4.1 CHANGES IN COUNTRY-LEVEL TAXATION FRAMEWORKS

Evidence available from Chapters 2 and 3 shows the importance of introducing or refining elements related with weight, footprint, material requirements and equity to the criteria already used for the determination of vehicle taxation. Doing this can be instrumental in steering consumer demand and industry investments away from the continued increase in vehicle size and weight, mitigating the negative effects of the SUV shift, managing those of EVs in areas where they face greater criticalities, and ultimately reducing risks of asset stranding from governmental action to foster climate change mitigation and sustainability.

Policies already deployed in some countries offer important examples of taxation and pricing reforms capable of better addressing challenges related with trends towards vehicle weight and size increases and electrification. They can also inform strategies to transition from incentivizing EV adoption through

subsidies or preferential taxation to regulatory regimes that recognize the need to address the externalities of EVs, and to collect revenues to maintain infrastructure.

In Japan, fiscal advantages for Kei-cars<sup>60</sup> were deployed with the aim to limit energy use, rather than vehicle (or battery<sup>61</sup>) weight. This is because Japan is fully reliant on fossil energy imports, and this reliance also had negative impacts on its trade balance. However, increased consideration of battery materials as critical commodities sheds new light on the Japanese Kei-car policies: similar instruments could be worth serious consideration, especially in circumstances where the availability of battery materials is constrained and in countries that do not have access to the necessary resources, domestically or via their trade partners.

Norway, the country that is by far the global leader in transitioning to electric light-duty vehicles – at 88% market share in 2022 (IEA, 2023b) – has since 1995 levied a purchase tax on ICEV vehicles that is based on vehicle weight, CO<sub>2</sub> and NO<sub>x</sub> emissions. The weight tax applies to cars above 500 kg, and increases linearly, with the tax per kg increasing above 1,200 kg and again above 1,500 kg. The CO<sub>2</sub> emissions tax curve increases at regular intervals as well, and vehicles with CO<sub>2</sub> emissions below a certain value are awarded deductions to the tax (although the minimum tax is 0; i.e., consumers do not receive a subsidy or tax rebate). Starting in 2023, Norway discontinued its exemption of electric vehicles with a sticker price exceeding NOK 500,000 (about USD 46,000) from VAT. At the same time, it added an additional fee on vehicle imports (including all EVs and used vehicles) based on weight (Toll Customs Norway, 2023). While the announced change in the tax regime led to a spike in ICEV and BEV sales in December 2022, with sales of more than 2.5 times the December 2021 volumes (Holland, 2023), longer term impacts are more likely to lead to increased product diversification for EVs, away from heavy vehicles (and batteries).





France's bonus/malus feebate scheme was revised in 2022 to levy additional taxes on heavier vehicles. Vehicles that weigh more than 1,800 kg are subject to an additional tax of EUR 10/kg, with the additional weight tax ceiling at EUR 50,000. However, BEVs, FCEVs, and PHEVs with an all-electric range higher than 50 km are exempt (Government of France, 2023). A recent proposal suggested to define an eligibility scale for the French bonus/malus (still dependent on g CO<sub>2</sub>/km), modulated on the basis of size or weight of the vehicle, rather than based on its price, or by crossing weight and size (Robinet and Gérardin, 2022). The idea follows an earlier proposal, also aiming to support consumer demand and value creation for smaller and lighter vehicles, helping to make EVs available at lower prices, minimize CO<sub>2</sub> emissions compared to ICE vehicles, and also compared with the lifecycle emissions of larger EVs (Meilhan, 2019). Other benefits include the possibility to limit increases in public spending linked to incentive schemes by limiting their applicability. Further benefits are associated with lower pressure on resource extraction related with EV battery materials.

Other vehicle taxation tools that can help disincentivise the purchase of larger and heavier EVs and favour the purchase of smaller, more efficient ones, include scaling down EV purchase incentives proportionally to energy consumption (with advantages for more energy efficient EVs), and adding a purchase tax proportional to EV energy consumption.

Due to the variability of mission profiles for different vehicles, including in particular highly utilized cars and vans used in taxi and car- or ridesharing services (both of which are more likely to need large battery packs to fulfil daily driving operations), there is merit in the consideration of dedicated exceptions/rules for these use cases (conditional to effective use of vehicles for these services, e.g., by requiring minimum amount of km/year to access to tax rebates). California's Clean Miles Standard (Government of California, 2018), which requires that ridesourcing services reduce GHG emissions per passenger km, is synergistically paired with incentive programs for a shift to EVs, is an example of a policy capable of delivering CO<sub>2</sub> cuts at lower costs (Rajagopal and Phadke, 2019).

Regarding corporate cars, equity considerations call for existing privileges to be effectively removed (Harding, 2014; Carpenter and Antich, 2022). Especially if paired with an overall upward revision, freeing up budget for redistributive purposes,<sup>62</sup> corporate car taxes can also be better used to foster an alignment with sustainability objectives.<sup>63</sup> This may be achieved by factoring in stronger differentiations based on GHG emissions (reversing lower purchase grants for EVs in many countries), size, weight or a combination of these (integrating elements capable of addressing

resource depletion and road safety concerns, while also accounting for the relevance of changes in battery chemistries to manage material criticalities), as well more stringent requirements for active road safety features and progressivity of taxation with price increases.

As corporate cars can account for large shares of new vehicle registrations — and are the majority in a high-income areas like the European Union (Carpenter and Antich, 2022), likely more than that in medium- and low-income countries — these changes can also provide a way to increase the availability of more affordable and sustainable second-hand cars, including EVs, for lower-income households and businesses.

#### 4.4.2 CHANGES IN VEHICLE TAXATION RELATED WITH INTERNATIONAL TRADE

Decisions taken at the WTO considered that the use of differentiated taxation based on prices (and therefore also product differentiation within the automobile category), including for imports, is aligned with WTO rules, as long as the differentiation is not implemented to protect the domestic production of automobiles (WTO, 1994). The compliance of automobile emission standards aiming to protect air quality and reduce GHG emissions with WTO rules (by virtue of Article XX of the GATT) also indicates that, in principle, there are possibilities to consider other criteria allowing to address environmental challenges induced by vehicle weight increases, such as those associated with mineral availability related with EV batteries.

As in the case of other the more general considerations on trade-related taxes, developed in Section 4.3.3, the topic is the subject of significant geopolitical tensions. Part of the reason lies in export restrictions, especially in cases where these are applied to materials for which a major global supplier controls high shares of overall global extraction and processing, and which serve as key inputs for the automotive EV and battery industries, along with other strategic sectors — with key examples relating to practices applied by China, for rare earths and, more recently, graphite (Wu and Salzman, 2014, European Commission, 2023b).

This suggests that, while there is the technical possibility to make progress on changes in vehicle taxation related with international trade that could help addressing criticalities flagged in Chapter 3 (namely vehicle weight increases, mineral availability, and equity aspects), their practical viability depends upon developments in the effectiveness of processes facilitating dialogue, and on negotiations taking place at the intergovernmental level.



#### 4.4.3 CHANGES IN LOCAL VEHICLE TAXES AND CHARGES

Taxes and charges adopted at the local level can also be tailored to specific objectives associated with challenges posed by vehicle weight increases and equity-related aspects. Higher parking fees for larger, heavier vehicles adopted in Paris and other French cities, starting in 2024, are recent prominent examples of differentiated fees based on vehicle weight, currently representing best practice globally.

Differentiated fees will first be rolled out in the four central urban districts, taking into account the vehicle size and weight, and engine type (Ville de Paris, 2023; Riposseau, 2023; Willsher, 2023; Dow, 2023 and Sergeev, 2023). EVs may be exempt from larger fees or be subject to different weight thresholds, aiming to account for higher weight for comparable size with ICEVs. Exemptions are also foreseen for large families, low-income families, and disabled drivers. Fees are expected to range from EUR 15 per month for electric vehicles to triple that for the largest and heaviest ICE SUVs. In France, Lyon has also announced the plan to adopt a similar parking fee structure from 2024, and has already proposed a fee structure that starts at EUR 15 per month for all but the largest cars with low-emissions stickers (Crit'Air vert); EUR 30 per month for ICE cars from 1000-1725 kg and HEVs from 1000-1900 kg; and EUR 45 per month for ICEVs and HEVs heavier than 1725 and 1900 kg, respectively, as well as for cars with low-emission stickers weighing more than 2200 kg (Riposseau, 2023).

Grenoble is expected to adopt a similar measure in the near future.

Regarding equity-related challenges, due to the SUV shift and EV transition and the application of differentiated charges for large vehicles and ICEVs vs. EVs (but also regulatory measures limiting circulation for ICEVs, and in particular low- and zero-emission zones), recent analysis developed in France flagged the importance of targeted relief measures accompanying low-income households, especially in cases of limited access to alternative modes, and in a phase when limited volumes of second-hand EVs are available<sup>64</sup> (Robinet and Gérardin, 2023).

### 4.5 FUEL TAXATION AND CARBON PRICES

Efficient levels of taxation on fossil fuels used in transport, are crucial for discouraging the deployment of vehicles with larger weight and footprint, and also for fostering the EV transition, as shown in Chapter 2. A first priority is removing harmful and unsustainable subsidies for fossil fuels, but efficient taxation should include also other “external” costs due to environmental damage, congestion, crashes, road damage and general consumption taxes (Parry et al., 2021).<sup>65</sup> Taxing fossil fuels for road transport is also crucial to avoid giving a competitive advantage to carbon-intensive options, which risk locking in GHG emissions for long periods of time.



Some level of fuel taxation is already in place in most — but not all — countries, primarily in the form of excise and value added taxes.<sup>66</sup> Differences in existing taxation schemes across countries are influenced by the historical availability (or lack thereof) of oil resources, with lower tax rates generally applied in countries with higher oil reserves, resources and domestic production, and higher tax rates for net oil importing countries. According to the International Monetary Fund, however, under-pricing of road fuels is pervasive across many countries, with 70% of global gasoline consumption being priced, in 2021, at less than 60% of efficient levels<sup>67</sup>, and 50% of diesel fuel being priced at less than half the efficient level (Parry et al., 2021).

Beyond taxation of transport fuels, the adoption of economy-wide carbon pricing is particularly relevant in countries that have limited availability of fossil energy. Notwithstanding challenges related to increases in fossil fuel prices due to geopolitical tensions, carbon pricing is essential to meeting objectives aligned with climate imperatives, including a global transition to net zero emissions. Carbon prices not only support shifts in consumer choices towards low- and zero-carbon technologies, but also leverage the residual demand for carbon-intensive fuels to collect government revenues, which will be crucial to financing redistributive policies during the energy transition (an aspect that has specific relevance for EVs, in transport, due to their higher upfront cost and the resulting equity challenges).

One of the best practices regarding the adoption of carbon pricing for equity-related considerations is the case of the creation of a Social Climate Fund accompanying the creation of a separate Emissions Trading System (ETS), specifically dedicated to road transport and buildings, in the European Union, with fuel distributors as regulated entities.<sup>68</sup> Starting in 2027, this instrument will ensure price signals pass to consumers to stimulate investments in energy efficiency and energy diversification (European Parliament, 2022 and European Council, 2022). It will also use revenues generated by the ETS — up to a maximum amount of EUR 65 billion (European Parliament, 2022 and European Council, 2022) — to support Social Climate Plans meant to address the impact of carbon pricing on vulnerable households, microenterprises and vulnerable transport users. EU Member States will be required to contribute at least to 25% of the estimated total costs of their Plans.

In Europe, the reform of the ETS (European Union, 2023e), paired with the introduction of a Carbon Border Adjustment Mechanism (CBAM) (European Union, 2023f), are also instrumental to supporting the transition of the industry sector towards technologies that are compatible with the achievement of economy-

wide net zero emissions included in the Climate Law (European Union, 2021). This includes the production of key materials needed in the automotive sector, in particular aluminium and steel, as well as other materials necessary for road transport infrastructure (namely iron, steel, and cement).

#### 4.5.1 ROAD USER CHARGES TO COMPLEMENT OR PROGRESSIVELY REPLACE FUEL TAXATION

Road user charges are a policy solution that offers the potential to make up for lost fuel-duty revenues and adequately price vehicle operations. Opting for this solution would effectively switch the tax base to distance travelled rather than energy use (ITF, 2021b; OECD, 2019b).

Distance-based charges effectively apply the ‘polluter pays’ principle, where those who produce pollution bear the costs of the damage they inflict on others or the environment. Location-specific and time-dependent distance-based charges could provide a cost-effective way to address congestion, whose costs are particularly high in urban areas and at certain times of day. Charges could also potentially be differentiated to incentivize PHEVs to drive in all-electric mode and to reflect different impacts on street space occupation and road safety risks for vehicles with different sizes, weight and safety features, helping to address other negative environmental and social externalities of road transport, in particular emissions of local air pollutants, noise and traffic crashes. Since electric vehicles have fewer negative externalities associated with pollutant and GHG emissions than conventional vehicles, user charges applying to EVs would likely be lower than for comparable ICEVs (ITF, 2021b).

The shift to road user charges is likely to be complex, since governments need to find the balance between stimulating innovation and the technology transition, while also addressing the issue of revenue shortfalls (although carbon pricing can mitigate this, at least for some time, but not without challenges, particularly in the context of increasing oil prices). Moreover, road user charges will be needed to restrain potential increases in vehicle use driven by the lower travel costs of EVs, while maintaining incentives to switch to EVs and limiting social equity impacts. This complexity calls for a gradual shift, as well as the establishment of a solid technological basis for managing the transition, along with clear communication between stakeholders (including individuals that will adopt EVs) that will be affected by the change (ITF, 2021b).



## 4.6 ALTERNATIVE ENERGY INFRASTRUCTURE (EV CHARGERS)

The analysis in Chapter 3 highlights the fact that increased EV sales are being accompanied by increases in battery size. This is due to preferences oriented towards long-range vehicles, especially for wealthy consumers, a choice that is likely to be exacerbated by limitations in the availability of EV charging infrastructure.

Large batteries for EVs are an inefficient use of scarce resources, especially for personal vehicles, as they are not being driven for the vast majority of the time (typically they are parked around 95% of the time). Bottlenecks limiting the availability of materials needed to manufacture batteries are exacerbated by these choices, calling for demand-side measures to mitigate these issues (Box 2). Policies that can shift sales toward smaller EVs, incentives based on actual electric vkm for early deployment, and promoting all-electric driving for PHEVs,<sup>69</sup> could effectively deliver more fossil fuel displacement at lower costs than a strategy promoting fewer EVs with larger batteries. Large EV batteries also increase average vehicle costs, thus limiting the EV transition, and its benefits (lower total cost of ownership) to high income households.

The value-added of long-range EVs for consumers is likely to decrease as access to EV charging

infrastructure, at affordable electricity prices, is effectively developed. Governments and OEMs should therefore collaborate to speed up the development of a capillary charging infrastructure network.

The Alternative Fuels Infrastructure Regulation (AFIR) of the European Union is the first example of a regulatory instrument that requires the construction of a minimum network of charging and refuelling stations along the trans-European road network, including several urban nodes and, as national plans are also finalized, on other major roads, in each Member State (European Union, 2023g).

In addition, a wide range of technical standards and other regulatory requirements are still being negotiated at the time of writing, such as the Energy Performance of Buildings Directive. The Directive includes provisions regarding electric vehicles, grounded on the consideration that charging in relation to buildings is particularly important, since this is where electric vehicles park regularly and for long periods of time, slow charging is economical and the installation of recharging points in private spaces can provide energy storage services to the building and integration of smart charging services and system integration services in general (European Commission, 2021). Pre-cabling is to become the norm for all new buildings and buildings undergoing major renovation, and barriers to the installation of recharging points in residential buildings, ensuring a “right to plug”, need to be removed. These provisions have been reinforced in following negotiating steps with clearer references to bidirectional charging, and the role of e-bikes and e-scooters in terms of the allocation of parking space, also in non-residential buildings (European Parliament, 2023a).



Other major initiatives enabling a widespread development of EV chargers have also been undertaken, over the years, in major EV economies, including China (with major investments over the years by its State Grid Corporation) and the United States. In the case of the United States, these have significantly accelerated thanks to activities and funds disbursed by the Joint Office of Energy and Transportation, established by the Bipartisan Infrastructure Law of 2021 (US DOT, n.d.) and representing a modernized inter-agency approach, bringing together expertise from the Departments of Energy and Transport to support the deployment of zero-emission, convenient, accessible, equitable transportation infrastructure (Joint Office, n.d.).

Public support, leveraging revenues from carbon taxation and debt-driven investments for infrastructure deployment (including funds that became available in the context of Covid-19 response package following the Covid-19 pandemic) can also be effective to support private investments in EV chargers, beyond

minimum regulatory requirements.<sup>70</sup> Public revenue has effectively been allocated for this purpose in major initiatives like the NextGenerationEU instrument (European, Commission, 2023c) in Europe and the bipartisan Infrastructure Law in the United States (DOT, n.d.). Similar considerations also apply to grid reinforcements, including with interconnectors, to enhance the reliability and the profitability of variable renewable electricity generation.

Reforms in electricity market designs — such as the one developed in the European Union (European Commission, 2023d) and previous EU reforms — are not only essential in cases where the existing structure is being challenged by geopolitical circumstances, but also helpful to enable to extract value from the effective management of EV charging, including via demand-side flexibility mechanisms (Bashar Anwar et al., 2022). This can effectively support the use of EVs and related charging infrastructure as assets providing grid services, rather than as liabilities for the electricity systems.

## 4.7 SUSTAINABLE FINANCE AND DEVELOPMENT AID FUNDING

Sustainable finance frameworks are important to help achieving a better alignment between the decisions taken by investors, corporations and other entities with the needs dictated by risks (including those posed to the financial system) associated with climate change, biodiversity loss and other environmental consequences of economic and industrial activities. These include instruments that ensure transparent reporting and financial disclosures of exposure to these risks. They also include frameworks that help steering investments towards low-carbon and clean solutions, thanks to the clear identification of sustainability-aligned assets.

Key instruments belonging to this category of policy tools include the Taxonomy Regulation developed in the European Union in the recent past, and a number of similar initiatives being undertaken in other geographies. These include specific references to sustainability-aligned vehicles, components/parts, including EVs, and also cover charging infrastructure.

Their development can ensure that costs of borrowing for sustainability-aligned assets is subject to lower rates of interest in comparison with other products and serve as a corrective mechanism in cases of misaligned responsibility in the socialization of costs due to environmental impacts.

Current taxonomies, when considering the automotive sector, tend to be primarily focused on tailpipe emissions of CO<sub>2</sub>. While lifecycle accounting can be effectively accounted for by other provisions, e.g., in the energy transformation and industry sectors, existing frameworks give very limited — if any — consideration to weight-related attributes of vehicles. A better integration of these aspects can effectively address risk mitigation goals of these frameworks, in similar fashion to the case of investments in less energy intensive modes of transport with respect to passenger cars and LCVs. Financial mechanisms, including debt service

reserves (where governments keep cash deposits to make interest and principal payments in case a private borrower fails to make scheduled payments), government-held subordinated debt (where a public agency agrees to take on a lower priority position for debt repayment than senior debt holders), credit insurance products for bond financing (consisting of government insurance agreeing to make bond payments in case the issuer defaults), public loans and loan guarantees (enabling act as a guarantor for the private sector to obtain a market loan with a lower interest rate), grants and co-investment are also important to complement other measures (such as advance market commitments, e.g., linked with public procurement) that help to de-risk private investments needed for the industrial transformation that accompanies the EV transition.

Other initiatives are also important to better align the needs for a technological transition and equity-related aspects. These include the development of instruments facilitating access to EVs for capital-constrained households and small businesses. One example is the micro-credit mechanism developed in France, targeting entities lacking access to credit from conventional financial institutes and including a 50% guarantee by the government (Government of France, 2021).

In the international context, initiatives favouring access to capital at lower cost are crucial to help low- and medium-income countries to seize opportunities to accelerate their transition to EVs. This can be enabled by the possibility for Multilateral Development Banks (MDBs) to borrow (and therefore also lend) and at very favourable terms, if this possibility is focused on projects characterized with a better alignment with the SDGs (Cazzola and Santos Alfageme, 2023). The development of an internationally agreed, science-based international classification system (a taxonomy, similar to the one mentioned above for the EU) is a likely prerequisite to enable this development. The integration of EVs (especially if qualified based on considerations related with intensity of use and battery size), battery material extraction (subject to other sustainability and due diligence requirements) and battery recycling facilities into such a taxonomy are all in line with the objectives to ensure a greater sustainability of the value chain, to contribute to more equitable investments for industrial development, to foster the EV transition in the Global South, and also to address weight-related challenges discussed in this report.



# ANNEX: METHODOLOGICAL NOTE

This edition of the GFEI benchmarking report marks a change in the data and methodology used to obtain the results. Previous iterations of the GFEI report used model-level sales and technical characteristics for all included countries; this data was then aggregated at a country and global level to assess the progress of new vehicle specific energy consumption. This iteration of the GFEI report differs in two respects:

- The source of core sales data changed from a provider that gives model-level (and for some countries, trim-level) data — including technical specifications such as fuel and powertrain type, vehicle weight, footprint, engine capacity, and more — to another provider that provides segment level data without detailed vehicle technical specifications, and with less granular designation of powertrains (i.e. ICE, mild hybrid, hybrid, plug-in hybrid, battery electric, and fuel cell electric).
- In switching data providers, both the resolution and country coverage have changed. In order to ensure consistency across data sources, vehicle segment definitions were standardised, both between data sources and across countries).

This section describes three elements of the renewed methodology. It first outlines the data sources used, then describes the key data processing steps that were carried out, and concludes by explaining the new WLTP conversion factors applied.

## A.1 DESCRIPTION OF DATA SOURCES

### A.1.1 FUEL ECONOMY IN MAJOR CAR MARKETS (2005-2017) DATA, GFEI\_0517

These are the data underpinning the GFEI Working Paper 19, published in 2019 (IEA, 2019a).

The data have varying levels of granularity, with data for most major car markets being at the model-trim level.

- Vehicle characteristics include: size (wheelbase, width, height), weight (gross weight, kerb weight), engine (displacement, power), powertrain, segment, price.
- Vehicle segments are: Small Car, Medium Car, Large Car, Small SUV, Large SUV, Light Commercial Vehicle
- Powertrains: Diesel, Petrol, LPG, CNG, Hybrid, Battery Electric, Plug-in Hybrid, Fuel Cell Electric

### A.1.2 GFEI 2021 DATA, IEA\_19

These are the data made publicly available on the online GFEI 2021 Data Explorer by the IEA with the 2021 version of the GFEI report (IEA, 2021a).

This dataset contains information for the same set of countries as those included in the GFEI\_0517 data, and the data underlying the analysis are organized according to the same segment and powertrain categories.

The publicly available data reported in the Data Explorer are aggregated output data, not the high-resolution input data used to develop that report. This means that the results are only available at for broad categories, namely:

- fuel consumption by country, powertrain, and year
- fuel consumption by country, segment, and year
- footprint by country and year,
- weight by country and year.

### A.1.3 AUTOMOTIVE SALES DATA FROM MARKLINES

Marklines is a provider of automotive industry intelligence, including sales volumes, for a wide range of countries, as shown in Table A1. Vehicle sales are categorized by Type, Segment, and Powertrain. The

TABLE A1: Country coverage by data source and regional grouping

| Country              | GFEI_0715 | IEA_19 | Marklines | EEA |
|----------------------|-----------|--------|-----------|-----|
| Argentina            | x         | x      | x         |     |
| Australia            | x         | x      | x         |     |
| Belarus              |           |        | x         |     |
| Brazil               | x         | x      | x         |     |
| Canada               | x         | x      | x         |     |
| Chile                | x         | x      | x         |     |
| China                | x         | x      | x         |     |
| Colombia             |           |        | x         |     |
| EEA countries        | x         | x      | x         | x   |
| Egypt                | x         | x      | x         |     |
| India                | x         | x      | x         |     |
| Indonesia            | x         | x      | x         |     |
| Israel               |           |        | x         |     |
| Japan                | x         | x      | x         |     |
| Kazakhstan           |           |        | x         |     |
| Korea                | x         | x      | x         |     |
| Kuwait               |           |        | x         |     |
| Malaysia             | x         | x      | x         |     |
| Mexico               | x         | x      | x         |     |
| Myanmar              |           |        | x         |     |
| New Zealand          | x         | x      | x         |     |
| North Macedonia      |           |        | x         |     |
| Oman                 |           |        | x         |     |
| Pakistan             |           |        | x         |     |
| Peru                 | x         | x      |           |     |
| Philippines          | x         | x      | x         |     |
| Puerto Rico          |           |        | x         |     |
| Russia               | x         | x      | x         |     |
| Saudi Arabia         |           |        | x         |     |
| Singapore            |           |        | x         |     |
| South Africa         | x         | x      | x         |     |
| Switzerland          | x         | x      | x         |     |
| Taiwan               |           |        | x         |     |
| Thailand             | x         | x      | x         |     |
| Turkey               | x         | x      | x         |     |
| United Arab Emirates |           |        | x         |     |
| Ukraine              | x         | x      | x         |     |
| United Kingdom       | x         | x      | x         |     |
| United States        | x         | x      | x         |     |
| Uruguay              |           |        | X         |     |
| Uzbekistan           |           |        | x         |     |
| Vietnam              |           |        | x         |     |

**Note:** Table A1 also provides information on data availability from other data sources used in this assessment.



data download extends from 2005 to 2022. Over this period there are varying degrees of granularity for the data within in each country. This means that for a given country, model level data might only be available for certain years and not for others. When model level data is missing, regional averages are used to fill the gaps.

A.1.4 CO<sub>2</sub> EMISSIONS FROM CARS AND VANS, EEA, EEA

This dataset includes registrations of new vehicles at a model level in the European Economic Area (the European Union plus Norway, Switzerland, and Iceland).

Vehicle characteristics include: size (wheelbase, width, height), weight (gross weight, kerb weight), engine (displacement, power), and powertrain. These data were downloaded from 2017 to 2022 (with the 2022 data being provisional), from the EEA data hub (EEA, 2023a; EEA, 2023b).

A.2 DESCRIPTION OF DATA PROCESSING STEPS

The aim of the data processing is to use all available datasets to provide an update to the GFEI benchmarking report, without having access to the data from the original data provider. Therefore, data processing must harmonise datasets in terms of category names, segments (and segment-specific weight and footprint), powertrains (and powertrain-specific weight and footprint), fuel economy test cycles, and geographical coverage.

This can be done by moving the analysis to the minimum common level of granularity across the available datasets. In this case, that is the “country-powertrain-segment” combination (i.e. the level of resolution provided in the Marklines dataset).

A.2.1 PREPARING MARKLINES SALES DATA

Filter Marklines sales data to remove sales that do not fall in the definition of Light Duty Vehicles (gross vehicle weight < 3,500 kg).

Harmonise the Marklines vehicle segmentation naming to what is used in the IEA\_19 data, based on the matching approach shown in Table A2.

A.2.2 PREPARING IEA SPECIFIC ENERGY CONSUMPTION DATA

The IEA specific energy consumption data is only available at the aggregated level for country-powertrain-year and country-segment-year combinations. These data were combined: SEC of each country-segment combination was scaled up or down depending on the powertrain.

The powertrain scaling factors depend on the relative SEC of each powertrain (e.g., hybrid vehicles consume 20% less energy than conventional gasoline, all else being equal) and on the powertrain mix within each country-segment combination in 2019.

The GFEI\_0517 data fed the information underpinning the powertrain scaling factors. The final result is a dataset of country-powertrain-segment time series of sec.

A.2.3 PREPARING EEA DATA

The specific energy consumption for each vehicle was calculated starting from the CO<sub>2</sub> emissions by using CO<sub>2</sub> emissions per unit volume for different fuels and then by converting them based on the volumetric energy density of the fuels. The final values (shown in Table A2) are consistent with the indication given by the IPCC regarding the way emissions of greenhouse gas emissions from mobile sources should be reported (IPCC, 2006).

For electric vehicles, specific energy consumption was calculated from the available data on electrical consumption stated in Wh/km. This was converted to Lge/100 km, assuming an energy content of gasoline of 9.3 kWh/Lge.

For PHEVs, the electric consumption was added the fuel consumption derived from CO<sub>2</sub> emission data and the electric consumption data combined through a utilisation factor, calculated according to the “best estimate” Utility Factor formula developed by Fraunhofer ISI (Fraunhofer ISI, 2021) based on the electric range of each model. When this data was not available, a default utilisation factor of 0.5 was used instead.

TABLE A2: Mapping from GFEI / IEA\_19 segment to Marklines segment

| GFEI Segment | Marklines Segment |
|--------------|-------------------|
| Small car    | A                 |
|              | B                 |
| Medium car   | C                 |
| Large car    | D                 |
|              | MPV               |
|              | E                 |
|              | F                 |
| Small SUV    | SUV-A             |
|              | SUV-B             |
|              | SUV-C             |
|              | SUV-D             |
| Large SUV    | SUV-E             |
|              | Pickup Truck      |

TABLE A3: CO<sub>2</sub> emissions per unit volume of different fuels

| EEA fuel type   | Carbon content (kg CO <sub>2</sub> /Lge) |
|-----------------|------------------------------------------|
| petrol          | 2.32                                     |
| petrol/electric | 2.32                                     |
| e85             | 2.32                                     |
| diesel          | 2.48                                     |
| diesel/electric | 2.48                                     |
| ng              | 1.88                                     |
| lpg             | 2.1                                      |
| ng-biomethane   | 1.88                                     |
| cng             | 1.88                                     |
| gnl             | 1.88                                     |
| other           | 2.32                                     |
| Unknown         | 2.32                                     |

Source: in line with the IPCC guidelines on the reporting of CO<sub>2</sub> emissions from fuel combustion from mobile sources, considering 69.3 g CO<sub>2</sub>/MJ, for gasoline (IPCC, 2006), and 33.5 MJ/L for gasoline.



A.2.4 MATCHING OF POWERTRAIN CATEGORIES WITH MARKLINES CATEGORIES

A list of all car models included in the EEA list was manually matched to the model names available in Marklines. This matching of information enables to assign a vehicle segment to each registration included in the EEA data.

A.2.5 JOINING SPECIFIC ENERGY CONSUMPTION, WEIGHT, AND FOOTPRINT DATA TO SALES DATA

Specific energy consumption data from IEA\_19 data was merged with the relevant “segment-powertrain-country” combination of the Marklines data.

Footprint and weight data from GFEI\_0517 was associated with the relevant “segment-powertrain-country” combination of the Marklines data. It was necessary to use this older dataset for footprint and weight because IEA\_19 does not provide sufficient granularity.

A.2.6 IMPROVEMENTS IN ICE VEHICLE EFFICIENCY TECHNOLOGIES

A drawback of the current approach is that, except for EEA countries where model-level data on specific energy consumption is available (for 2017-2022), it is impossible to assess improvements over time within powertrain-segment groupings. This is especially important for ICE engines, where specific

fuel consumption can vary significantly depending on the technology applied (turbocharging, cylinder deactivation, etc.).

The approach followed focused a survey of recent changes in specific fuel consumption in top-selling models. The top 20 selling models in the USA, China, and Japan in 2022 were identified. The fuel economy of these vehicles was matched with external sources in each market — USA (Fuel Economy Guide, 2023), Japan (MLIT, 2020), and China (MIIT, 2023).

For the above countries, the observed annual improvement for each year between 2019 and 2022 in the top 20 selling models was applied to ICE vehicles. For all other countries, a 1% per year improvement rate was assumed, a value that is in line with historical improvement rates.

A.2.7 MISMATCH BETWEEN VEHICLE FACTORY SHIPMENTS AND REGISTRATIONS IN CHINA

Light-duty vehicle volumes reported in Marklines correspond to official sales volumes reported by the China Association of Automobile Manufacturers (CAAM, 2023). CAAM data is collected from car manufacturers and represents factory shipments, and hence includes exports and excludes imports.

Since the GFEI database set seeks to compare LDVs registered in and across national and regional markets, total registrations were estimated by matching sales volumes reported in the Global EV Outlook (IEA, 2023b). The corrected volumes very closely match totals reported by CAAM, after deducting exports of ICE and new energy vehicles (NEVs include plug-in hybrid, battery electric, and fuel-cell electric vehicles).

A.3 APPLYING NEW WLTC CORRECTIONS

All specific energy consumption values in this report are defined in WLTC terms. In previous iteration of the report, theoretical conversion factors between WTLC and other drive cycles were used. This year, it was possible to use real world data on WTLC and NEDC test cycles, thus enabling a re-benchmarking of the data. The difference between NEDC and

WLTC varies by fuel type and, to a lesser extent, by segment type.

Table A4 shows the zero-intercept regression values by fuel-powertrain combination and by vehicle category, where passenger cars in the EEA database corresponds to Passenger Light-Duty Vehicles (PLDVs) and Light-Commercial Vehicles are LCVs, in this report). These new conversion factors were applied to the GFEI\_0517 data across all fuel-powertrain-category (PLDV/LCV) combinations, to generate updated WLTC-harmonised specific energy consumption value for each “segment-powertrain-country” timeseries.

TABLE A4: NEDC to WLTC conversion factors, based on EEA database, 2019-2022

| Powertrain      | Category | Ratio | Source                             |
|-----------------|----------|-------|------------------------------------|
| Diesel          | LCV      | 1.28  | EEA database analysis              |
| Electric        | LCV      | 1.21  | JRC, 2017                          |
| Petrol          | LCV      | 1.17  | EEA analysis                       |
| Hybrid petrol   | LCV      | 1.17  | Set equal to Petrol, by assumption |
| Unspecified     | LCV      | 1.17  | Set equal to Petrol, by assumption |
| Petrol-Electric | LCV      | 1.19  | EEA analysis                       |
| CNG             | LCV      | 1.13  | EEA analysis                       |
| LPG             | LCV      | 1.09  | EEA analysis                       |
| Flexfuel        | LCV      | 1.00  | EEA analysis                       |
| Hybrid diesel   | LCV      | 1.28  | Set equal to Diesel, by assumption |
| Diesel plug-in  | LCV      | NA    | See table note                     |
| Hydrogen        | LCV      | 1.21  | JRC, 2017                          |
| Diesel          | PC       | 1.24  | EEA analysis                       |
| Electric        | PC       | 1.283 | JRC, 2017                          |
| Petrol          | PC       | 1.19  | EEA analysis                       |
| Hybrid          | PC       | 1.19  | Set equal to Petrol, by assumption |
| Unspecified     | PC       | 1.19  | Set equal to Petrol, by assumption |
| Hydrogen        | PC       | 1.28  | JRC, 2017                          |
| Petrol-Electric | PC       | NA    | See table note                     |
| CNG             | PC       | 1.16  | EEA analysis                       |
| LPG             | PC       | 1.15  | EEA analysis                       |
| Flexfuel        | PC       | 1.06  | EEA analysis                       |
| Hybrid diesel   | PC       | 1.24  | Set equal to Diesel, by assumption |
| DIESEL PLUG-IN  | PC       | NA    | SEE TABLE NOTE                     |
| CNG             | PC       | 1.19  | EEA ANALYSIS                       |

Note: Plug-in hybrid electric vehicles were assumed to have specific energy consumption intermediate to BEVs and HEVs, assuming a Utility Factor of 0.5. The segment, country, and year-specific updated SEC of BEVs and HEVs were used to estimate the specific energy consumption of PHEVs, so: SEC<sub>PHEV</sub> = (SEC<sub>BEV</sub> \* UR + (1-UF) \* SEC<sub>HEV</sub>).



A.3.1 RE-BENCHMARKING NEDC TO WLTC CONVERSION FACTORS

From 2011 to 2021, analysts at the IEA have updated assessments of the rated specific fuel consumption of light-duty vehicles (LDVs) based on proprietary data covering nearly 90% of new LDV sales/registrations (Cuenot and Fulton, 2011, Cuenot and Körner, 2013, IEA, 2019a, and IEA, 2021a). These data were merged, cleaned and validated based on publicly available databases, reported technical specifications for various models from OEMs, and research and technical reports. To enable global comparisons across countries and major markets, conversion from regional or national test cycles to a single globally harmonized test cycle, the Worldwide harmonized Light-duty Test Cycle (WLTC), was performed on the basis of engineering-based simulation models designed to measure fuel consumption and CO<sub>2</sub> emissions for a variety of vehicle and technology packages and for a particular driving cycle. From 2016 to 2021, conversion factors were taken from powertrain-specific (i.e. gasoline and diesel ICE) zero intercept regressions developed by the ICCT (Kühlwein et al., 2014). These were developed based on modelling from Ricardo’s Data Visualization Tool (DVT), (Meszler et al., 2013) based on MSC Easy5 (Hexagon, n.d.). Conversion factors across test cycles (CAFE, NEDC, JC08, WLTC) are reported for gasoline and diesel in Table 5.2 of the ICCT 2014 report (Kühlwein et al., 2014).

For the data update in progress, based on recent literature demonstrating that the gap between NEDC and WLTC is larger than had been initially assessed in 2014 (Tsiakmakis et al., 2017, Pavlovic et al., 2018, JRC, 2023; Dornoff et al., 2020, Dornoff, 2023), the regressions were done using actual type approval data on NEDC and WLTC test cycle CO<sub>2</sub> emissions performance for all light-duty vehicles registered across Europe from 2019-2022, as reported by the European

Environmental Agency (EEA) and shown, for diesel and gasoline passenger cars, in Figure A4.

These ratios were determined also separately for passenger vehicles and light commercial vehicles for all basic powertrain-fuel combinations in the EEA dataset (gasoline, diesel, natural gas, LPG, gasoline-electric, diesel-electric, e85). Since direct CO<sub>2</sub> emissions for battery-electric and fuel-cell electric vehicles are 0 g CO<sub>2</sub>/km, ratios for specific energy consumption as measured by NEDC versus WLTC are taken from the JRC (Tsiakmakis et al., 2017).

These results summarized in Table A5, indicate that the simulated estimate for conversion factors between NEDC and WLTC developed in 2014 were lower by a factor of 1.05 for gasoline and 1.20 for diesel LDVs.

Figure A5 points to a larger gap in Europe than elsewhere and also to larger corrections in earlier years. This is primarily due to the larger share of diesel vehicles (which are subject to a greater rebasing factor of 1.2, versus 1.05 for gasoline) in Europe than in any other markets. At a global level, the larger gap in earlier years is attributable to the greater weight of European vehicle sales in global totals.

A.4 REGIONAL AGGREGATIONS

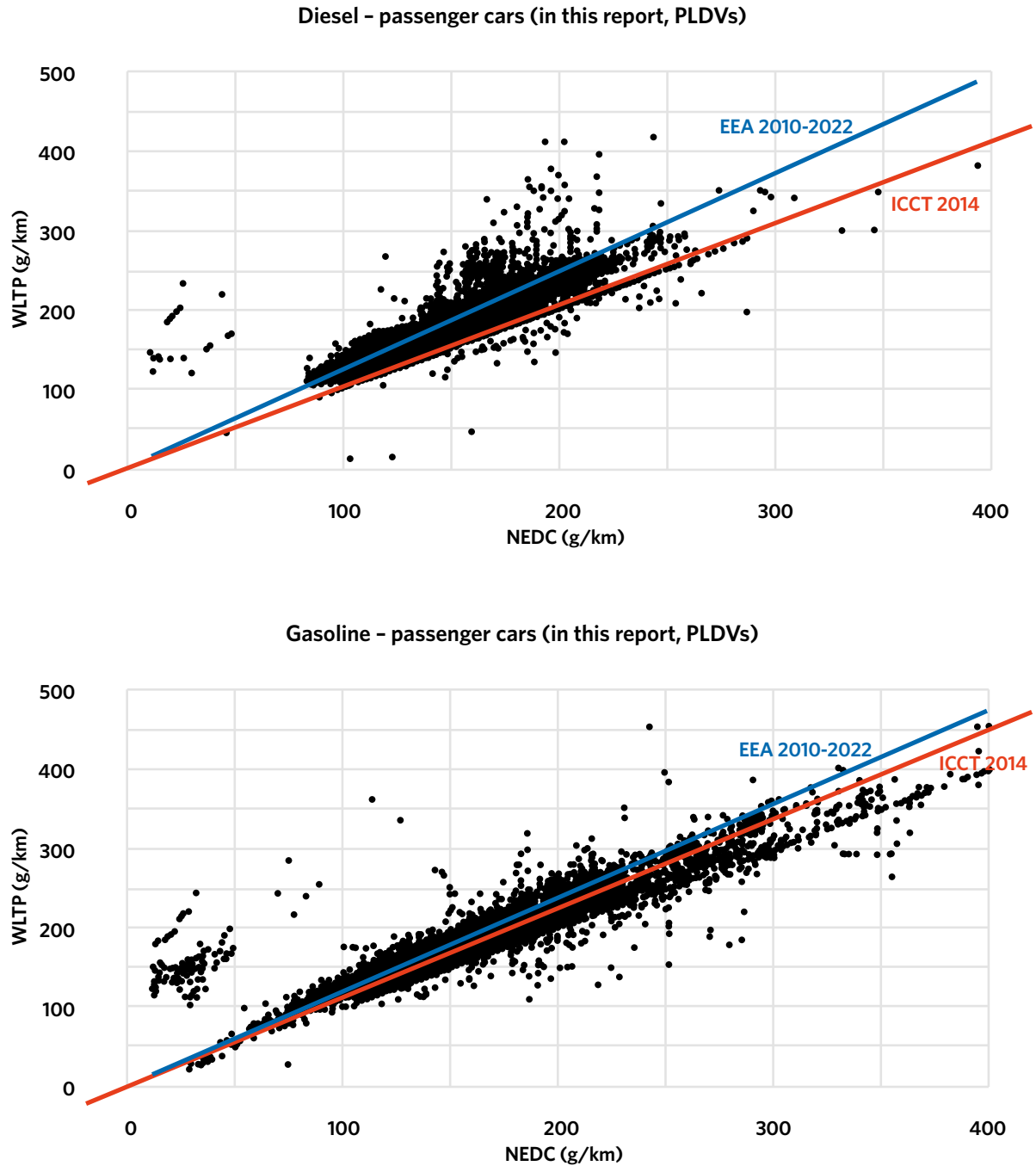
The analysis developed in Chapters 2 and 3 uses regional aggregations based on the data available at the country level, as discussed in earlier sections of this Annex. Table A6 contains information on the criteria used for the regional aggregation used for the representation of global vehicle markets in Figure 1.

TABLE A5: Regression results for gasoline and diesel conversion between NEDC and WLTC

| Powertrain | NEDC to WLTC ratio ICCT 2014 | NEDC to WLTC ratio update EEA data 2019-22 | Ratio between 2014 and updated factor |
|------------|------------------------------|--------------------------------------------|---------------------------------------|
| Gasoline   | 1.128                        | 1.185*                                     | 1.05                                  |
| Diesel     | 1.0291                       | 1.234*                                     | 1.20                                  |

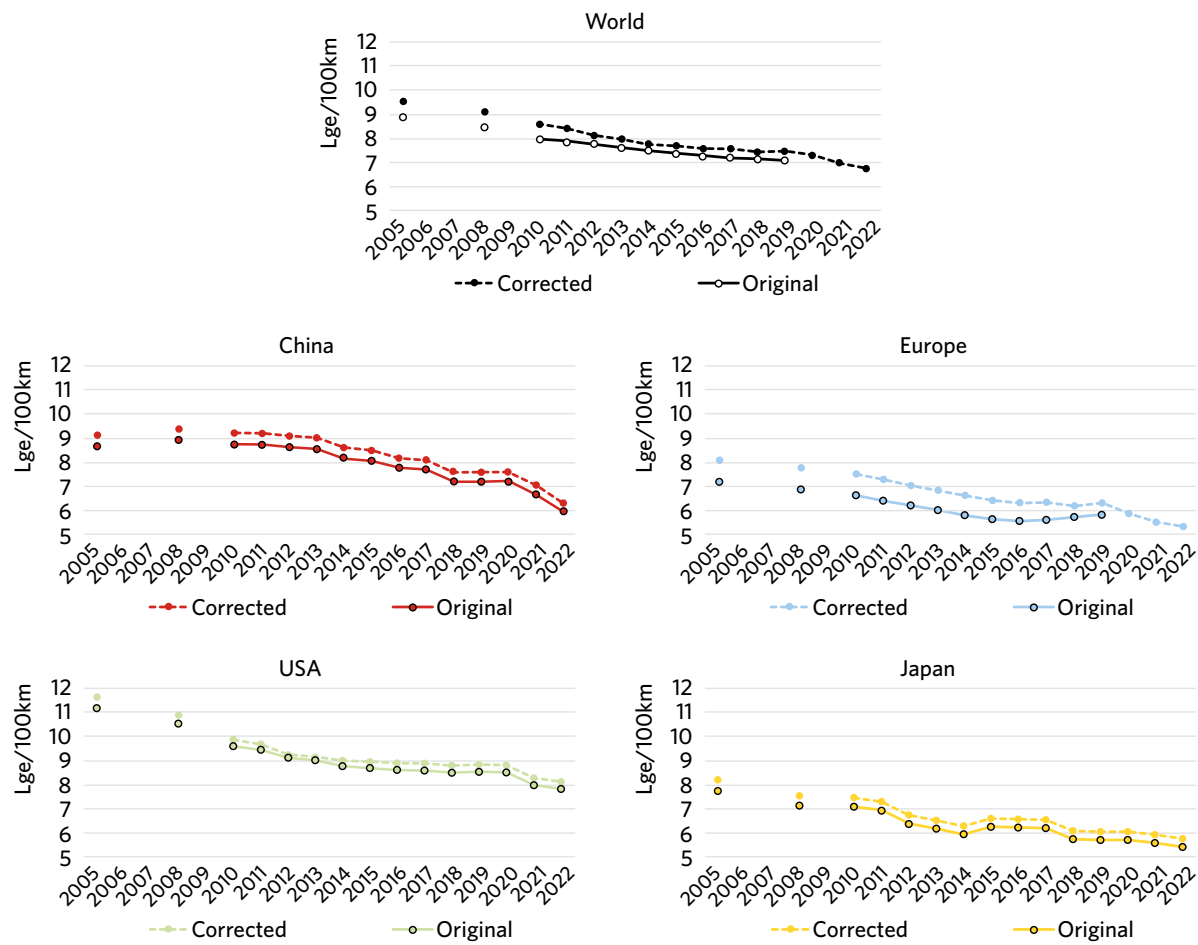
\*The values reported here are for the ratio between NEDC and WLTC emissions performance (g CO<sub>2</sub>/km) for passenger cars.

FIGURE A4: Powertrain-specific zero-intercept regressions between NEDC and WLTC, based on EEA data from 2019-2022



**Note:** For both gasoline- and diesel-fuelled LDVs, certain values for type-approval models seem to follow regression lines (in the case of gasoline, this regression line is quite close to the original ICCT 2014 zero-intercept factor). The authors suspect that this is due to the fact that some models were not assessed on the NEDC test cycle, but instead the NEDC values were derived by using the CO<sub>2</sub>MPAS modelling tool (JRC, 2020).

FIGURE A5: WLTC harmonized sales-weighted average specific energy consumption for LDVs, 2005-2022



**Note:** Dotted lines indicate the update sales-weighted average specific energy consumption (based on the updated NEDC to WLTC rebenchmarking). Solid lines show the previously estimated specific energy consumption adopted in previous GFEI benchmarking reports.

**Source:** this assessment (details in the Annex) based on EEA, 2023 and Marklines data.

Key criteria used for this categorization are summarized in the following list:

- Canada and the United States are both high income, low population density countries, with comparatively low fuel taxes (based on purchasing power parities [PPP]), with domestic auto manufacturing capacity (with legacy OEMs and established and emerging EV focused ones), not reliant on major amounts of oil imports, leading to markets with very large cars and, until recently, limited EV market penetration (often focused in specific States – such as California, and/or Provinces – such as Quebec).
- The European Union, countries in the European Economic Area, Switzerland and the United Kingdom are high income, comparably high fuel tax, often with greater population density and auto manufacturing capacity (including major exporting countries, with many legacy OEMs and few EV focused ones), and generally (with targeted exceptions) net oil importers, with interest in energy diversification. They have a mixed segmentation of the car market, leaning towards larger vehicles in recent times, sizeable EV shares globally, even if still heterogeneous.

TABLE A6: Aggregation criteria for the representation of global market developments

| Country              | Region (code name) | Region (full name)                            |
|----------------------|--------------------|-----------------------------------------------|
| Argentina            | 11_ROW             | Rest of the World                             |
| Australia            | 10_Australia       | Australia                                     |
| Belarus              | 11_ROW             | Rest of the World                             |
| Brazil               | 7_BRA_MEX_MYS      | Brazil, Malaysia, Mexico                      |
| Canada               | 1_USA_CA           | North America                                 |
| Chile                | 11_ROW             | Rest of the World                             |
| China                | 5_China            | China                                         |
| Colombia             | 11_ROW             | Rest of the World                             |
| EEA countries        | 2_Europe           | Europe                                        |
| Egypt                | 11_ROW             | Rest of the World                             |
| India                | 6_India            | India                                         |
| Indonesia            | 8_INDO_GRP         | Indonesia, South Africa, Thailand and Vietnam |
| Israel               | 9_MiddleEast       | Middle East                                   |
| Japan                | 4_Japan            | Japan                                         |
| Kazakhstan           | 11_ROW             | Rest of the World                             |
| Korea                | 3_Korea            | Korea                                         |
| Kuwait               | 9_MiddleEast       | Middle East                                   |
| Malaysia             | 7_BRA_MEX_MYS      | Brazil, Malaysia, Mexico                      |
| Mexico               | 7_BRA_MEX_MYS      | Brazil, Malaysia, Mexico                      |
| Myanmar              | 11_ROW             | Rest of the World                             |
| New Zealand          | 11_ROW             | Rest of the World                             |
| North Macedonia      | 11_ROW             | Rest of the World                             |
| Oman                 | 9_MiddleEast       | Middle East                                   |
| Pakistan             | 11_ROW             | Rest of the World                             |
| Peru                 | 11_ROW             | Rest of the World                             |
| Philippines          | 11_ROW             | Rest of the World                             |
| Puerto Rico          | 11_ROW             | Rest of the World                             |
| Russia               | 2_Europe           | Europe                                        |
| Saudi Arabia         | 9_MiddleEast       | Middle East                                   |
| Singapore            | 11_ROW             | Rest of the World                             |
| South Africa         | 8_INDO_GRP         | Indonesia, South Africa, Thailand and Vietnam |
| Switzerland          | 2_Europe           | Europe                                        |
| Taiwan               | 11_ROW             | Rest of the World                             |
| Thailand             | 8_INDO_GRP         | Indonesia, South Africa, Thailand and Vietnam |
| Turkey               | 11_ROW             | Rest of the World                             |
| United Arab Emirates | 9_MiddleEast       | Middle East                                   |
| Ukraine              | 11_ROW             | Rest of the World                             |
| United Kingdom       | 2_Europe           | Europe                                        |
| United States        | 1_USA_CA           | North America                                 |
| Uruguay              | 11_ROW             | Rest of the World                             |
| Uzbekistan           | 11_ROW             | Rest of the World                             |
| Vietnam              | 8_INDO_GRP         | Indonesia, South Africa, Thailand and Vietnam |



- Korea and Japan are both countries with high income, high density, high PPP fuel tax, domestic auto manufacturing (and export) capacity (with legacy OEMs, some of which have strong EV ambitions, especially in Korea). Both are also oil importers, with interest in energy diversification despite limited opportunities to shift towards renewables. They have a car market segmentation similar to Europe.
- China is a major economy with medium income levels, medium/high urban density (especially in the coastal area), fairly high PPP fuel tax, with domestic auto manufacturing capacity. It is also an oil importer, with strong interest in energy diversification. Its car market is diverse, including small/medium and large cars/SUVs, reflecting the combination of an income effect that keeps vehicles smaller than in high Europe, Korea and Japan, and lower fuel prices (with an upward impact on segment shifts towards SUVs). China also have large EV shares, globally.
- India as a comparatively low income (with respect to earlier cases), medium to high population density (including some very densely populated States), high PPP fuel tax, domestic auto manufacturing capacity. It is a major oil importer, with interest in energy diversification. Its vehicles are smaller than in countries outlined earlier, due to the combination of income and fuel price effects. EV shares are still limited, most likely due to income- and affordability-related constraints and presence of legacy OEMs.
- Brazil, Malaysia and Mexico have comparatively low incomes with respect to Canada, Europe and the United States, rather low population density (despite major densely populated megacities) and medium to low PPP fuel taxes. They are auto

manufacturers, and self-sufficient, if not exporters, of oil. Their vehicle segmentation is mixed, as a result of an income effect favouring smaller cars and fuel prices allowing for larger models to be more appealing. EV shares are limited, for reasons similar to those identified for India, with the additional reason of self-sufficiency for oil supplies.

- Indonesia, Thailand South Africa and Vietnam have comparatively low incomes with respect to Canada, Europe and the United States, low population density (except for major urban agglomerations), medium to low PPP fuel taxes. They have domestic car manufacturing capacity, they are net oil importers, with interest in oil diversification. Their automotive market segmentation is not strongly focused on large SUVs, due to the income effect, even if this is mitigated by medium to low fuel taxation. EV shares are limited, for reasons similar to those identified for India.
- The Middle East includes many countries with medium income, heterogeneous (and often low, outside of cities) density, low PPP fuel tax. The region is not an auto manufacturer, it is a strong oil exporter, with limited interest in oil diversification, except for climate-related risks. Vehicles in the Middle East tend to be large, in line with low fuel taxation, similar to North America. EV market penetration is small, mainly paired with early moves on economic diversification.
- The rest of the World includes mainly small and rather low-income countries, with heterogeneous population densities, a tendency to apply low to medium PPP fuel tax and no major auto manufacturing capacity (Turkey being a key exception to many of these criteria). Most countries are net oil importers. Vehicle segmentation is mixed and EV shares tend to be low.

# ABBREVIATIONS AND ACRONYMS

|                 |                                                                                                                         |
|-----------------|-------------------------------------------------------------------------------------------------------------------------|
| BEV             | battery electric vehicle                                                                                                |
| CAFE            | corporate average fuel economy                                                                                          |
| CNG             | compressed natural gas                                                                                                  |
| CO <sub>2</sub> | carbon dioxide                                                                                                          |
| EPA             | Environmental Protection Agency                                                                                         |
| FCEV            | fuel cell electric vehicle                                                                                              |
| GFEI            | Global Fuel Economy Initiative                                                                                          |
| GREET           | Greenhouse Gases, Regulated Emissions, and Energy Use in Technologies                                                   |
| HEV             | hybrid electric vehicle                                                                                                 |
| ICE             | internal combustion engine                                                                                              |
| IEA             | International Energy Agency                                                                                             |
| LCV             | light commercial vehicle                                                                                                |
| LNG             | liquefied natural gas                                                                                                   |
| LPG             | liquefied petroleum gas                                                                                                 |
| NEDC            | New European Driving Cycle                                                                                              |
| OICA            | International Organisation of Motor Vehicle Manufacturers (Organisation Internationale des Constructeurs d'Automobiles) |
| PHEV            | plug-in electric vehicle                                                                                                |
| SEC             | specific energy consumption                                                                                             |
| WLTC            | Worldwide Harmonized Light-Duty Vehicle Test Cycle                                                                      |

## UNITS OF MEASURE

|                       |                                     |
|-----------------------|-------------------------------------|
| cm <sup>3</sup>       | cubic centimetre                    |
| g CO <sub>2</sub> -eq | gramme of carbon dioxide equivalent |
| Gt                    | gigatonne                           |
| kg                    | kilogramme                          |
| km                    | kilometre                           |
| kW                    | kilowatt                            |
| kWh                   | kilowatt-hour                       |
| L                     | litre                               |
| Lge                   | litre of gasoline equivalent        |
| m <sup>2</sup>        | square metre                        |
| MJ                    | megajoule                           |



# REFERENCES

ACEA (European Automobile Manufacturers' Association) (2022). ACEA Tax Guide 2022. <https://www.acea.auto/publication/acea-tax-guide-2022/>

Adler, M.W., Peer, S. Sinozic, T. (2019), Autonomous, connected, electric shared vehicles (ACES) and public finance: An explorative analysis. Transportation Research Interdisciplinary Perspectives. <https://doi.org/10.1016/j.trip.2019.100038>

Adolf, Simon (2022, 8 July). Comment l'Ami permet à Citroën d'attirer une nouvelle clientèle. <https://www.lesechos.fr/thema/articles/comment-lami-permet-a-citroen-dattirer-une-nouvelle-clientele-1775422>

ARB (Air Resources Board) (n.d.), Low-Emission Vehicle (LEV III) Program, <https://ww2.arb.ca.gov/our-work/programs/advanced-clean-cars-program/lev-program/low-emission-vehicle-lev-iii-program>

Aizhu, Chen, Blenkinsop, Philip (2023, 4 October). China rebukes EU after formal launch of EV subsidy probe. <https://www.reuters.com/business/autos-transportation/china-rebukes-eus-rushed-request-consultations-over-ev-subsidy-probe-2023-10-04/>

Australian Government (n.d.), Vehicle emission standards, <https://www.infrastructure.gov.au/infrastructure-transport-vehicles/vehicles/vehicle-safety-environment/emission-standards>

Autovista24 (2023, 16 August), What can be expected from Europe's automotive markets in the second half of 2023?, <https://autovista24.autovistagroup.com/news/what-can-be-expected-europes-automotive-markets-second-half-2023/>

Bashar Anwar, Muhammad, et al., (2022). Assessing the value of electric vehicle managed charging: a review of methodologies and results. Energy and Environmental Science. Issue 2, 2022. <https://pubs.rsc.org/en/content/articlelanding/2022/ee/d1ee02206g>

Battery Design (2022), Cell Gravimetric Energy Density, <https://www.batterydesign.net/cell-gravimetric-energy-density/>

Bieker, Georg (2021, July 20), A global comparison of the life-cycle greenhouse gas emissions of combustion engine and electric passenger cars, International Council for Clean Transportation (ICCT), <https://theicct.org/publication/a-global-comparison-of-the-life-cycle-greenhouse-gas-emissions-of-combustion-engine-and-electric-passenger-cars/>

Brinley, Stephanie (2023, 12 July), The semiconductor shortage is – mostly – over for the auto industry, S&P Global, <https://www.spglobal.com/mobility/en/research-analysis/the-semiconductor-shortage-is-mostly-over-for-the-auto-industry.html>

British Parking Association (2022, 24 October). New car park design guidance. <https://www.britishparking-media.co.uk/news/car-park-design-guidance>

Bureau of Labor Statistics (2023, February 14), Measuring Price Change in the CPI: New vehicles, <https://www.bls.gov/cpi/factsheets/new-vehicles.htm>

Burkacky, Ondrej, Lingemann, Stephanie and Pototzky, Klaus (2021, May 27), Coping with the auto-semiconductor shortage: Strategies for success, McKinsey & Co., <https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/coping-with-the-auto-semiconductor-shortage-strategies-for-success>

Burkacky, Ondrej, Deichmann, Johannes, Pfingstag, Philipp and Werra, Julia (2022, 10 June), Semiconductor shortage: How the automotive industry can succeed, McKinsey & Co., <https://www.mckinsey.com/industries/semiconductors/our-insights/semiconductor-shortage-how-the-automotive-industry-can-succeed>

California Air Resources Board (California ARB) (n.d.). Clean Vehicle Rebate Program (CVRP). <https://ww2.arb.ca.gov/sites/default/files/movingca/cvrp.html>

California Sales Tax Handbook (n.d.). How are vehicle sales taxed in California? <https://www.salestaxhandbook.com/california/sales-tax-vehicles>

Carpenter, Griffin, Antich, Arnau Oliver (2022, October). The good tax guide; A comparison of car taxation in Europe. <https://www.transportenvironment.org/wp-content/uploads/2022/10/The-good-tax-guide.pdf>

Cazzola, Pierpaolo and Santos Alfageme, Maria (2023), Facilitating a Transition to Zero-emission Vehicles in the Global South, UC Davis Institute of Transportation Studies, <https://doi.org/10.7922/G2PKODGM>

China Association of Automobile Manufacturers (CAAM) (2023). Automotive Data Portal, <http://en.caam.org.cn/Index/lists/catid/68.html>

Craglia, Matteo and Cullen, Jonathan (2019, November), Do technical improvements lead to real efficiency gains? Disaggregating changes in transport energy intensity, Energy Policy, <https://doi.org/10.1016/j.enpol.2019.110991>

CSIS (Center for Strategic and International Studies) (2022). An Electric Debate: Local Content Requirements and Trade Considerations. <https://www.csis.org/analysis/electric-debate-local-content-requirements-and-trade-considerations>

Cuenot, François and Fulton, Lew, (2011), International comparison of light-duty vehicle fuel economy and related characteristics, Global Fuel Economy Initiative and International Energy Agency, <https://www.globalfueleconomy.org/media/44069/wp5-iea-fuel-economy-report.pdf>

Cuenot, François and Körner, Alexander (2013), International comparison of light-duty vehicle fuel economy and related characteristics, Global Fuel Economy Initiative and International Energy Agency, <https://www.globalfueleconomy.org/media/44082/wp8-international-comparison.pdf>

Cuenot, François (2017), Wider, taller, heavier: evolution of light duty vehicle size over generations, Global Fuel Economy Initiative, <https://www.globalfueleconomy.org/media/460880/gfei-wp17-ldv-global-vehicle-size-analysis.pdf>

Daina, Nicolò (2023, 10 October). Focus on Fleets to Manage Critical Minerals Demand. <https://www.energypolicy.columbia.edu/focus-on-fleets-to-manage-critical-minerals-demand/>

Dornoff, Jan, Tietge, Uwe and Mock, Peter (2020), On the way to "real world" CO<sub>2</sub> values: the European passenger car market in its first year after introducing the WLTP, International Council for Clean Transportation, <https://theicct.org/publication/on-the-way-to-real-world-co2-values-the-european-passenger-car-market-in-its-first-year-after-introducing-the-wltp/>

Dornoff, Jan (2023), CO<sub>2</sub> emission standards for new passenger cars in the European Union, International Council for Clean Transportation, <https://theicct.org/publication/eu-co2-standards-cars-vans-may23/>

Dow, Cat (2023, 12 July). From 2024, SUV drivers will be charged more for parking in Paris. <https://www.topgear.com/car-news/suvs/2024-suv-drivers-will-be-charged-more-parking-paris>

Edwards, Mickey and Leonard, Daniel (2022, September) Effects of large vehicles on pedestrian and pedalcyclist injury severity. Journal of Safety Research. <https://doi.org/10.1016/j.jsr.2022.06.005>

EEA (European Environment Agency) (2023a), Monitoring of CO<sub>2</sub> emissions from passenger cars Regulation (EU) 2019/631, <https://www.eea.europa.eu/en/datahub/datahubitem-view/fa8b1229-3db6-495d-b18e-9c9b3267c02b>

EEA (2023b), Monitoring of CO<sub>2</sub> emissions from vans - Regulation (EU) No 2019/631, <https://www.eea.europa.eu/en/datahub/datahubitem-view/9636827c-bd0c-40f5-814e-c4065c11c9a0>

Electrive (2023, 20 September). France: New environmental bonus could push out imported EVs. <https://www.electrive.com/2023/09/20/france-new-environmental-bonus-could-push-out-imported-evs/>

EnergNETMob (2021, 10 September). Interview with Mr. Enton Punavija, Director of Transport in Tirana Municipality on the development of electric transport in Tirana. <https://www.enernetmob.eu/announcements/interview-with-mr-enton-punavija-director-of-transport-in-tirana-municipality-on-the-development-of-electric-transport-in-tirana>

EPA (Environmental Protection Agency) (2023), Control of Air Pollution From New Motor Vehicles: Tier 2 Motor Vehicle Emissions Standards and Gasoline Sulfur Control Requirements, <https://www.govinfo.gov/content/pkg/FR-2000-02-10/pdf/00-19.pdf>

Euro NCAP (The European New Car Assessment Programme) (2016). Vision 2030: A Safer Future for Mobility. <https://cdn.euroncap.com/media/74468/euro-ncap-roadmap-vision-2030.pdf>

European Commission (n.d.), CO<sub>2</sub> emission performance standards for cars and vans, [https://climate.ec.europa.eu/eu-action/transport/road-transport-reducing-co2-emissions-vehicles/co2-emission-performance-standards-cars-and-vans\\_en](https://climate.ec.europa.eu/eu-action/transport/road-transport-reducing-co2-emissions-vehicles/co2-emission-performance-standards-cars-and-vans_en)



European Commission (2019). Proposal for a Regulation of the European Parliament and of the Council on Methane Emissions Reduction in the Energy Sector and Amending Regulation (EU) 2019/942. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A805%3AFIN&qid=1639665806476>

European Commission (2021). Proposal for a Directive of the European Parliament and of the Council on the Energy Performance of Buildings. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0802&qid=1641802763889>

European Commission (2023a, 11 July). Regulation of the European Parliament and of the Council on the Accounting of Greenhouse Gas Emissions of Transport Services. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023PC0441>

European Commission (2023b, 12 September). Trade Barriers. [https://trade.ec.europa.eu/access-to-markets/en/barriers/details?barrier\\_id=17542&sps=false](https://trade.ec.europa.eu/access-to-markets/en/barriers/details?barrier_id=17542&sps=false)

European Commission (2023c). Use of NextGenerationEU proceeds. [https://commission.europa.eu/strategy-and-policy/eu-budget/eu-borrower-investor-relations/nextgenerationeu\\_en](https://commission.europa.eu/strategy-and-policy/eu-budget/eu-borrower-investor-relations/nextgenerationeu_en)

European Commission (2023d, 14 March). Commission proposes reform of the EU electricity market design to boost renewables, better protect consumers and enhance industrial competitiveness. [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_23\\_1591](https://ec.europa.eu/commission/presscorner/detail/en/IP_23_1591)

European Council (2022, 19 December). Member States agree on new rules to slash methane emissions. <https://www.consilium.europa.eu/en/press/press-releases/2022/12/19/member-states-agree-on-new-rules-to-slash-methane-emissions/>

European Council (2023, 18 October). 'Fit for 55': Council and Parliament reach provisional deal on EU emissions trading system and the Social Climate Fund. <https://www.consilium.europa.eu/en/press/press-releases/2022/12/18/fit-for-55-council-and-parliament-reach-provisional-deal-on-eu-emissions-trading-system-and-the-social-climate-fund/>

European Court of Auditors (2019, February). The EU's response to the "dieselgate" scandal Briefing Paper, [https://www.eca.europa.eu/lists/ecadocuments/brp\\_vehicle\\_emissions/brp\\_vehicle\\_emissions\\_en.pdf](https://www.eca.europa.eu/lists/ecadocuments/brp_vehicle_emissions/brp_vehicle_emissions_en.pdf)

European Parliament (2022, 31 May). Review of the EU ETS: 'Fit for 55' package. [https://www.europarl.europa.eu/thinktank/en/document/EPRS\\_BRI\(2022\)698890](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)698890)

European Parliament (2023a, 14 March). Energy performance of buildings (recast) Amendments adopted by the European Parliament on 14 March 2023 on the proposal for a directive of the European Parliament and of the Council on the energy performance of buildings (recast) (COM(2021)0802 – C9-0469/2021 – 2021/0426(COD)). [https://www.europarl.europa.eu/doceo/document/TA-9-2023-0068\\_EN.pdf](https://www.europarl.europa.eu/doceo/document/TA-9-2023-0068_EN.pdf)

European Parliament (2023b, 14 March). Fit for 55: MEPs boost methane emission reductions from the energy sector. <https://www.europarl.europa.eu/news/en/press-room/20230505IPR84920/fit-for-55-meps-boost-methane-emission-reductions-from-the-energy-sector>

European Union (2021, 30 June). Regulation (EU) 2021/1119 of the European Parliament and of the Council of 30 June 2021 establishing the framework for achieving climate neutrality and amending Regulations (EC) No 401/2009 and (EU) 2018/1999 ('European Climate Law'). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021R1119>

European Union (2023a, 13 July). Proposal for a Regulation on circularity requirements for vehicle design and on management of end-of-life vehicles. [https://environment.ec.europa.eu/publications/proposal-regulation-circularity-requirements-vehicle-design-and-management-end-life-vehicles\\_en](https://environment.ec.europa.eu/publications/proposal-regulation-circularity-requirements-vehicle-design-and-management-end-life-vehicles_en)

European Union (2023b, 12 July). Regulation (EU) 2023/1542 of the European Parliament and of the Council of 12 July 2023 concerning batteries and waste batteries, amending Directive 2008/98/EC and Regulation (EU) 2019/1020 and repealing Directive 2006/66/EC (Text with EEA relevance) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1542>

European Union (2023c, 19 April). Regulation (EU) 2023/851 of the European Parliament and of the Council of 19 April 2023 amending Regulation (EU) 2019/631 as regards strengthening the CO<sub>2</sub> emission performance standards for new passenger cars and new light commercial vehicles in line with the Union's increased climate ambition (Text with EEA relevance). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R0851>

European Union (2023d, 13 September). 2023 State of the Union Address by President von der Leyen. [https://ec.europa.eu/commission/presscorner/detail/en/speech\\_23\\_4426](https://ec.europa.eu/commission/presscorner/detail/en/speech_23_4426)

European Union (2023e, 10 May). Directive of the European Parliament and of the Council Amending Directive 2003/87/EC Establishing a System For Greenhouse Gas Emission Allowance Trading Within the Union and Decision (EU) 2015/1814 Concerning the Establishment and Operation Of a Market Stability Reserve For The Union Greenhouse Gas Emission Trading System. [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CONSIL%3APE\\_9\\_2023\\_REV\\_1&qid=1694541583332](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CONSIL%3APE_9_2023_REV_1&qid=1694541583332)

European Union (2023f, 10 May). Official Journal of the European Union. L 130. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2023:130:FULL>

European Union (2023g, 13 July). Regulation of the European Parliament and of the Council on the Deployment of Alternative Fuels Infrastructure, and Repealing Directive 2014/94/EU. [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CONSIL%3APE\\_25\\_2023\\_INIT&qid=1694540889430](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CONSIL%3APE_25_2023_INIT&qid=1694540889430)

EV Volumes (2023), EV Data Center, [www.ev-volumes.com/datacenter/](http://www.ev-volumes.com/datacenter/)

Feiqi, Liu, Fuquan, Zhao, Zongwei, Liu and Han, Hao (2020, 22 January), The Impact of Purchase Restriction Policy on Car Ownership in China's Four Major Cities, Journal of Advanced Transportation, <https://doi.org/10.1155/2020/7454307>

Frith, James, Lacey, Matthew and Ulissi, Uledrico (2023, 26 January), A non-academic perspective on the future of lithium-based batteries. Nature Communications. <https://doi.org/10.1038/s41467-023-35933-2>

Fuel Economy Guide (2023). United States Department of Energy and Environmental Protection Agency, www.fueleconomy.gov, the official U.S. government source for fuel economy information, <https://www.fueleconomy.gov/feg/download.shtml>

GfK (2023, 16 March), 60% of consumers planning to get a new car say affordability is impacting their purchase decision, <https://www.gfk.com/press/automotive-affordability-financing-trends>

Global NCAP (Global New Car Assessment Programme) (2018, 17 October). Crashing Cars To Save Lives. <https://www.globalncap.org/blog/crashing-cars-to-save-lives>

Global Environment Facility (GEF) (2021). Transition Towards Electric Mobility in Armenia. <https://www.thegef.org/projects-operations/projects/10280>

Global Trade Alert (2022, 1 March). Indonesia: Introduced Import duties exemption on electric vehicles and their components. <https://www.globaltradealert.org/intervention/101766/import-tariff/indonesia-introduced-import-duties-exemption-on-electric-vehicles-and-their-components>

Government of California (2018, 13 September). SB-1014 California Clean Miles Standard and Incentive Program: zero-emission vehicles. [https://leginfo.ca.gov/faces/billTextClient.xhtml?bill\\_id=201720180SB1014](https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1014)

Government of France (2021, March). Le microcrédit véhicules propres. [https://www.ecologie.gouv.fr/sites/default/files/21045\\_2p\\_microcredit-vehicules-propres\\_grandpublic.pdf](https://www.ecologie.gouv.fr/sites/default/files/21045_2p_microcredit-vehicules-propres_grandpublic.pdf)

Government of France (2023, 1 January). Taxe 2023 sur la masse en ordre de marche (malus au poids). <https://www.service-public.fr/particuliers/vosdroits/F35950#:~:text=V%C3%A9hicule%20immatricul%C3%A9%20%C3%A0%20l'%C3%A9tranger,partir%20de%201%20800%20kg.&text=2000%20%E2%82%AC-,La%20taxe%20sur%20la%20masse%20en%20ordre%20de%20marche%20est,et%20le%20malus%20au%20poids.>

Harding, Michelle (2014, 11 July). Personal Tax Treatment of Company Cars and Commuting Expenses Estimating the Fiscal and Environmental Costs. <https://doi.org/10.1787/5jz14cgs7vl-en>

Hasselwander, Samuel, Meyer, Markus and Österle, Ines (2023, 15 July), Techno-Economic Analysis of Different Battery Cell Chemistries for the Passenger Vehicle Market, <https://doi.org/10.3390/batteries9070379>

He, Hui, Jin, Lingzhi, Cui, Hongyang, Zhou, Huan (2018, October 18), Assessment of electric car promotion policies in Chinese cities, International Council for Clean Transportation, <https://theicct.org/publication/assessment-of-electric-car-promotion-policies-in-chinese-cities/>

Hersh, Adam (2023, 12 September), UAW-automakers negotiations pit falling wages against skyrocketing CEO pay. Economic Policy Institute. <https://www.epi.org/blog/uaw-automakers-negotiations/>

Hexagon (n.d.), Advanced Controls & Systems Simulation with Easy5, <https://simulatemore.mscsoftware.com/advanced-controls-systems-simulation-with-easy5/>

Highway Loss Data Institute (2018), Effect of hybrid vehicles on pedestrian-related bodily injury liability claim frequencies, [https://www.iihs.org/media/0a02ebc5-5b17-46a2-971b-Obd1e5706156/yK6Yzw/HLDI%20Research/Bulletins/hldi\\_bulletin\\_35-11.pdf](https://www.iihs.org/media/0a02ebc5-5b17-46a2-971b-Obd1e5706156/yK6Yzw/HLDI%20Research/Bulletins/hldi_bulletin_35-11.pdf)

Holland, Maximilian (2023, 4 January). Norway's EV Sales Explode Ahead Of Policy Changes. [https://cleantechnica.com/2023/01/04/norways-ev-sales-explode-ahead-of-policy-changes/#:~:text=Pull%20Forward%20Ahead%20Of%20Tax%20Changes&text=The%20first%20is%20a%20weight,27%2C500%20NOK%20\(%E2%82%AC2%2C590\).](https://cleantechnica.com/2023/01/04/norways-ev-sales-explode-ahead-of-policy-changes/#:~:text=Pull%20Forward%20Ahead%20Of%20Tax%20Changes&text=The%20first%20is%20a%20weight,27%2C500%20NOK%20(%E2%82%AC2%2C590).)

ICCT (International Council on Clean Transportation) (2013), Mexico light-duty vehicle CO<sub>2</sub> and fuel economy standards, [https://theicct.org/sites/default/files/publications/ICCTupdate\\_Mexico\\_LDVstandards\\_july2013.pdf](https://theicct.org/sites/default/files/publications/ICCTupdate_Mexico_LDVstandards_july2013.pdf)

ICCT (2019), Japan 2023 fuel economy standards, [https://theicct.org/sites/default/files/publications/Japan\\_2030\\_fuel\\_standard\\_update\\_20191007.pdf](https://theicct.org/sites/default/files/publications/Japan_2030_fuel_standard_update_20191007.pdf)

IPCC (Intergovernmental Panel on Climate Change) (2006), Chapter 3: Mobile Combustion. 2006 IPCC Guidelines for National Greenhouse Gas Inventories, [https://www.ipcc-nggip.iges.or.jp/public/2006gl/pdf/2\\_Volume2/V2\\_3\\_Ch3\\_Mobile\\_Combustion.pdf](https://www.ipcc-nggip.iges.or.jp/public/2006gl/pdf/2_Volume2/V2_3_Ch3_Mobile_Combustion.pdf)

IPCC (2022), Climate Change 2022: Mitigation of Climate Change, <https://www.ipcc.ch/report/sixth-assessment-report-working-group-3/>

IRS (Internal Revenue Service) (2023). Credits for New Clean Vehicles Purchased in 2023 or After. <https://www.irs.gov/credits-deductions/credits-for-new-clean-vehicles-purchased-in-2023-or-after#:~:text=You%20may%20qualify%20for%20a%20credit%20up%20to%20%247%2C500%20under,purchased%20from%202023%20to%202032.>

IEA (International Energy Agency) (2017, June), Global EV outlook 2017, <https://www.iea.org/reports/global-ev-outlook-2017>

IEA (2018, May), Global EV outlook 2018, <https://www.iea.org/reports/global-ev-outlook-2018>

IEA (2019a, March), Fuel Economy in Major Car Markets: Technology and Policy Drivers, 2005-2017, Global Fuel Economy Initiative, International Energy Agency, International Council on Clean Transportation, <https://www.iea.org/reports/fuel-economy-in-major-car-markets>

IEA (2019b, January), The Future of Rail, <https://www.iea.org/reports/the-future-of-rail>

IEA (2020, June), Global EV outlook 2020, <https://www.iea.org/reports/global-ev-outlook-2020>

IEA (2021a, November), Global Fuel Economy Initiative 2021 - Vehicle fuel economy in major markets, 2005-2019, Global Fuel Economy Initiative and International Energy Agency, <https://www.iea.org/reports/global-fuel-economy-initiative-2021>

IEA (2021b, April), Global EV outlook 2021, <https://www.iea.org/reports/global-ev-outlook-2021>

IEA (2022, May), Global EV outlook 2022, <https://www.iea.org/reports/global-ev-outlook-2022>

IEA (2023a), Energy Prices, <https://www.iea.org/data-and-statistics/data-product/energy-prices>

IEA (2023b, April), Global EV outlook 2023, <https://www.iea.org/reports/global-ev-outlook-2023>

IEA (2023c, January), Energy Technology Perspectives 2023, <https://www.iea.org/reports/energy-technology-perspectives-2023>

ILO (International Labour Organization) (2021, February), The future of work in the automotive industry: The need to invest in people's capabilities and decent and sustainable work. TMFWAI/2021. [https://www.ilo.org/wcmsp5/groups/public/---ed\\_dialogue/---sector/documents/meetingdocument/wcms\\_741659.pdf](https://www.ilo.org/wcmsp5/groups/public/---ed_dialogue/---sector/documents/meetingdocument/wcms_741659.pdf)

ITF (International Transport Forum) (2020, 17 September). Good to Go? Assessing the Environmental Performance of New Mobility. [https://www.oecd-ilibrary.org/transport/good-to-go-assessing-the-environmental-performance-of-new-mobility\\_f5cd236b-en](https://www.oecd-ilibrary.org/transport/good-to-go-assessing-the-environmental-performance-of-new-mobility_f5cd236b-en)

ITF (2020a, 10 December), How Urban Delivery Vehicles can Boost Electric Mobility, <https://doi.org/10.1787/eea08a2a-en>

ITF (2020b, 15 September), Regulations and Standards for Clean Trucks and Buses, <https://doi.org/10.1787/ed7ef18b-en>

ITF (2021a). Reversing Car Dependency; Summary and Conclusions. <https://www.itf-oecd.org/sites/default/files/docs/reversing-car-dependency.pdf>

ITF (2021b). Cleaner Vehicles Achieving a Resilient Technology Transition. <https://www.itf-oecd.org/sites/default/files/docs/cleaner-vehicles-technology-transition.pdf>

ITF (2022). Implementing the ASEAN Fuel Economy Roadmap. [https://www.itf-oecd.org/sites/default/files/docs/implementing-asean-fuel-economy-roadmap\\_1.pdf](https://www.itf-oecd.org/sites/default/files/docs/implementing-asean-fuel-economy-roadmap_1.pdf)

ITF (2023, 27 September). Shifting the Focus: Smaller Electric Vehicles for Sustainable Cities. <https://www.itf-oecd.org/shifting-focus-smaller-electric-vehicles>

Jin, Lingzhi, Chu, Yidan and Wang, Xiyuan (2023, February 27), Accelerating new energy vehicle uptake in Chinese cities: assessment of policies for private passenger cars in leading city markets, International Council for Clean Transportation (ICCT), <https://theicct.org/publication/pv-chinese-cities-nev-policies-feb23/>

JRC (Joint Research Centre) (2017). From NEDC to WLTP: effect on the type-approval CO<sub>2</sub> emissions of light-duty vehicles. <https://publications.jrc.ec.europa.eu/repository/handle/JRC107662>

JP Morgan (2023, 18 April), Supply chain issues and autos: When will the chip shortage end?, <https://www.jpmorgan.com/insights/current-events/supply-chain/supply-chain-chip-shortage>

JRC (Joint Research Center), CO<sub>2</sub> Model for Passenger and commercial vehicles Simulation, Modelling Inventory and Knowledge Management System of the European Commission (MIDAS), <https://web.jrc.ec.europa.eu/policy-model-inventory/explore/models/model-co2mpas/>

Khan, Tanzila, Yang, Zifei, Kohli, Sumati and Miller, Josh (2022, 9 February), A critical review of ZEV deployment in emerging markets, <https://theicct.org/publication/zev-market-review-global-feb22/>

Komnos, Dimitrios, Tsiakmakis, Stefanos, Pavlovic, Jelica, Ntziachristos, Leonidas and Fontaras, Giorgios (2022, October), Analysing the real-world fuel and energy consumption of conventional and electric cars in Europe, Energy Conversion and Management, <https://doi.org/10.1016/j.enconman.2022.116161>

Krajinska, Anna (2023), Small and profitable: why affordable electric cars in 2025 are feasible, Transport & Environment, [https://www.transportenvironment.org/wp-content/uploads/2023/09/2023\\_09\\_TE\\_report\\_Why\\_affordable\\_electric\\_cars\\_in\\_2025\\_are\\_feasible.pdf](https://www.transportenvironment.org/wp-content/uploads/2023/09/2023_09_TE_report_Why_affordable_electric_cars_in_2025_are_feasible.pdf)

Krisher, Tom (2022, 16 April), Modest-income buyers being priced out of new-vehicle market, <https://fortune.com/2022/04/16/modest-income-buyers-priced-out-new-vehicle-market/>

Kühlwein, Jörg, German, John and Bandivadekar, Anup (2014, December 3), Development of test cycle conversion factors among worldwide light-duty vehicle CO<sub>2</sub> emission standards, International Council for Clean Transportation (ICCT), <https://theicct.org/publication/development-of-test-cycle-conversion-factors-among-worldwide-light-duty-vehicle-co2-emission-standards/>

Leplâtre, Simon (2023, 18 April), China leads the charge in electric vehicles, Le Monde, [https://www.lemonde.fr/en/economy/article/2023/04/18/china-leads-the-charge-in-electric-vehicles\\_6023288\\_19.html](https://www.lemonde.fr/en/economy/article/2023/04/18/china-leads-the-charge-in-electric-vehicles_6023288_19.html)

Lipsy, Phillip Y., Schipper, Lee. (2013). Energy efficiency in the Japanese transport sector. [http://www.lipsy.org/Japan\\_Transport\\_EnergyPolicy.pdf](http://www.lipsy.org/Japan_Transport_EnergyPolicy.pdf)

Liu, Antung, Dua, Rubal, Hu, Wei-min, and Lin Ku, Arthur (2022, October), Choosing to diet: The impact and cost-effectiveness of China's vehicle ownership restrictions, Transportation Research Part D: Transport and Environment, <https://doi.org/10.1016/j.trd.2022.103456>

Mayor of London (2019, 17 June). Mayor sets out plans for London's electric vehicle future. <https://www.london.gov.uk/press-releases/mayoral/mayor-sets-out-londons-electric-vehicle-future>

Manheim (2023), Used Vehicle Value Index, <https://site.manheim.com/en/services/consulting/used-vehicle-value-index.html>

Meilhan, Nicolas. (2019, June). Comment faire enfin baisser les émissions de CO<sub>2</sub> des voitures. <https://www.actu-environnement.com/media/pdf/news-33784-etude-emission-voitures-france-strategie-juin2019.pdf>

Meszler, Dan, German, John, Mock, Peter, Bandivadekar, Anup (2013, 4 February), Initial processing of Ricardo vehicle simulation modeling CO<sub>2</sub> data, International Council for Clean Transportation (ICCT), <https://theicct.org/publication/initial-processing-of-ricardo-vehicle-simulation-modeling-co2-data/>

MLIT (Ministry of Land, Infrastructure, Transport and Tourism) (2020, March). Car fuel efficiency list (March 2020). [https://www.mlit.go.jp/jidosha/jidosha\\_fr10\\_000051.html](https://www.mlit.go.jp/jidosha/jidosha_fr10_000051.html)

MIIT (Ministry of Industry and Information Technology, 2023). China Automotive Fuel Consumption Database. <https://yhgscx.miit.gov.cn/fuel-consumption-web/mainPage>

Monfort, Samuel and Nolan, Joseph (2018, 18 November), Trends in aggressivity and driver risk for cars, SUVs, and pickups: Vehicle incompatibility from 1989 to 2016. Traffic Injury Prevention. <https://doi.org/10.1080/15389588.2019.1632442>

Morfeldt, Johannes, Johansson, Daniel J.A. (2022, 27 October). Impacts of shared mobility on vehicle lifetimes and on the carbon footprint of electric vehicles. Nature Communications. <https://www.nature.com/articles/s41467-022-33666-2>



Muir, Jamie (2023, 8 April), Our analysis of used car prices, Auto Trader, <https://www.autotraderinsight-blog.co.uk/auto-trader-insight-blog/used-car-prices-analysis>

NCAP (New Car Assessment Programme) (2016). Quadricycle Safety – How do L7s fare in standard crash tests? Presented at the WP29 170th session. <https://unece.org/DAM/trans/doc/2016/wp29/WP29-170-38e.pdf>

NEA Singapore (National Environment Agency). (2022, 30 June). Enhanced Vehicular Emissions Scheme To Be Extended With Tightened Pollutant Thresholds. <https://www.nea.gov.sg/media/news/news/index/enhanced-vehicular-emissions-scheme-to-be-extended-with-tightened-pollutant-thresholds>

New Zealand Transport Agency (2023). Clean Car Discount overview. <https://www.nzta.govt.nz/vehicles/clean-car-programme/clean-car-discount/overview/>

NHTSA (National Highway Traffic Safety Administration) (2022), Corporate Average Fuel Economy Standards for Model Years 2024-2026 Passenger Cars and Light Trucks, [https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-04/Final-Rule-Preamble\\_CAFE-MY-2024-2026.pdf](https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-04/Final-Rule-Preamble_CAFE-MY-2024-2026.pdf)

Nuria Tapia-Ruiz et al., (2021), 2021 roadmap for sodium-ion batteries, Journal of Physics: Energy, <https://doi.org/10.1088/2515-7655/ac01ef>

Nuytens, Nina and Ben Messaoud Younes (2023, 8 August), Impact des caractéristiques des véhicules sur la gravité des lésions des occupants de voiture et de la partie adverse. Vias. Rapport n°2023-R-17FR. [https://www.vias.be/publications/Impact%20voertuigkenmerken/Impact\\_des\\_caract%C3%A9ristiques\\_des\\_v%C3%A9hicules.pdf](https://www.vias.be/publications/Impact%20voertuigkenmerken/Impact_des_caract%C3%A9ristiques_des_v%C3%A9hicules.pdf)

Organisation for Economic Cooperation and Development (OECD) (2019). Taxing Energy Use 2019; Using Taxes for Climate Action. <https://www.oecd.org/tax/taxing-energy-use-efde7a25-en.htm>

OECD (2019b). Taxing vehicles, fuels, and road use; Opportunities for improving transport tax practice. [https://www.oecd-ilibrary.org/taxation/taxing-vehicles-fuels-and-road-use\\_e7f1d771-en](https://www.oecd-ilibrary.org/taxation/taxing-vehicles-fuels-and-road-use_e7f1d771-en)

OECD (2020). Taxing Vehicle Use (Chapter 4 in Consumption Tax Trends 2020; VAT/GST and Excise Rates, Trends and Policy Issues). <https://www.oecd-ilibrary.org/sites/d5115edf-en/index.html?itemId=/content/component/d5115edf-en>

Ou, Xunmin, Yuan, Zhiyi, Wang, Yanzhe, and Ren Lei (2022), The Development of High-Speed Rail in China - Impact Research on Transportation Modal Shift and CO<sub>2</sub> Emission Reduction Potential, Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH, [https://transition-china.org/wp-content/uploads/2022/06/20220621\\_HSR-Study-English-Final.pdf](https://transition-china.org/wp-content/uploads/2022/06/20220621_HSR-Study-English-Final.pdf)

Ossiander, Eric, Koepsell, Thomas, McKnight, Barbara (2014, 16 May), Crash fatality and vehicle incompatibility in collisions between cars and light trucks or vans. Injury prevention. <https://doi.org/10.1136/injuryprev-2013-041146>

Parking Reform Atlas (2021). Japan's Proof-of-Parking rule (shako shomeisho). [https://www.parkingreformatlas.org/parking-reform-cases-1/japan-s-proof-of-parking-rule-\(shako-shomeisho\)](https://www.parkingreformatlas.org/parking-reform-cases-1/japan-s-proof-of-parking-rule-(shako-shomeisho))

Pavlovic, Jelica, Ciuffo, Biagio, Fontaras, Giogios, Valverde, Victor and Marotta, Alessandro (2018, May). How much difference in type-approval CO<sub>2</sub> emissions from passenger cars I Europe can be expected from changing to the new test procedure (NEDC vs. WLTP)?. Transportation Research Part A: Policy and Practice, <https://doi.org/10.1016/j.tra.2018.02.002>

Parekh, Nishant and Campau, Todd (2022, May 23), Average Age of Vehicles in the US Increases to 12.2 years, according to S&P Global Mobility, S&P Global, <https://www.spglobal.com/mobility/en/research-analysis/average-age-of-vehicles-in-the-us-increases-to-122-years.html>

Parry, Ian, W.H., Black, Simon, Vernon, Nate (2021, 24 September). Still Not Getting Energy Prices Right: A Global and Country Update of Fossil Fuel Subsidies. <https://www.imf.org/en/Publications/WP/Issues/2021/09/23/Still-Not-Getting-Energy-Prices-Right-A-Global-and-Country-Update-of-Fossil-Fuel-Subsidies-466004>

Perl, Andreas (2020). Vehicles have to fulfill these safety requirements. <https://www.vda.de/en/topics/automotive-industry/Standardization-and-technical-standards/euro-ncap-anforderungen>

Pernice, Davide and Debyser, Ariane (2023), Road traffic and safety provisions. Fact Sheets on the European Union. European Parliament. <https://www.europarl.europa.eu/factsheets/en/sheet/129/road-traffic-and-safety-provisions>

PwC (2022). 2022 Global Automotive Tax Guide. [https://www.pwc.com/ee/et/assets/document/2022-Global-Automotive\\_FormatierteVersion.pdf](https://www.pwc.com/ee/et/assets/document/2022-Global-Automotive_FormatierteVersion.pdf)

Rajagopal, Deepak, Phadke, Amol (2019, 6 September). Prioritizing electric miles over electric vehicles will deliver greater benefits at lower cost. Environmental Research Letters. <https://iopscience.iop.org/article/10.1088/1748-9326/ab3ab8>

Randall, Chris (2022, 24 November). Philippines drops import duties for electric vehicles. <https://www.electrive.com/2022/11/24/philippines-drop-import-duties-for-electric-vehicles/>

Reuters (2023, May 2022), China's Wuling Motors cuts Mini EV starting prices to as low as 29,800 yuan, <https://www.reuters.com/business/autos-transportation/chinas-wuling-motors-cuts-mini-ev-starting-prices-low-29800-yuan-2023-05-22/>

Riofrancos, Thea, Kendall, Alissa, Dayemo, Kristi, Haugen, Matthew, McDonald, Kira, Hassan, Batul, Slattery, Magaret, and Lillehei, Xan (2023), Achieving Zero Emissions with More Mobility and Less Mining, Climate and Community Project, <https://www.climateandcommunity.org/files/ugd/d6378bb03de6e6b0e14eb0a2f6b608abe9f93d.pdf>

Riposseau, Gatién-Hugo (2023, 22 June). Stationnement voiture. Comment Paris va taxer les SUV. <https://www.largus.fr/actualite-automobile/stationnement-voiture-comment-paris-va-taxer-les-suv-30027746.html>

Robert, Emmanuel (2020, 14 March). Citroën AMI — Decrypting disruptive innovation with C-K theory. <https://medium.com/@emmanuel.robert/citro%C3%ABn-ami-decrypting-disruptive-innovation-with-c-k-theory-ab03a08274e0>

Robinet, Alice and Gérardin, Maxime (2022, November). Voiture électrique : à quel coût ? [https://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/fs-2022-na-115-voiture-electrique-a-quel-cout-novembre\\_1.pdf](https://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/fs-2022-na-115-voiture-electrique-a-quel-cout-novembre_1.pdf)

Roch Baranowski, Brin, Zayer, Eric, Stricker, Klaus and Stein, Ingo (2023, 17 February), The Outlook for the European Used Car Market, Bain & Company, <https://www.bain.com/insights/the-outlook-for-the-european-used-car-market-brief/>

Romei, Valentina (2022, 30 October), European consumers cut back on discretionary spending, Financial Times, <https://www.ft.com/content/b26e11b4-feb5-4c68-a742-f41c114fab03>

SAC (2021), 乘用车燃料消耗量评价方法及指标 Fuel consumption evaluation methods and targets for passenger cars, <https://std.samr.gov.cn/gb/search/gbDetailed?id=9B70DDA94012A80CE05397BE0A0A84AC>

Shaffer, Blake, Auffhammer, Maximilian and Samaras, Constantine (2021). Make electric vehicles lighter to maximize climate and safety benefits. Nature. <https://doi.org/10.1038/d41586-021-02760-8>

Schmuel, John (2022, 29 April), Canadians increasing budget or delaying car purchases amid high prices: Survey, Bloomberg, <https://www.bnnbloomberg.ca/canadians-increasing-budget-or-delaying-car-purchases-amid-high-prices-survey-1.1759003>

Sergeev, Angel (2023, 12 July). Paris To Fight Pollution With Higher Parking Fees For SUVs. <https://www.motor1.com/news/676490/paris-higher-parking-fees-suvs/>

Slowik, Pete, Isenstadt, Aaron, Pierce, Logan and Searle, Stephanie (2022, 18 October), Assessment of light-duty electric vehicle costs and consumer benefits in the United States in the 2022-2035 time frame, International Council for Clean Transportation (ICCT), <https://theicct.org/publication/ev-cost-benefits-2035-oct22/>

Sprei, Frances (2018, March), Disrupting mobility. Energy Research & Social Science. <https://doi.org/10.1016/j.erss.2017.10.029>

Straughan, David (2023, 6 September), The Semiconductor Shortage Explained: The Auto Industry's Big Challenge, <https://www.automoblog.net/research/news/semiconductor-shortage-explained/>

Stricker, Klaus and Correa, Pedro (2023, 27 September), Automotive Profitability: How OEM and Supplier Margins Are Faring, Bain & Company, <https://www.bain.com/insights/automotive-profitability-how-oem-and-supplier-margins-are-faring-interactive/>

Sussams, Luke, Mintenig, Jana, Röttmer, Nicole and Brunke, Jean-Christian (2018), Transition risks in the automotive sector, Kepeler Cheuvreux Transition Research, <https://et-risk.eu/wp-content/uploads/2018/07/Transition-risks-for-autos.pdf>

Te Manatū Waka (n.d.), Ngā Waka Mā - Clean Cars, <https://www.transport.govt.nz/area-of-interest/environment-and-climate-change/clean-cars/>

TfL (Transport for London) (2016). Taxi and Private Hire Action Plan 2016. <https://content.tfl.gov.uk/taxi-and-private-hire-action-plan-2016.pdf>

TfL (2020). Emissions standards for taxis. <https://tfl.gov.uk/info-for/taxis-and-private-hire/emissions-standards-for-taxis>



Tietge, Uwe, Mock, Peter, German, John and Bandivadekar, Anup (2017, November 5), From laboratory to road: a 2017 update of official and real-world fuel consumption and CO<sub>2</sub> values for passenger cars in Europe, , International Council for Clean Transportation (ICCT), <https://theicct.org/publication/from-laboratory-to-road-a-2017-update/>

TransportPolicy.net (n.d.), <https://www.transportpolicy.net/>

TrendsInAfrica (2023, 5 July). Rwanda exempts electric vehicles from import duties. <https://trendsnafrica.com/rwanda-exempts-electric-vehicles-from-import-duties/>

True (2021, November), Real-world NO x emissions of Euro 6d-TEMP and 6d passenger cars, [https://theicct.org/wp-content/uploads/2022/01/TRUE-Brussels-nov2021-facts-6d-TEMP\\_EN.pdf](https://theicct.org/wp-content/uploads/2022/01/TRUE-Brussels-nov2021-facts-6d-TEMP_EN.pdf)

Tsiakmakis, Stefanos, Fontaras, Giorgios, Cubito, Clausio, Pavlovic, Jelica, Anagnostopoulos, Konstantinos and Ciuffo, Biagio, From NEDC to WLTP: effect on the type-approval CO<sub>2</sub> emissions of light-duty vehicles, EUR 28724 EN, Publications Office of the European Union, <https://dx.doi.org/10.2760/93419>

Toll Customs Norway (2023). Electric Vehicles. <https://www.toll.no/en/goods/motor-vehicles/electric-vehicles/#:-:text=From%201%20January%202023%2C%20a,per%20kg%20must%20be%20calculated.>

Tyndall, Justin (2021, September), Pedestrian deaths and large vehicles. Economics of Transportation. <https://doi.org/10.1016/j.ecotra.2021.100219>

Tyndall, Justin (2023, 10 July), The Effect of Vehicle Size On Pedestrian Death Risk. <http://dx.doi.org/10.2139/ssrn.4505494>

Uber (2018, 23 October). Uber's Clean Air Plan to help London go electric. <https://www.uber.com/en-GB/newsroom/uber-helps-london-go-electric/>

Ueckerdt, Falko, Bauer, Christian, Dirnaichner, Alois, Overall, Jordan, Sacchi Romain and Luderer, Gunnar (2021, 6 May), Potential and risks of hydrogen-based e-fuels in climate change mitigation, Nature Climate Change. <https://doi.org/10.1038/s41558-021-01032-7>

UN (United Nations) (2005), Special Resolution No. 1 concerning the common definitions of vehicle categories, masses and dimensions (S.R.1), <https://unece.org/fileadmin/DAM/trans/doc/2005/wp29/TRANS-WP29-1045e.pdf>

UN (2021), UN Vehicle Regulations for road safety Cost-benefit methodology, [https://unece.org/sites/default/files/2021-09/CBA%20publication%20E%20web\\_0.pdf](https://unece.org/sites/default/files/2021-09/CBA%20publication%20E%20web_0.pdf)

UN (2022, 14 April). United Nations Global Technical Regulation on In-vehicle Battery Durability for Electrified Vehicles Addendum 22: United Nations Global Technical Regulation No. 22, [https://unece.org/sites/default/files/2023-01/ECE\\_TRANS\\_180a22e.pdf](https://unece.org/sites/default/files/2023-01/ECE_TRANS_180a22e.pdf)

UN (2023), Consolidated Resolution on the Construction of Vehicles (R.E.3), [https://unece.org/sites/default/files/2023-05/ECE\\_TRANS\\_WP.29\\_78\\_Rev.7.pdf](https://unece.org/sites/default/files/2023-05/ECE_TRANS_WP.29_78_Rev.7.pdf)

UNECE (United Nations Economic Commission for Europe) (2023a, 21 June), UNECE adopts groundbreaking regulation introducing methodology to measure particle emissions from cars and vans' braking systems. <https://unece.org/environment/press/unece-adopts-groundbreaking-regulation-introducing-methodology-measure-particle>

UNECE (2023b), Automotive - Life Cycle Assessment (A-LCA), <https://wiki.unece.org/pages/viewpage.action?pagelId=172852228>

UNECE (2023c), Electric Vehicle Safety (EVS), <https://wiki.unece.org/pages/viewpage.action?pagelId=3178628>

UNECE (2023d), Working Party on Passive Safety (GRSP), <https://wiki.unece.org/pages/viewpage.action?pagelId=2523227>

UNECE (2023e, 22 June). UNECE to develop battery durability requirements for electric heavy-duty vehicles. <https://unece.org/media/press/380042>

UNEP (United Nations Environment Programme) et al., (2019). Electric Mobility: Status in Latin America and the Caribbean and Opportunities for Regional Collaboration 2019. <https://movelatam.org/wp-content/uploads/2020/09/Report-of-Electric-Mobility-in-Latin-America-and-the-Caribbean-2019-LQ.pdf>

UNEP (2021), Used vehicles and the environment - Progress and updates 2021, <https://www.unep.org/resources/report/used-vehicles-and-environment-progress-and-updates-2021>

United States Congress (2022, 3 January). Inflation Reduction Act of 2022 (H. R. 5376—3). <https://www.govinfo.gov/content/pkg/BILLS-117hr5376enr/pdf/BILLS-117hr5376enr.pdf>

United States Department of Transportation. (n.d.). Bipartisan Infrastructure Law. <https://www.transit.dot.gov/BIL>

United States Joint Office of Energy and Transportation. (n.d.) Joint Office vision: A future where everyone can ride and drive electric. <https://driveelectric.gov/>

United States Treasury (2023, 31 March). Treasury Releases Proposed Guidance on New Clean Vehicle Credit to Lower Costs for Consumers, Build U.S. Industrial Base, Strengthen Supply Chains. <https://home.treasury.gov/news/press-releases/jy1379>

Urban Access Regulations (n.d.), Urban Access Regulations in Europe, <https://urbanaccessregulations.eu/low-emission-zones-main>

Van den Berghe, Wouter (2021), European Road Safety Observatory Road Safety Thematic Report – Speed, [https://road-safety.transport.ec.europa.eu/system/files/2021-07/road\\_safety\\_thematic\\_report\\_speeding.pdf](https://road-safety.transport.ec.europa.eu/system/files/2021-07/road_safety_thematic_report_speeding.pdf)

Van Wyk, Barry (2023, 17 February), Mini electric cars are big in China — will the rest of the world catch on?, The China project, <https://thechinaproject.com/2023/02/17/mini-electric-cars-are-big-in-china-will-the-rest-of-the-world-catch-on/>

VDA (2022, 3 March), Support for sanctions - significant impact of the war, German Association of the Automotive Industry, [https://www.vda.de/en/press/press-releases/2022/220303\\_PM\\_Support-for-sanctions---significant-impact-of-the-war](https://www.vda.de/en/press/press-releases/2022/220303_PM_Support-for-sanctions---significant-impact-of-the-war)

Ville de Paris (2023, June). Code de la Rue : Redonner la Priorité aux Piétons. <https://cdn.paris.fr/presse/2023/06/28/cb7323a60a9aab56db4824f21195b827.pdf>

Waka Kotahi (n.d.), Clean Car Standard, <https://www.nzta.govt.nz/vehicles/clean-car-programme/clean-car-standard/>

Welch, David and Naughton, Keith (2023, 14 February), New cars are only for the rich now as automakers rake in profits, Bloomberg, <https://www.bloomberg.com/news/features/2023-02-14/new-car-prices-are-so-high-only-rich-americans-can-afford-them>

Willsher, Kim (2023, 11 July). Paris to charge SUV drivers higher parking fees to tackle 'auto-besity'. <https://www.theguardian.com/world/2023/jul/11/paris-charge-suv-drivers-higher-parking-fees-tackle-auto-besity>

World Bank (2023), World Bank Open Data, <https://data.worldbank.org/>

WTO (World Trade Organization) (1994, 11 October). United States – Taxes on Automobiles. <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=Q:/GG/DS/31R.PDF&Open=True>

WTO (n.d.a). Agreement on Subsidies and Countervailing Measures ("SCM Agreement"). [https://www.wto.org/english/tratop\\_e/scm\\_e/subs\\_e.htm](https://www.wto.org/english/tratop_e/scm_e/subs_e.htm)

WTO (n.d.b). General Agreement on Tariffs and Trade (GATT) 1994. [https://www.wto.org/english/res\\_e/publications\\_e/ai17\\_e/gatt1994\\_e.htm](https://www.wto.org/english/res_e/publications_e/ai17_e/gatt1994_e.htm)

WTO (n.d.c). WTO rules and environmental policies: key GATT disciplines. [https://www.wto.org/english/tratop\\_e/envir\\_e/envt\\_rules\\_gatt\\_e.htm](https://www.wto.org/english/tratop_e/envir_e/envt_rules_gatt_e.htm)

WTO (n.d.d). WTO rules and environmental policies: GATT exceptions. [https://www.wto.org/english/tratop\\_e/envir\\_e/envt\\_rules\\_exceptions\\_e.htm](https://www.wto.org/english/tratop_e/envir_e/envt_rules_exceptions_e.htm)

WTO (n.d.e). Article XX. General Exceptions. [https://www.wto.org/english/res\\_e/booksp\\_e/gatt\\_ai\\_e/art20\\_e.pdf](https://www.wto.org/english/res_e/booksp_e/gatt_ai_e/art20_e.pdf)

WTO (n.d.f). WTO legal texts. [https://www.wto.org/english/docs\\_e/legal\\_e/legal\\_e.htm#GATT94](https://www.wto.org/english/docs_e/legal_e/legal_e.htm#GATT94)

Wu, Mark, Salzman, James (2014). The Next Generation of Trade And Environment Conflicts: The Rise Of Green Industrial Policy. <https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1022&context=nulr>

Xinhua (2020), Full Text: Sustainable Development of Transport in China, [http://english.scio.gov.cn/whitepapers/2020-12/22/content\\_77040131\\_4.htm](http://english.scio.gov.cn/whitepapers/2020-12/22/content_77040131_4.htm)

Yin, Zhifang, Zhang, Wandi and Li, Chao (2022), Promoting China's Transition Towards Sustainable Transport Integration, Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH, <https://transition-china.org/wp-content/uploads/2022/11/Promoting-Chinas-Transition-Towards-Sustainable-Transport-Integration-3.pdf>

Zipper, David (2023, 4 January). Electric Vehicles Are Bringing Out the Worst in Us. The Atlantic. <https://www.theatlantic.com/ideas/archive/2023/01/electric-vehicles-suv-battery-climate-safety/672576/>

# ENDNOTES

- 1 Europe includes all member countries of the European Economic Area (EEA) plus Switzerland and the United Kingdom. North America includes the United States and Canada but excludes Mexico, as that country's vehicle market and regulatory framework both are quite different from those of United States and Canada (whose market and regulations are quite similar). For the full list of countries in each region, see the Table A6 of the appendix.
- 2 Data collected and reported here attempt, to the extent possible, to focus on vehicles classified as M1 in the Consolidated Resolution on the Construction of Vehicles of the United Nations (UN, 2023), considered as passenger cars and SUVs. Light commercial vehicles are classified as N1 in the same Resolution. For markets not applying these definitions (in particular the United States), passenger cars are considered as the Category 1-1 vehicle according to the Special Resolution 1 concerning the common definitions of vehicle categories, masses and dimensions (S.R.1) of the United Nations (UN, 2005). Light commercial vehicles belong to Category 2 and include vans. More specifically, they include vehicles in Classes 1 and 2 (i.e. Light Duty Vehicles) based on the classification of the Federal Highway Administration (AFDC, n.d.).
- 3 These affected, at once, near-term deployment of shared vehicles, vehicle lifetime and turnover rates and consumer interest. Available evidence from global reviews (such as Sprei, 2018; Adler, 2019; Tirachini, 2019; and ITF, 2020a) indicates that these may have contributed to contain the growth in personal vehicle ownership, despite remaining uncertainties.
- 4 North America includes the United States and Canada but excludes Mexico, as that country's vehicle market and regulatory framework both are quite different from those of United States and Canada (whose market and regulations are quite similar). Europe includes all member countries of the European Economic Area (EEA) plus Switzerland and the United Kingdom. For the full list of countries in each region, see Table A1 of the appendix.
- 5 Consumer prices for new cars and trucks have risen by over 20% over four years since the second half of 2020; slightly higher than the overall increase in consumer prices of 18% over the same period (Bureau of Labor Statistics, 2023).
- 6 Where Lge stands for litres of gasoline equivalent. Lge is used to standardise fuel consumption according to their volumetric energy content. One litre of diesel equals 1.14 litres of gasoline equivalent. As Lge measures energy, it is directly converted into kWh or MJ: considering 33.5 MJ/Lge, 44.8 MJ/kg and 3.6 MJ/kWh, 1 Lge corresponds to 9.3 kWh. This is in line with the IPCC guidelines on the reporting of CO<sub>2</sub> emissions from fuel combustion from mobile sources, considering 69.3 g CO<sub>2</sub>/MJ, for gasoline (IPCC, 2006).
- 7 Since gasoline and diesel are a globally traded commodity, their cost of production varies little across countries. Most of the variability in fuel prices can be explained by fuel taxation and subsidy regimes.
- 8 European countries, Japan and Korea tend to apply high fuel taxes, which push fuel prices above USD 1.5/litre (scaled to reflect affordability using PPP). The sales-weighted average fuel consumption of light-duty vehicles sold in many of these countries are among the lowest in the world. In these countries, fuel economy regulations are also stringent. In contrast, fuel taxes in Australia, Canada and the United States are low, fuel prices are just below USD 1/litre, and the average fuel consumption of light-duty vehicles is above the global average. While high level results are also clear for developing countries, specific trends for the 2019 to 2022 developments are less homogeneous. If fuel prices, following a scale up based on purchasing power, are high, vehicle size and energy consumption in emerging markets and developing countries tend to have a similar magnitude to those observed in Europe, Japan and Korea. If fuel prices are lower, average energy consumption in emerging markets and developing economies tends to lie in between the values in North America and those in Europe.
- 9 These are not included in the data shown in Figure 5, as they are the result of driving cycles that account for a range of accelerations and speeds (with the ambition to represent real-world driving) and do not yet include test procedures to fully integrate auxiliary loads.
- 10 Conversion factors across test cycles (CAFE, NEDC, JC08, WLTC) are reported for gasoline and diesel in Table 5.2 of the ICCT 2014 report. ICCT regressions were developed based on modelling results from Ricardo's Data Visualization Tool (DVT) (Meszler et al., 2013), itself based on MSC Easy5 (Hexagon, n.d.).
- 11 Data came from EEA databases of CO<sub>2</sub> emissions from new passenger cars (PLDV's, in the GFEI reports) and CO<sub>2</sub> emissions from light commercial vehicles (LCV's), using EEA final data for 2019-2021 and preliminary data for 2022.
- 12 The recognition of a systemic mismatch between real-world and rated NOx emissions increased regulatory pressure and reduced consumer interest in diesel vehicles. Since 2015, the stringency of pollutant emissions standards in Europe has increased markedly, especially for diesel vehicles (European Court of Auditors, 2019). The need to comply with these stricter pollutant emissions standards eroded the cost advantages of diesel cars, especially for small and medium vehicles, segments where the decline in diesel sales shares has been fastest.
- 13 These included a super credit multiplier for vehicles with rated emissions below 50 g CO<sub>2</sub>/km, which was gradually phased out through 2022, as well as incentives awarded in cases where the share of zero- and low-emissions vehicles exceeds a determined benchmark.
- 14 As discussed in Chapter 3, Japan's designation of and preferential policies toward Kei-cars contribute to the continued resilience of the small car segment there.
- 15 Footprint is defined as the area defined by the four points where the tires touch the ground. It is calculated as the product of the wheelbase and the average track width of the vehicle (US DOE, 2011).
- 16 Intended as kerb mass, defined in international regulations as the mass of the vehicle in running order, without occupant or load, but with fuel, coolant, lubricant, toolkit and spare wheel (UN, 2023).
- 17 As detailed in the "Micro analysis" section of the GFEI Working Paper 17, "Wider, Taller, Heavier: Evolution of Light Duty Vehicle Size Over Generations," vehicle models within segments have also gradually grown larger (as measured by footprint and height) and heavier (as measured by kerb weight) (Cuenot, 2019).
- 18 Environmental impacts also depend on pollutant emissions, with consequences on air quality. In the case of SUVs, emissions of local pollutants are not discussed in a specific sub-section. The reason lies in the nature of regulatory measures regarding pollutant emissions of passenger cars and part of the LCVs, since these are set in terms of grams per km, and not per unit of energy use, meaning that – excluding (i) compliance-related aspects (which are beyond the scope of this work) (ii) powertrain shifts across ICEVs (namely, between gasoline and diesel), and (iii) increased emissions of non-tailpipe large particulate emissions (road dust, tyre wear, and brake wear) resulting from the weight increases – the SUV shift has no direct implications on variations in pollutant emissions. Regarding ICE powertrain shifts, differentiated impacts relate primarily with the evolution of sales shares and differences in regulatory requirements between spark ignition (reliant on the gasoline fuel blend) and compression ignition vehicles (reliant on diesel fuel).
- 19 According to a similar analysis developed by the IEA in 2021 (for the period 2010-2019), at the global scale, the segment shift eroded as much as 40% of the fuel consumption improvements that would otherwise have occurred, without the shift (IEA, 2021a).
- 20 Small increases in biofuel use have limited impacts on the carbon intensities of the fuels. These are neglected here.
- 21 In this context, small cars have the lowest consumer appeal, as car buyers in developed economies have higher purchasing power, and low fuel prices/taxes lead them to give less consideration operating costs.
- 22 Other reasons for this tendency towards an increase in vehicle age may include quality enhancements in vehicles, enabling them to become more durable. More recent developments in connectivity and over the air software updates – although they are not yet paired with sizable impacts at the scale of the global stock – could also strengthen this trend further, in the future.
- 23 Prices of second-hand cars have been heavily influenced by Covid-19 related supply chain shortages, in particular for semiconductors, resulting in lower-than-expected availability of new vehicles. These constraints contributed to a price surge in 2021 that has only been moderately easing in 2022 and 2023 (Muir, 2023; Autovista24, 2023; Mannheim, 2023). Both in Europe and North America, second-hand vehicle prices are currently still well above pre-pandemic values.

- 24** Chapter 1 and other analyses on the EV market developments show that the increase in EV shares is currently mainly occurring in China, Europe and North America (IEA, 2023; Cazzola and Santos Alfageme, 2023).
- 25** Similar to the case of the SUV shift, impacts of the EV transition on emissions of local pollutants are not assessed in detail in this report. High-level indications available from other assessments point towards counteracting effects, as EVs lead to greater tyre wear and road dust, but they also come with zero emissions of local pollutants at the tailpipe. Differences in overall levels of pollutant emissions also depend on the regulatory framework and the compliance policies in place in different countries. EVs have been found in a recent OECD report to emit levels of non-exhaust emissions similar to those of well-maintained ICE vehicles in developed economies (OECD, 2020), even if non-exhaust emissions of particulate matter from tyre and brake wear were largely unregulated before the Euro 7 norm (currently being finalized). This suggests that they are likely to lead to net benefits in terms of air quality in many countries, as most of the world still applies pollutant emission norms that are less stringent than Euro 6 (i.e., the norms considered in the comparison in the OECD assessment). Importantly, analyses related with health impacts also point to lower risks for tyre wear and road dust than for exhaust emissions, due to lower content of ultra-fine particles and different chemical composition (ITF, 2021b). This also suggests that health impacts of EVs related with emissions of local air pollutants are likely to be lower than those of ICEVs.
- 26** The presence of the ICE and its volume is one of the key reasons why PHEVs tend to be marketed primarily in larger vehicle segments. For this reason, PHEVs may have had a relevant role, in recent years, for OEM design choices that privileged a shift to SUVs.
- 27** BEVs can also benefit from opportunities for radical redesign, in comparison with PHEVs.
- 28** Welch and Naughton, 2023 also refer to a price gap of 35% between EVs and their gasoline-fuelled counterparts.
- 29** This is due to lower energy efficiency of ICEV with respect to EVs and higher relevance of operational costs for ICEV drivers. Fossil fuel price volatility is partly mitigated by fuel taxation, especially in countries with higher fuel taxes. EV drivers are also affected by fossil fuel price volatility, especially in cases where electricity is still reliant on thermal

generation and where electricity prices are set by the marginal electricity producer.

- 30** This is possible in cases showing greater demand for EVs from high-income households and from businesses subject to lower capital availability constraints. The effect may be enhanced by fossil fuel price increases.
- 31** It is worth noting that increased demand for batteries for stationary applications could also have positive impacts on EV battery costs, thanks to the possibility to offer greater economies of scale in battery manufacturing.
- 32** As long as motorization does not lead to a surge in traffic congestion. This underlines the need for a systemic approach to the management of transport decarbonization, including measures related with the development of land use and transport infrastructure, across different transport modes.
- 33** A shift toward EVs comes with significant costs for incumbent OEMs. These not only include research and development, but also – and probably above all – investments in new industrial facilities and re-skilling of personnel. Additional indirect costs are paired with the risk of an early dismissal of existing facilities, or parts of them. The risk of losing market share, especially in the context of policies mandating reductions in GHG emissions, due to the competitiveness of EVs in that environment, provides a strong counterbalancing force to delayed investments in the powertrain transition.
- 34** The greater material intensity of SUVs—and in particular steel and aluminium content—together with recovery rates of recycled materials that are even in the best cases less than one, plus the need for high-quality (and often primary) materials in certain cases (e.g., for advanced high-strength steel), means that even circular material flows would not be sufficient to supply materials for newly produced vehicles.
- 35** These relate with lower risks of supply disruptions in a diverse material extraction, material processing and battery manufacturing environment.
- 36** Vehicle and energy production, along with the construction and maintenance of the infrastructure they require, are important sources of direct and indirect employment (ILO, 2018).
- 37** China's vehicles exports boomed starting in mid-2020, with new passenger vehicle exports

increasing from 1.6 million in 2021 to over 2.5 million in 2022, and 1.75 million in the first half of 2023 (CAAM, 2023), with 2023 volumes approaching exports of Germany and Japan, the world's two largest car exporters. Electric passenger vehicle export shares roughly match China's market shares – for instance, both were 29% in 2022 (CAAM, 2023), and most have gone to upper middle and high income countries (The Economist, 2023).

- 38** This argument may partially explain the interest of some of the major OEMs to enter more prominently in the L6 and L7 markets – i.e. quadricycles, based on UN definitions (UN, 2023) – with EVs, taking advantage of lower regulatory barriers. Possible drawbacks related to road safety challenges – including due to lower barriers in terms of vehicle age and license to drive, alongside minimum safety features of these lighter vehicles, and the fact that they would share the road with cars, pickups and SUVs – need to be adequately managed.
- 39** A focus on global areas with high renewable energy availability could enable the cost-effective production of low-carbon hydrogen and e-fuels. However, it should be noted that the required technologies, namely different approaches to direct air capture, are not yet commercialised. Moreover, the scale of fuel demand would require very significant rates of deployment of renewable energy production capacity in these global areas (Ueckerdt et al., 2021). This is subject to significant geopolitical challenges, including those of intended North-South relations, and questions of social justice, exacerbating (due to lower lifecycle energy efficiency) those already observed for the Desertec Industrial Initiative (DII), meant to bring large amounts of renewable electricity to Europe, from North Africa (Schmitt, 2018). Additional challenges, for e-fuels containing carbon, stem from the same sustainable biomass availability constraints already mentioned for biofuels (despite the possibility, through co-location of renewable or nuclear electricity and biomass supplies, to increase biofuel yields, with power-and-biomass to fuel technologies), as well as from the volumes of air that would need to be processed for large-scale direct air capture (DAC).
- 40** The same issue of huge volumes of air to be processed, for DAC-based carbon dioxide removal technologies, also apply for offsets, in addition to e-fuel production.
- 41** Regulations, for LDVs and beyond, may not only be enacted for environmental or safety reasons,

but also as part of an industrial strategy, and even with protectionist objectives. However, in cases where the solutions promoted by regulatory developments are not cost-effective, this exposes economies and societies to risks, underlining the importance to maintain a focus on economic competitiveness when designing technology-specific regulatory tools.

- 42** Key examples exist in the case of biofuels, since increased demand for bio-based feedstocks (e.g., waste oils or lignocellulosic materials) in road transport can trigger shifts in demand in other sectors (e.g., the chemical and/or paper and pulp industries), or in the case of hydrogen, since increased demand for low-carbon electricity to produce renewable hydrogen can reduce the availability of low-carbon electricity in the grid, increasing demand for thermal (fossil-based) generation, and ultimately increasing GHG emissions, due to lower energy efficiency of hydrogen use vs. the direct use of electricity across many end-uses (where the higher efficiency of direct use of electricity is an indicator of better energy quality, especially for the combination of renewable electricity and electricity-based energy conversion appliances).
- 43** The working group aims to develop methodologies and standards to promote carbon intensity (CI) reductions across all stages of the automotive production (material and material recycling, parts and vehicle production), use, fuel and energy provision, and end-of-life. Said standards would both define default carbon intensity (CI) values for the purposes of regulation, and define procedures for monitoring, reporting and verification of operations that perform better (i.e. reduce CI) than the defaults, to enable such operations to be certificated and incentivized in the marketplace.
- 44** Similar considerations also apply to the case of hydrogen-powered vehicles, even if these are not the focus of this analysis. Key examples include hydrogen refuelling protocols, nozzles, compressed and/or liquid hydrogen leaks in confined spaces and crash exposure risks (ITF, 2020b).
- 45** This is also the case for life-cycle assessments across almost all global geographies, as many analyses have shown (e.g., IEA, 2019c and Bieker, 2021), largely thanks to the possibility to access, with low losses, at least in part, primary electricity from renewable energies and also thanks to lower energy conversion losses occurring in stationary thermal electricity generation facilities than in mobile ICEs.



- 46** Targeted adoption of higher regulatory stringency, as in the case of public procurement, can also effectively bridge the barrier of the development of different technical specifications (especially regarding safety), as these (with very few exceptions – e.g., light commercial vehicles for postal services in the United States) are developed in ways that are uniform across all LDVs, and not specific to different usage patterns.
- 47** Also due to their role in the context of material circularity, as the minerals become part of the vehicle stock representing an asset in the context of cross-sectoral decarbonisation, thanks to lower energy intensity in processes converting scrap metals than in processes requiring processing virgin materials.
- 48** More intensive use is not limited to the case of taxis and ridesourcing services, but it is also relevant for heavy duty road vehicles, like buses and trucks, as well as shared motorcycles.
- 49** Alongside other emission reduction approaches (e.g., reduced deadheading, increased reliance on shared services, including on-demand shuttle services operated by vans and minibuses (ITF, 2020a).
- 50** This was part of a comprehensive scheme that includes mandatory age limits for taxis, incentives for the early retirement of vehicles, investments for the deployment of publicly accessible electric vehicle chargers and the possibility to express preferences on their location, financial support for the installation of home chargers and discounted charging rates (ITF, 2020a; TfL, 2020).
- 51** An example of provisions that goes in the opposite direction, offering an opportunity to learn lessons on practices that are detrimental for the management of vehicle size and weight increase, is the case of new design guidance issued in 2022 for parking space dimensions in the United Kingdom. This proposes to increase the length (from 4.8 to 5 meters) and width (from 2.4 to 2.6 meters) of parking spaces, and claims that the principles behind these increases have global applicability (British Parking Association, 2022).
- 52** Differentiated taxation is rarely applied as a measure aiming to enhance road safety, instead safety is usually addressed via regulatory measures.
- 53** As in the case of luxury taxes.
- 54** Especially for EVs with high price tags. For high income countries, this is only partly mitigated by the possibility that an accelerated EV deployment, thanks to tax advantages, can have on the EV availability for low- and middle-income families, as they trickle down to the second-hand vehicle market.
- 55** This argument is also applicable to pollutant emissions, but only for second hand imports, as new light duty vehicles are subject to the same regulatory limits, per km driven.
- 56** Doing so may require technology-specific provisions (e.g., favouring more energy efficient vehicles, due to lower risks of higher emissions from fuel production). Not doing so risks providing signals that mislead investments, with negative implications for assets that are not aligned with overall sustainability requirements.
- 57** Moreover, specific company car taxation schemes exclude a variable component per unit of distance travelled, resulting in incentives to increase car use over other transport options (Harding, 2014). Others, excluding a fixed component (e.g., related with vehicle acquisition costs), may provide incentives to increase the size or value of the vehicle beyond what would be held if the full costs were taxed (Harding, 2014).
- 58** Where vehicle ownership is restricted to high-income households and businesses, generally representing a smaller fraction of the total, in comparison with high-income countries.
- 59** Most of the WTO agreements are the result of the 1986-94 Uruguay Round negotiations, signed at the Marrakesh ministerial meeting in April 1994 (WTO, n.d.f).
- 60** Kei-cars are Japan's smallest vehicle segment as defined by maximum dimension, engine displacement and power limits. They are subject to preferential taxation, parking, and other regulatory policies.
- 61** As Kei-car policies pre-date the EV transition by decades.
- 62** Tilting the tax rules alone does not guarantee a positive or even neutral environmental result if the overall estimated benefit is too far below the neutral fiscal level (Harding, 2014).
- 63** The socio-economic and distributional argument, together with the focus of businesses on the total cost of ownership rather than purchase prices, likely explains the lower purchase grants for EVs in many countries for corporate cars (Carpenter and Antich, 2022). Revising EV and other incentives for corporate vehicles requires redistribution of the additional governmental revenues generated from higher taxes on company cars. Negative impacts on the balance sheet of businesses can be handled through a shift in vehicle purchase decisions away from larger and more expensive vehicles towards more environmentally friendly technologies.
- 64** And as many of the second-hand EVs available are anyways in larger and more expensive market segments.
- 65** Clear prospects for low electricity costs reinforce this effect for the EV transition (Robinet and Gérardin, 2023). These are more likely in contexts with high shares of low-cost and low-carbon generation technologies, also because of the need to rationally apply taxes to address the externalities of unablated fossil energy used for electricity generation (OECD, 2019a).
- 66** Fuel excise duties are generally considered a very effective tax instrument to deal with negative implications of fossil fuel use on transport vehicles (Carpenter and Antich, 2022).
- 67** Net of energy security aspects, the efficient price per unit of a fossil fuel product includes supply costs, costs due to environmental damage (due to emissions of GHG and local air pollutants) congestion, crashes, road damage and general consumption taxes (Parry et al., 2021).
- 68** The 'Fit for 55' package included a proposal (European Commission, 2021) to create a separate new Emissions Trading System (ETS) for road transport and buildings, with fuel distributors as regulated entities. The Council and the Parliament reached a provisional political agreement regarding this matter in December 2022 (European Parliament, 2022, European Council, 2022) and the final legislative text regarding this file was finalised in May 2023 (European Union, 2023).
- 69** Strict requirements for all-electric driving in zero emission environmental zones are important to ensure that there is greater consumer and industry focus on larger PHEV batteries (still far smaller than BEV batteries) in a transitional phase towards high shares of EVs for road transport electrification. Digital technologies, including solutions enabling geofencing, can help ensure that all-electric driving for PHEVs in these areas is effectively enforced, mobilizing PHEV owners to use electricity as external energy source. Other policies supporting increased shares of all-electric driving for PHEVs include the recent corrections of utility factors in the context of the WLTP test procedure, as well as continued on-board monitoring of driving habits on PHEVs, with respect to these indicators.
- 70** This includes (but is not limited to) fast chargers, which may require targeted support, also to enable better availability of low-cost electricity, given continuing challenges to ensure that they have an effective business model, possibly also in cases where they are owned by OEMs or by joint ventures (as these models may still require subsidization from revenues generated by vehicle sales).
- 71** For instance, requirements for quadricycles do not include airbags and are not subject to crash test requirements (NCAP, 2016, UN, 2023).
- 72** In the context of UN Regulations, these vehicles correspond to the L6 and L7 categories, rather than M1 for cars and N1 for light commercial vehicles.
- 73** In European cities, electric micro vehicles can be used by people as young as 14 (ITF, 2023).
- 74** The same considerations emerge from the need for alternative transport modes needed for extra-urban travel (ITF, 2023).



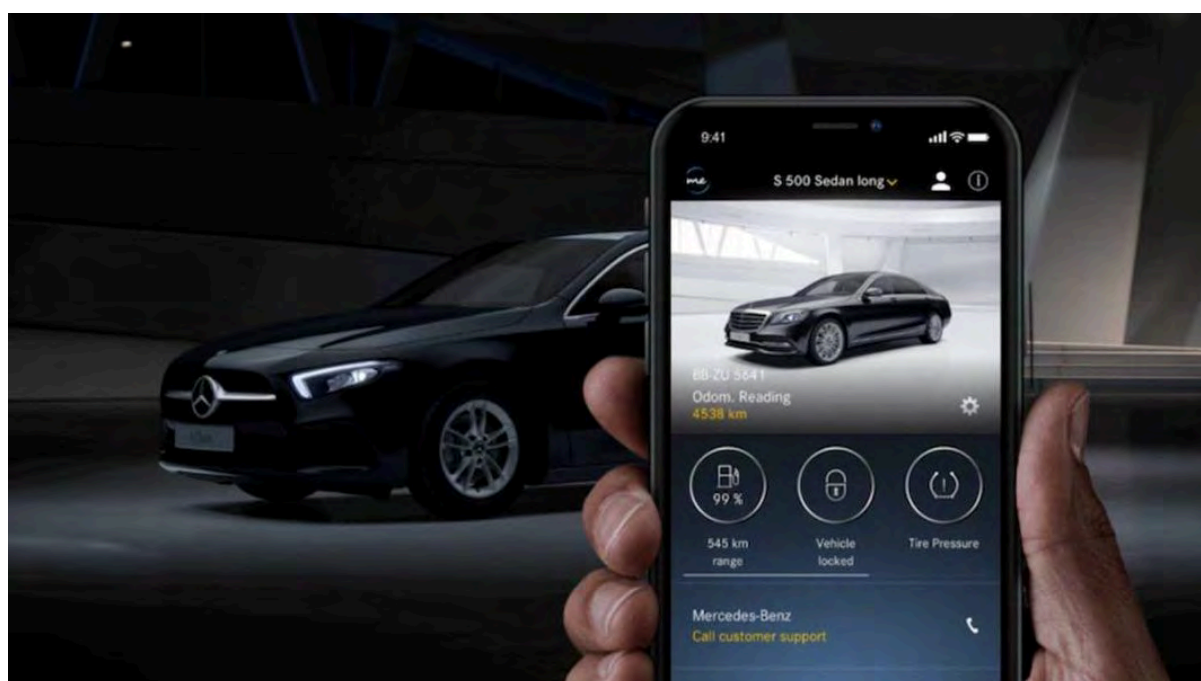


# CONSEJOS DE CIBEREXPERTOS, RECOMENDACIONES DE CIBERSEGURIDAD, CASOS REALES



# POR QUÉ ES BÁSICO TENER UNA CONTRASEÑA ROBUSTA EN LA APP PARA CONTROLAR TU AUTO O LOS MODELOS DE TU FLOTA

Son muy cómodas pero, en cuanto a seguridad, algunas dejan bastante que desear. Dan acceso a muchas funciones de los autos de forma remota, así que cuidado y atención con las contraseñas de la 'app' de tu auto o gestión de flota. Aprende a protegerte.



En medio de la revolución tecnológica que ha transformado la industria del motor, la ciberseguridad se ha convertido en un tema crucial. **Los vehículos conectados cuentan ya**



con más de 100 millones de líneas de código -más de lo que usa el propio Facebook para funcionar- y la **evolución constante de la Inteligencia Artificial plantea nuevos desafíos en la protección de nuestros datos** y, en este caso, en la seguridad de las contraseñas de nuestros automóviles.

La fiebre de las **‘apps para todo’** también han llegado a las marcas de autos, y **gigantes como Mercedes o Sköda han lanzado las suyas al mercado**. Controlar tu auto desde el smartphone te brinda una comodidad muy futurista pero, ¿son estas apps realmente seguras?

**Las contraseñas son a menudo la primera línea de defensa.** Los crackers utilizan herramientas avanzadas para descifrar contraseñas y, **si logran acceder a la app de tu vehículo de forma remota, nada les impide hacer uso de todas las funciones del vehículo** que permite la aplicación. La **Mercedes me**, en su paquete ‘premium’, **incluye las posibilidades de apertura y cierre remotos de las puertas**, la regulación de la calefacción/ventilación, regulación de las ventanillas y del techo corredizo de forma remota, **un localizador del vehículo a distancia**, e, incluso, **la posibilidad de compartir el auto a distancia con su función de ‘entrega digital de llaves’**.

**Seguramente, no haya aplicaciones con mayor valor en el teléfono que la de tu vehículo y la de tu banco.** Una de ellas lleva detrás un trabajo de criptografía que se considera prácticamente irrompible y la otra es la de tu auto. Por eso, al igual que se escucha innumerables veces la necesidad de



mantener una higiene sólida de contraseñas en las webs, plataformas de streaming, correos o teléfonos... ocurre igual con la aplicación de tu auto.



Contraseñas descifradas en minutos: defiéndelas

La **primera capa de la defensa de la app reside en la elección de la contraseña**. Tal y como nos recuerdan los expertos del Área Técnica de [EUROCYBCAR](#), optar por combinaciones complejas de caracteres, evitando información predecible -como fechas señaladas, fechas de cumpleaños o números consecutivos-.

**Activar la autenticación de doble factor** en caso de que no venga de serie también sería ideal, ya que eleva el nivel de seguridad mediante la implementación de una nueva capa de verificación -si te llega un SMS con un código, significa que puedes estar dejando en jaque al ‘cracker’-.

Las **actualizaciones constantes de software**, tanto del propio teléfono como de la aplicación y como las del propio vehículo, **son importantísimas**. Dentro de ellas, se encuentran todas las correcciones necesarias para cubrir y contrarrestar las vulnerabilidades/puertas de entrada ya conocidas.

También es vital concienciar sobre la importancia de **ir con cautela a la hora de interactuar con enlaces o archivos**, incluso si parecen provenir de fuentes confiables; **es esencial no abrir nada que no esperásemos con anterioridad**. La amenaza de ataques de phishing y de nuevas estrategias cada vez más retorcidas subrayan la importancia de cuidar con mucho mimo las credenciales de inicio de sesión.

Todos los posibles escenarios de riesgo

**Imagina el riesgo de permitir a un atacante activar funciones como la apertura o el cierre de puertas**, darle el control de las ventanillas y el del encendido del motor. Un poder así, además de presentar peligros tangibles, podría derivar en situaciones extremas como el secuestro del vehículo.

Otra posibilidad sería la de **aprovechar la función de localización remota del vehículo para realizar un seguimiento no autorizado de éste**, eliminando la privacidad del propietario. Ya se ha dado un caso en Australia en el que, a través de una 'app' , [un ex-marido](#)

controlaba los lugares en los que estaba su ex-pareja constantemente.



Recordar que la comodidad trae consigo inconvenientes es el primer paso para entender que con la movilidad conectada siempre hay que estar un paso por delante. Tener ojo avizor y no perder de vista los básicos para ciberprotegerse, además de instar por concienciar a las marcas de la importancia de respaldar con seguridad todo producto que ponga en peligro la seguridad o privacidad de las personas. Puedes encontrar **más información sobre aplicaciones como Mercedes me** [pinchando aquí](#).



# ¿CÓMO GARANTIZAR UN FUTURO DE AUTOS CONECTADOS Y FLOTAS CIBERSEGURAS?

En la era actual de vehículos inteligentes y tecnologías interconectadas, la ciberseguridad del automóvil se antoja como algo fundamental para garantizar la integridad de los automóviles conectados.



*Imagen generada por la IA de Bing*

Y ese hecho no es algo que se vaya a detener aquí: a medida que la industria y el sector automovilístico **continúen volviéndose cada vez más digitales**, parece de lo más

**razonable que la protección de esos vehículos**, cada vez más conectados, se convierta en una prioridad y una preocupación primordial, tanto para los propios fabricantes como para los usuarios/conductores y para cualquier otra otra parte interesada del sector de la automoción, la movilidad, el transporte... **¿Qué aspectos se deben tener en consideración?** Un experto como Mac, que presume de tener hasta 15 vehículos en su garaje, nos cuenta algunas de las claves.

Proteger el vehículo conectado, pero... ¿cómo?

### **Mediante cifrado y autenticación**

¿Te suena? Es algo habitual en cualquier dispositivo, servicio en Internet... En el caso de los vehículos conectados, que dependen de redes de comunicación complejas, se antoja más necesario, si cabe. **La implementación de medidas sólidas de cifrado y autenticación protege estas redes del acceso no autorizado y las amenazas cibernéticas.**

### **Con la ayuda de actualizaciones inalámbricas -OTA-**

De nuevo, esta medida ya se ha comprobado que es eficaz en todo tipo de dispositivos -principalmente móviles y ordenadores-. Y es que las actualizaciones de software, cuando son periódicas y se extienden en el tiempo, resultan algo esencial ya no solo por mantener al día las funcionalidades de un dispositivo, sino también para corregir las vulnerabilidades. En el caso que nos ocupa, la capacidad de realizar actualizaciones OTA garantiza que los vehículos reciban los últimos parches de seguridad rápidamente.

## **Levantando muros -firewalls- y ‘dividiendo’ para vencer**

La instalación de firewalls y el empleo de estrategias de segmentación de red agregan capas de defensa contra las amenazas cibernéticas, evitando el acceso no autorizado a los sistemas críticos de los vehículos. En ambos casos, hablamos de medidas que tienen la misión de limitar la expansión de una posible intrusión, limitando los posibles daños o consecuencias.

Pero... ¿qué amenaza la ciberseguridad de un automóvil?

### **Los piratas que quieren ‘abordarte’**

Los crackers pueden intentar atacar varios sistemas de los vehículos y tomar el control sobre funciones críticas, que pueden ir desde el manejo de la dirección hasta el de los frenos, el acelerador... y otros secundarios, pero que pueden interferir en la conducción, como el accionamiento del claxon, el volumen de la radio, el limpiaparabrisas... Comprender las vulnerabilidades potenciales ayuda a implementar medidas preventivas.

### **Los datos del auto son muy jugosos**

La gran cantidad de datos generados por los vehículos conectados plantea riesgos de robo de una información que puede tener un gran valor. Garantizar el almacenamiento y la transmisión seguros de datos es crucial para mitigar dichas amenazas.

## Que infecten o secuestren tu vehículo

El software malicioso -también conocido como malware- puede infiltrarse en los sistemas de los vehículos y provocar posibles ataques de ransomware -un tipo de ciberataque mediante el cual, un delincuente encripta o roba información, solicitando un rescate económico a cambio de liberarla o no filtrarla-. Las soluciones antivirus y la monitorización proactiva pueden convertirse en medidas esenciales.

Lo mejor: que el vehículo detecte la intrusión antes de que suceda

## Se llaman IDS, y pueden jugar un papel clave en la ciberseguridad automotriz

Los sistemas de detección de intrusiones -o IDS, por sus siglas en inglés: 'Intrusion Detection System'- actúan como auténticos guardianes, **que vigilan y monitorean, de forma constante, las redes de un vehículo en busca de actividades sospechosas** o comportamientos que se alejen de los patrones habituales. Hay distintos tipos de IDS; los que están basados en firmas y en análisis ofrecen diferentes enfoques para identificar amenazas potenciales, proporcionando un mecanismo de defensa integral.

## Monitoreo y respuesta en tiempo real

Precisamente, el hecho de estar controlando y monitoreando de manera constante es lo que permite llevar a cabo una respuesta inmediata ante las posibles amenazas detectadas, minimizando el impacto que un incidente de ciberseguridad pueda tener en el funcionamiento habitual del vehículo.





*Imagen generada por la IA de Bing*

La ciberseguridad como estándar entre los vehículos...

### **Descripción general de los estándares de la industria**

Que se cumpla con los estándares de ciberseguridad establecidos garantiza un enfoque unificado y sólido para proteger los vehículos en todo el sector del automóvil; un buen ejemplo es la conocida como UNECE/R155. La estandarización fomenta la coherencia y la compatibilidad, lo que facilita que los fabricantes, proveedores y los que prestan servicios alineen sus esfuerzos de ciberseguridad.

...y su integración desde el diseño inicial



## **Colaboración entre fabricantes de automóviles y expertos en ciberseguridad**

Igual que, desde que empieza a plasmar el boceto de un nuevo modelo en una hoja en blanco ya se cuenta con la colaboración de todos los departamentos que van a intervenir en el desarrollo de un vehículo, también se deben dedicar esfuerzos a que, **desde el mismo inicio, se efectúe una colaboración entre fabricantes de automóviles y expertos en ciberseguridad**. El resultado será el famoso ‘security by design’, es decir, vehículos que se han desarrollado, desde el momento de inicio, teniendo en cuenta la ciberseguridad. Implementarla a posteriori suelen llevar aparejadas más dificultades.

## **Inclusión de funciones de ciberseguridad en los nuevos lanzamientos**

A medida que la tecnología evoluciona y va implementándose en los nuevos vehículos -sean de cualquier precio o segmento-, la integración de funciones de ciberseguridad en esos modelos debería convertirse en una **medida proactiva para abordar las amenazas ya conocidas o las que vayan a ir surgiendo en los próximos tiempos**.

## **Mejora continua y adaptarse a lo que pueda llegar**

Es decir, se enfoque dinámico de la ciberseguridad implica una mejora y adaptación continuas para adelantarse a las cambiantes amenazas y vulnerabilidades cibernéticas.

El usuario también debe poner de su parte y estar concienciado

### **Es necesario educar a los conductores sobre los riesgos de ciberseguridad**

Sensibilizar a los conductores sobre los posibles riesgos de ciberseguridad les permite asumir un papel activo en la protección de sus vehículos conectados. Ha sido, desde nuestros inicios, una de las misiones principales de HackerCar: **no solo informar, sino también concienciar de que los vehículos actuales**, cada vez más tecnológicos y un mayor número de funciones conectadas, deben utilizarse de manera responsable y han de contar con un nivel de ciber-protección adecuado.

### **Importancia de las actualizaciones periódicas de software**

También es necesario educar a los usuarios sobre la importancia de actualizar de forma periódica el software del vehículo, ya que es algo que ayuda a mantener los parches de seguridad más recientes.

### **La necesidad de colaborar**

### **Iniciativas de colaboración e intercambio de información**

Los esfuerzos de colaboración y el intercambio de información entre los actores de la industria mejoran la capacidad colectiva para identificar y abordar las amenazas emergentes. Asimismo, las agencias gubernamentales y las

colaboraciones del sector privado contribuyen a la creación de un ecosistema sólido para abordar los desafíos de ciberseguridad desde un punto de vista más amplio. Y como la unión hace la fuerza, un frente unido contra las amenazas cibernéticas **implica iniciativas conjuntas, investigaciones y recursos agrupados para fortalecer la postura de ciberseguridad de la industria del Motor.**

¿Qué es lo que está por llegar en materia de ciberseguridad y automóvil?

### **Avances en tecnologías de ciberseguridad**

Los avances continuos en las tecnologías de ciberseguridad, incluida la **Inteligencia Artificial** y el aprendizaje automático -machine learning-, desempeñarán un papel fundamental para mantenerse a la vanguardia de las ciberamenazas sofisticadas. Y es que, al igual que los ciberdelincuentes recurren a esas nuevas tecnologías para conseguir llevar a cabo ataques más eficaces, los que estamos en el otro lado también nos tenemos que valer de dichas herramientas para combatir a los crackers.

### **¿Para qué sirven la Inteligencia Artificial y el aprendizaje automático?**

La integración de la IA y el aprendizaje automático permite el análisis predictivo, mejorando la capacidad de identificar y responder a las amenazas de ciberseguridad de forma proactiva.

## Amenazas emergentes y medidas preventivas

Anticipar y prepararse para las amenazas emergentes permite a la industria automotriz implementar medidas preventivas, minimizando los riesgos potenciales de ciberseguridad.

## Conclusión

A medida que la industria del automóvil adopta la era digital, priorizar la ciberseguridad no es solo una necesidad: es una responsabilidad. **Proteger los vehículos conectados requiere adoptar muchos enfoques**, que van desde el empleo de soluciones tecnológicas sólidas hasta la educación de los usuarios y la colaboración de la industria. Si se mantiene alerta y proactivo, el sector del Motor puede desenvolverse con más tranquilidad en el panorama cambiante de las ciberamenazas y garantizar un futuro seguro para los vehículos conectados.

# OJO A LOS RIESGOS SI EN TU EMPRESA SE USA LA COMPUTADORA PERSONAL PARA TRABAJAR

El laptop suele resultar un foco de problemas para todos los responsables de ciberseguridad de las empresas. ¿Es posible teletrabajar de forma segura? ¿Qué recomendaciones hacen los expertos?



Se escucha con frecuencia entre CISOs – perfiles encargados de proteger y mantener la seguridad de los datos de la empresa ante posibles ciberataques – de diferentes compañías que **“invertir en ciberseguridad en una**

**compañía no es tanto el dinero que gastes, sino más bien la fe que tengas en que todos se hayan enterado de lo que es seguro hacer y lo que no”.**

Es cierto que los empleados descuidados suelen ser el mayor lastre con el que lidian la gran mayoría de compañías en materias de ciberseguridad; y no necesariamente formando parte de grandes corporaciones, puesto que en España los datos de ataques a PYMES son arrolladores: **el 43% de pequeñas y medianas empresas han sufrido algún tipo de ataque a su red.**

## **Conectividad sólida y ordenadores ‘demasiado’ tecnológicos**

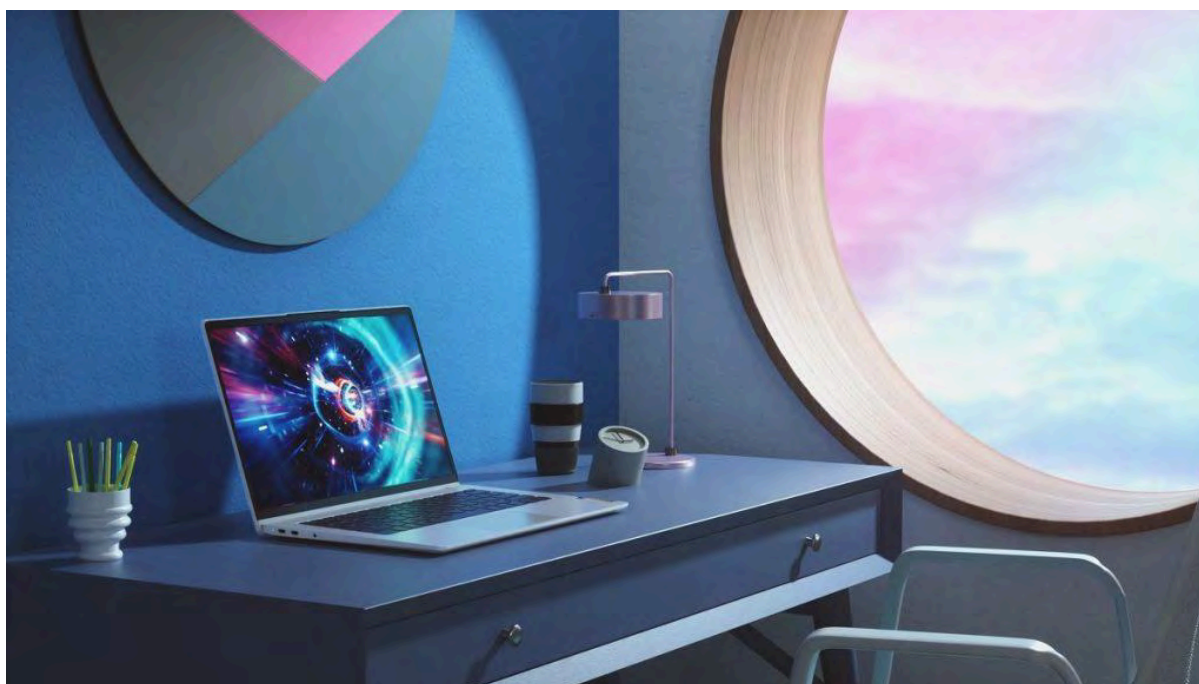
Si bien algunos empleados pueden ser algo descuidados o desconocedores de los peligros que acechan en la red, **sus herramientas del trabajo no deben ser igual de descuidadas que sus dueños.** En el mundo laboral actual, completamente digitalizado, los ordenadores portátiles de los trabajadores **deben estar diseñados con un firmware robusto y seguro** para dar soporte a la ciberseguridad.

**El Director General de Lenovo en Singapur, Nigel Lee,** hizo hincapié en la necesidad de contar con una conectividad sólida en los dispositivos de trabajos personales, ya que **se espera que el 75% de los datos se generen fuera de la oficina para 2025.** Puntualizó, también, la **importancia de aplicar también los mejores parámetros de ciberseguridad para aquellos ordenadores portátiles que**



respaldan la productividad en entornos de trabajo híbrido -ofrecen la capacidad 5G, tarjetas eSIM y una conectividad perfecta con la nube-.

Recordemos un principio básico de la ciberseguridad: **“cuanto mayores facilidades nos brinde una tecnología, mayores serán las consecuencias de su crackeo”**. El mismo principio se aplica en este caso con el **avance de las tecnologías de conectividad de los portátiles**. Para asegurar al máximo la seguridad de los empleados y sus dispositivos, existe una guía del INCIBE -Instituto Nacional de Ciberseguridad- que es **realmente instructiva respecto a normas y recomendaciones a seguir para asegurar un desarrollo del trabajo sin riesgos**.



## Aspectos básicos para un trabajo ciberseguro

La anteriormente citada '[Guía para el trabajo ciberseguro](#)' de INCIBE profundiza en varios aspectos que por normas de extensión este artículo no puede abarcar, pero sí esperamos dar las suficientes pinceladas como para llamar tu atención como empresario o empleado -también como mero lector- en cuanto a **políticas de ciberseguridad que puede implantar para evitarse cualquier tipo de susto.**

- **Red privada virtual o VPN:** utilizar una VPN es fundamental para asegurar la privacidad y seguridad de las comunicaciones en línea. Al conectarte a través de una VPN, tus datos se cifran y se canalizan a través de servidores seguros, evitando que los ciberdelincuentes puedan espiar tus comunicaciones o interceptar información sensible. Además, la VPN oculta tu dirección IP real, lo que proporciona un nivel adicional de anonimato y protección.
- **VPN + escritorio remoto:** al utilizar el escritorio remoto para acceder a computadoras o servidores en la oficina, es esencial hacerlo a través de una conexión VPN. Esto asegura que la comunicación entre tu dispositivo y el escritorio remoto se realice de forma segura, evitando riesgos derivados de vulnerabilidades o configuraciones inadecuadas que puedan ser explotadas por atacantes.
- **Dispositivos personales:** si se permite el uso de dispositivos personales para trabajar, es esencial





establecer una política BYOD -Bring Your Own Device- clara y estricta. Los empleados deben seguir las pautas establecidas para garantizar que sus dispositivos personales cuenten con las medidas de seguridad adecuadas antes de conectarse a la red corporativa. Esto puede incluir el uso de software de seguridad actualizado y el cifrado de datos sensibles. Si no cuentas con esta política BYOD, debes ponerte manos a la obra al respecto.

## Aspectos adicionales para un teletrabajo ciberseguro

- **Crea un entorno de trabajo seguro:** ya sea que trabajes desde casa o en una oficina, es fundamental respetar la política de protección del puesto de trabajo establecida por la empresa. Esto incluye medidas como mantener tu área de trabajo física segura y protegida, no dejar dispositivos desatendidos y cerrar sesión y bloquear la pantalla cuando no estés utilizando el ordenador. Un básico, pero siempre debe estar presente.
- **Protege tu conexión a Internet:** preferiblemente, utiliza la red doméstica para trabajar, ya que suele ser más segura que las redes Wi-Fi públicas. Las redes Wi-Fi públicas pueden ser vulnerables a ataques de crackers, por lo que es mejor evitarlas para tareas sensibles o confidenciales. Siempre que sea posible,

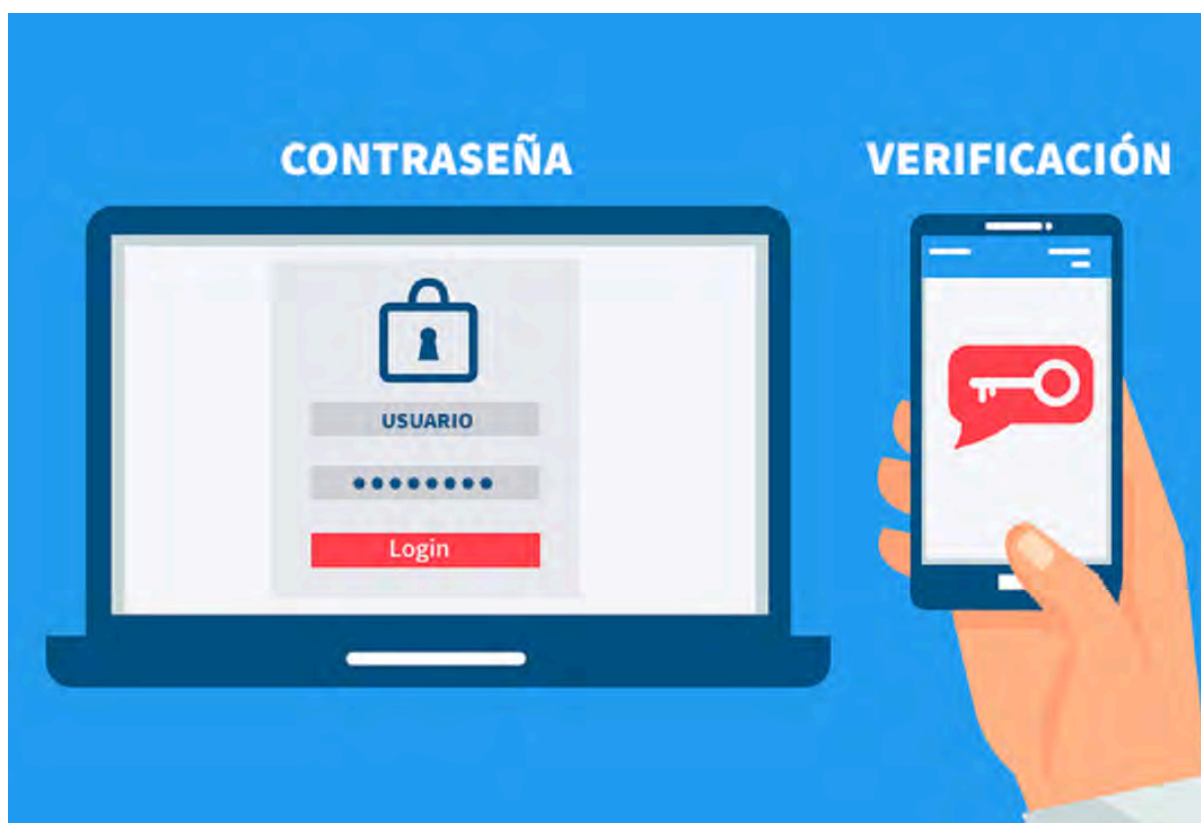


utiliza una conexión a Internet segura y protegida para mantener la integridad de tus datos y comunicaciones.

- **Red de datos móvil como plan B:** si no es posible utilizar la red doméstica o cualquier otra red considerada segura como alternativa, la red de datos móvil 4G o 5G puede ser una opción de respaldo. Asegúrate de tener una buena cobertura y considera el uso de una conexión VPN para agregar una capa adicional de seguridad cuando te conectes a través de datos móviles.

# PASO A PASO: QUÉ DEBES HACER SI HAN ROBADO TUS DATOS

Los expertos de Kaspersky, una de las compañías insignias de la industria de la ciberseguridad y la privacidad digital, han compartido los pasos que debes seguir una vez que tus datos se hayan visto envueltos en una filtración.



En la era digital actual, las fugas de datos y los robos de información personal son cada vez más frecuentes. Todos

hemos sentido la **preocupación de no saber en manos de quién está nuestra información más personal**, como también todos hemos sentido la necesidad de **tomar medidas para protegernos y evitar volver a sentir esa sensación**.

Si alguna vez te encuentras en la **desafortunada situación en la que tus datos personales han sido robados y expuestos en público**, es fundamental actuar con rapidez y seguir una serie de pasos para mitigar los daños y proteger tu identidad.

Los **expertos de Kaspersky compartieron con nosotros una serie de consejos** para hacer frente a esta situación y proteger tus datos personales de la forma más efectiva.

Toma nota:

## 1. Cambiar las contraseñas

Puede parecer más que obvio, pero muchos lo pasan por alto. En caso de una fuga de datos, es **crucial cambiar tus contraseñas tan pronto como sea posible**. Si utilizas la misma contraseña en diferentes servicios, será importantísimo modificarla en todos ellos.

Los expertos de Kaspersky, incluso, **recomiendan emplear un gestor de claves** -como Avira Password Manager o Bitwarden- que facilite la creación y gestión de contraseñas seguras para evitar caer en códigos fáciles de adivinar.

## 2. Extremo cuidado con el *phishing*

Los ciberdelincuentes pueden intentar aprovechar la situación enviando **correos electrónicos fraudulentos haciéndose pasar por contactos legítimos** -como entidades bancarias o Correos- y solicitando que cambies la contraseña a través de un enlace malicioso.

Es esencial **evitar hacer clic en enlaces sospechosos y acceder directamente al sitio web del servicio para cambiar la contraseña**. Si quieres saber más sobre el phishing, te recomendamos [este artículo](#).

## 3. Siempre elegir empresas confiables

Siempre es importante **investigar y seleccionar cuidadosamente las empresas con las que compartes información personal**. Si estás buscando un proveedor de VPN u otros servicios, verifica su reputación, experiencia y certificaciones de análisis independientes antes de confiarles tus datos. Haz una búsqueda lo más exhaustiva posible averiguando si alguien se ha visto envuelto en problemas de estafas con la compañía.

## 4. Comenzar a utilizar autenticación en dos pasos

Es, sin duda, una de las herramientas más valoradas a la hora de protegerte en la red. Si alguna **aplicación o dominio**

**web te propone utilizar autenticación de doble factor para reforzar la contraseña, no dudes en aceptar;** ya que añade una capa adicional de seguridad de mucho valor.

Cada vez que entres a la aplicación o web desde un dispositivo desconocido, se te solicitará un código único enviado a tu correo o teléfono antes de permitir el acceso a tu cuenta, lo que **aleja a la gran mayoría de crackers.**

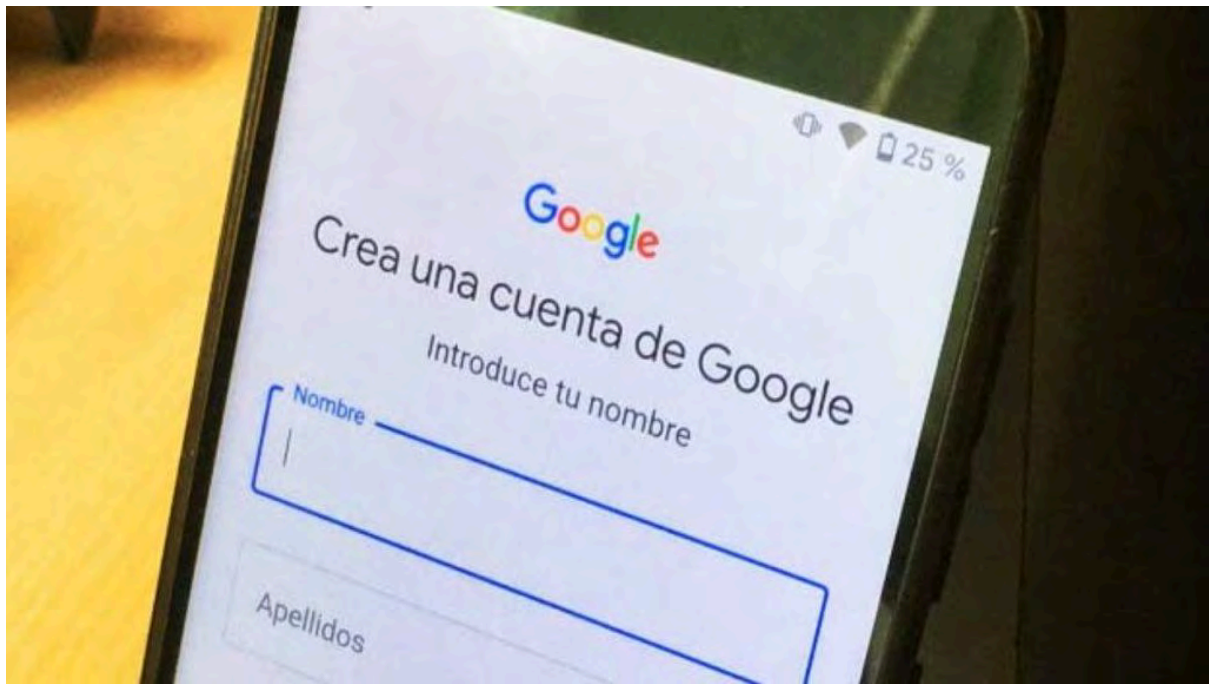
## **5. Bloquear tarjetas bancarias**

Si tus datos bancarios han sido comprometidos, bloquea tu tarjeta de inmediato y solicita una nueva. También, deberás **evitar almacenar información de pago en cualquier sitio web e incluso en tu propio auto** para prevenir futuros robos.

## **6. Eliminar las cuentas comprometidas**

Si ya no necesitas el servicio en el que has experimentado la fuga de datos, **lo más recomendable es que elimines la cuenta y solicites también la eliminación de toda la información** que haya recogido la web o aplicación sobre ti.

## **7. Compartir datos mínimos**



Como recomendación para evitar situaciones como esta en el futuro, **deberás limitar la cantidad de información personal que compartes con diferentes servicios y plataformas**, especialmente evitando proporcionar detalles como el domicilio o nombre real si no es estrictamente necesario. **Rellena únicamente los campos que están marcados como obligatorios**; recuerda que cuantos menos datos compartas, más segura estará tu información.

Bonus: Si sospechas que el ataque no ha sido fortuito y has podido ser víctima de un ataque especialmente dirigido, deberás contactar con el soporte técnico de inmediato, sacar capturas de pantalla para documentar la intrusión y utilizar una solución VPN confiable que te ayude a reducir riesgos de fuga de datos, ocultando tu huella digital.



# QUÉ ES EL PRETEXTING Y CÓMO INTENTARÁ ENGAÑARTE SI TRABAJAS EN UNA EMPRESA

Siempre se ha dicho que confiar es algo bueno... pero olvídate de esa máxima cuando te enfrentes a cualquier pantalla y al mundo digital. En esas situaciones, la cautela y el sentido común te pueden ahorrar problemas muy serios.



Imagina que recibes una llamada de alguien que se hace pasar por un colega de trabajo, un agente de policía, un empleado de tu banco o, incluso, un miembro de una



organización no gubernamental. Te piden datos personales, números de cuenta o información sensible. **¿Qué harías?**

**El pretexting es un elaborado juego de manipulación psicológica que los estafadores emplean para engañar a sus víctimas** y obtener acceso a información valiosa.

Utilizando una voz firme y decidida, tono serio y una habilidad excepcional para improvisar, estos delincuentes simulan tener la autoridad necesaria para solicitar datos personales.

Un caso llamativo ocurrió en 2020, cuando un grupo de impostores se hizo pasar por representantes de agencias de modelos y servicios de acompañantes. Utilizando **entrevistas falsas y antecedentes inventados**, lograron que mujeres, incluyendo adolescentes, les enviaran fotografías desnudas. Estas imágenes luego fueron vendidas a la industria pornográfica, generando enormes ganancias para los estafadores.

La clave para no caer en la trampa del pretexting es mantenerse siempre alerta y conscientes de los métodos utilizados por los atacantes. **Nunca debemos compartir información personal o sensible con alguien que no podamos verificar** completamente. Es esencial **estar informados y preparados** para **proteger nuestra privacidad y seguridad** en un mundo cada vez más digital.

**Pero, ¿qué técnicas de pretexting existen?**

En realidad, hay varias, siendo las siguientes algunas de las más comunes:



1. **Phishing:** Esta técnica consiste en enviar **correos electrónicos falsos** para obtener información personal, como nombres de usuario, contraseñas o datos bancarios. El objetivo principal del pretexting es establecer la confianza con las víctimas, enviándoles correos electrónicos falsificados que aparentan provenir de entidades autorizadas. De esta manera, intentan engañar a las personas para que revelen información personal al hacer clic en enlaces maliciosos.
2. **Smishing:** Es similar al phishing, pero en lugar de utilizar correos electrónicos, los atacantes utilizan **mensajes de texto -SMS-** para realizar el engaño. La



palabra “smishing” es una combinación de “SMS” y “phishing”. En esta técnica, se busca generar mayor intimidación con la víctima, ya que los números de teléfono suelen ser más personales y se crea una conexión de confianza cuando se envían mensajes de texto relacionados con una entidad bancaria.

3. **Vishing:** Esta técnica también es una variante del phishing, pero se utiliza la voz para realizar el engaño. Los atacantes se hacen pasar por **servicios de atención al cliente o entidades legítimas a través de llamadas telefónicas**. En estas llamadas, el atacante emplea el tono y las preguntas adecuadas para obtener información sensible de la víctima. Esta técnica es especialmente efectiva con personas mayores que no están familiarizadas con el uso de correos electrónicos o mensajes de texto.

## Ahora que los conoces... cómo evitar sus ataques

Si deseas prevenir los ataques de pretexting y eres una marca de vehículos, es importante seguir algunas medidas de seguridad:

- Asegúrate de que todos los empleados **usen credenciales y distintivos de identificación** en las instalaciones de la empresa para evitar el acceso no autorizado.



- Enfócate en **eliminar las señales que puedan dar pistas sobre tus contraseñas**. Utiliza tecnología actualizada, gestión de credenciales y autenticación multifactorial para garantizar una protección de contraseñas adecuada.
- **No hagas clic en enlaces desconocidos** en correos electrónicos.
- Mantén tu **software antivirus actualizado**.
- Brinda a tus empleados **capacitación en concienciación sobre seguridad** para que estén preparados contra errores humanos.
- **Verifica siempre las llamadas, correos electrónicos y mensajes de texto** antes de realizar cualquier acción.

Además, sería una buena idea contar con un equipo de hackers éticos debidamente capacitados, quienes puedan anticiparse a posibles incidentes de seguridad. No está de más **capacitar a tu equipo de soporte de TI en la certificación de hacking ético**.

Existen certificaciones que cubren las últimas tecnologías y desafíos en ciberseguridad. Si estás interesado en obtener una certificación en hacking ético, **considera participar en programas de capacitación especializados**.

# POR QUÉ NO DEBES RESPONDER “SÍ” CUANDO ESTÁS TRABAJANDO Y TE LLAMAN AL TELÉFONO

La industria automovilística se enfrenta a un riesgo oculto en las llamadas telefónicas. Descubre por qué debes ser cauteloso al responder con un "sí" al teléfono y cómo evitar caer en una astuta estafa.



*Imagen generada por la IA de Bing*

En un mundo digital donde la información personal se ha vuelto más vulnerable que nunca, los profesionales de la

industria automovilística se enfrentan a un peligro silencioso en las llamadas telefónicas. En este artículo, te contamos por qué es crucial evitar responder con un simple “sí” al teléfono **y cómo protegerte de una estafa que acecha en la era de la comunicación digital.**

## El “Fraude del ‘Sí’”: ¿Qué es y cómo funciona?

Imagina esta situación: te encuentras en tu oficina en una destacada empresa automovilística y, de repente, el teléfono suena. Del otro lado de la línea, un supuesto representante de una entidad de renombre te hace preguntas que parecen inofensivas, como “¿trabaja usted en [nombre de tu empresa]?” y, sin pensar, respondes con un “sí”. **Sin embargo, este acto aparentemente trivial podría desencadenar una serie de problemas.**

## Desglosando el engaño

### Paso 1: La llamada inicial

El estafador se hace pasar por un empleado legítimo de una entidad confiable, tal vez un banco o un proveedor de servicios vinculado a tu empresa. Su objetivo es ganarse tu confianza utilizando información que parece auténtica.

### Paso 2: Diálogo engañoso



Inician una conversación amigable y aparentemente inocua contigo, haciendo preguntas diseñadas para obtener respuestas afirmativas, como “¿está usted autorizando transacciones en este momento?” o “¿podría confirmar su nombre?”.

### **Paso 3: El momento crucial**

Cuando obtienen ese preciado “sí”, lo registran. Esta grabación de voz puede utilizarse para autorizar transacciones financieras, formalizar contratos o, peor aún, falsificar tu identidad.

## **Cómo protegerse en la industria de la automoción**

### **¿Qué medidas se deben tomar?**

1. **No ceder ante el “Sí” fácilmente:** Mantén una actitud cautelosa al responder llamadas telefónicas, incluso si parecen genuinas. No compartas información personal a menos que estés absolutamente seguro de la autenticidad de la llamada. Por cierto, siempre puedes decir “ahá” o similar para asentir a una pregunta o cuestión.
2. **Verifica la identidad:** Siempre verifica la identidad del interlocutor. Si tienes la menor duda, busca el número oficial de la entidad y llámalos directamente.



3. **Vigila tus transacciones:** Mantén un registro detallado de tus transacciones financieras y denuncia cualquier actividad sospechosa de inmediato.
4. **Controla tu presencia en línea:** Realiza búsquedas periódicas sobre ti en línea y configura alertas para detectar menciones no autorizadas de tu nombre.
5. **Cambia tus contraseñas:** Si has sido víctima de esta estafa, cambia tus contraseñas y códigos de seguridad relacionados con cuentas comprometidas.
6. **Documenta evidencias:** Conserva pruebas, como números de teléfono y grabaciones de llamadas, en caso de que necesites presentar una denuncia.

## **Toque de atención para los trabajadores automovilísticos**

La industria de la automoción no está exenta de estos peligros. A medida que los estafadores se vuelven más astutos, es vital que todos los profesionales en esta área estén alerta y conscientes de los riesgos asociados con un simple “sí” al teléfono. **La seguridad de tus datos y tu identidad están en tus manos**, y protegerlos debe ser una prioridad constante en el entorno digital actual.



# POR QUÉ ES IMPORTANTE TENER CUIDADO CON EL MÓVIL QUE CONECTAS AL VEHÍCULO

En esta época tan digitalizada y conectada, es más que común enlazar tu móvil inteligente con tu vehículo. Esto puede entrañar ciertos riesgos, así que debes actuar con precaución. ¿Cuáles son esos problemas y cómo evitarlos?



En la era digital en la que vivimos, los teléfonos móviles se han convertido en una parte indispensable en la vida de todos. Los utilizamos para comunicarnos, para acceder a información, jugar a juegos, sacar cientos de fotos o vídeos y realizar tareas del trabajo o el estudio. Además, **la integración de los teléfonos móviles con otros dispositivos conectados, como en el caso de los**

**automóviles**, ha brindado una mayor comodidad y posibilidades a la experiencia frente al volante.

Sin embargo, es **importante tener precaución al conectar tu teléfono móvil a la parte multimedia de un auto** La comodidad que brinda la conexión entre dispositivos no quita la existencia de ciertas vulnerabilidades que podrían comprometer tu seguridad y privacidad. En los siguientes párrafos, **analizaremos algunas investigaciones recientes que revelan riesgos asociados de esta práctica.**

Según un estudio realizado por **el grupo de defensa al consumidor británico Which?**, se descubrió que **varios teléfonos Android con tecnología de reconocimiento facial pueden ser engañados fácilmente con la impresión de una fotografía.** Esto plantea preocupaciones más que significativas, ya que algunos automóviles permiten el desbloqueo y arranque del vehículo mediante el reconocimiento facial del propietario -el Genesis GV60, por ejemplo-. Si un sistema de reconocimiento facial vulnerable está vinculado a tu teléfono y, a su vez, conectado al automóvil, podrías enfrentarte a un riesgo de acceso no autorizado a tu vehículo.



*El Genesis GV60, primer auto con apertura de puertas mediante reconocimiento facial*

Además, otro estudio realizado por investigadores de Tencent Labs y Zhejiang University reveló una **nueva técnica de ataque llamada 'BrutePrint'**. Este método utiliza **ataques de fuerza bruta para descifrar huellas dactilares en smartphones modernos** y así evadir la autenticación del usuario y tomar el control del dispositivo.

Los investigadores demostraron que esta técnica **puede superar los límites de intentos y detección de vida activa que protegen contra ataques de fuerza bruta**. Al explotar vulnerabilidades específicas, lograron realizar **intentos ilimitados en dispositivos Android y HarmonyOS, y hasta diez intentos adicionales en dispositivos iOS**. Si un atacante logra comprometer la seguridad de tu teléfono móvil y está vinculado al sistema de tu automóvil, podría obtener acceso sin ninguna restricción al vehículo.

Por otro lado, **la seguridad de las huellas dactilares también es un tema de preocupación**. Se encontró que en algunos dispositivos **Android los datos biométricos**

**almacenados en los sensores de huellas dactilares no estaban protegidos de forma adecuada.** Esto podría permitir ataques de intermediarios -MITM, los ataques 'Man In The Middle'- para secuestrar las imágenes de las huellas dactilares. Si un atacante intercepta la imagen de la huella digital y tiene acceso al sistema de tu automóvil, podría utilizarla para desbloquear el vehículo sin tu consentimiento.

## **Haz esto para evitar los peligros del ciberataque**

Estos hallazgos resaltan la importancia de tener cuidado al conectar tu teléfono móvil al sistema de tu auto. A continuación, se presentan algunas **recomendaciones para proteger tu seguridad y privacidad:**

- Mantén **actualizado tanto el software de tu teléfono móvil como el del sistema de tu automóvil.** Las actualizaciones suelen incluir parches de seguridad que solucionan vulnerabilidades conocidas. Es el gran cliché, pero siempre sirve de ayuda.
- Utiliza **contraseñas o patrones de desbloqueo seguros en tu teléfono móvil.** Evita patrones sencillos o contraseñas predecibles que puedan ser adivinadas fácilmente. Sobre todo no repliques la misma contraseña para todos tus dispositivos.  
[Aprende a tener la contraseña más segura aquí.](#)
- **Limita las conexiones inalámbricas.** Siempre que sea posible, utiliza una conexión por cable para



conectar tu teléfono móvil al sistema del automóvil en lugar de utilizar la conexión Bluetooth, que **suele entrañar muchos más riesgos.**

- **Investiga antes de instalar aplicaciones desconocidas.** Asegúrate de que las aplicaciones que descargas en tu teléfono móvil sean de fuentes confiables y estén debidamente verificadas. Las aplicaciones maliciosas pueden comprometer la seguridad de tu dispositivo y, potencialmente, afectar la conexión con el sistema del automóvil.
- Considera el **uso de soluciones de seguridad adicionales** – antivirus, servicios de protección en la nube... -. Existen aplicaciones y programas de seguridad diseñados específicamente para proteger los teléfonos móviles contra ataques y malware. Investiga y elige una solución confiable que se adapte a tus necesidades.
- **No compartas información sensible a través de la conexión con el automóvil.** Evita transmitir datos personales, como números de tarjetas de crédito o contraseñas, a través del sistema del automóvil mientras tu teléfono móvil esté conectado.

Recuerda que la seguridad y privacidad son aspectos fundamentales en la era digital. Al ser consciente de los riesgos asociados con la conexión de tu teléfono móvil al sistema del automóvil, puedes tomar medidas para proteger tus datos y prevenir accesos no autorizados. **Mantente siempre informado sobre las últimas investigaciones y recomendaciones de seguridad** -aquí en [HackerCar](#) podrás



encontrarlas- y toma decisiones informadas para proteger tus dispositivos e información personal.

## QUÉ HACER ANTES DE TIRAR ESE CELULAR QUE USASTE EN TU VEHÍCULO

¿Te vas a deshacer de tu viejo móvil? Deberías plantearte qué pasa con los datos que ha ido acumulando durante toda su vida útil. ¿Y qué pasa con la tarjeta de memoria? ¿Y la SIM? Lo mejor es que sigas estos consejos.

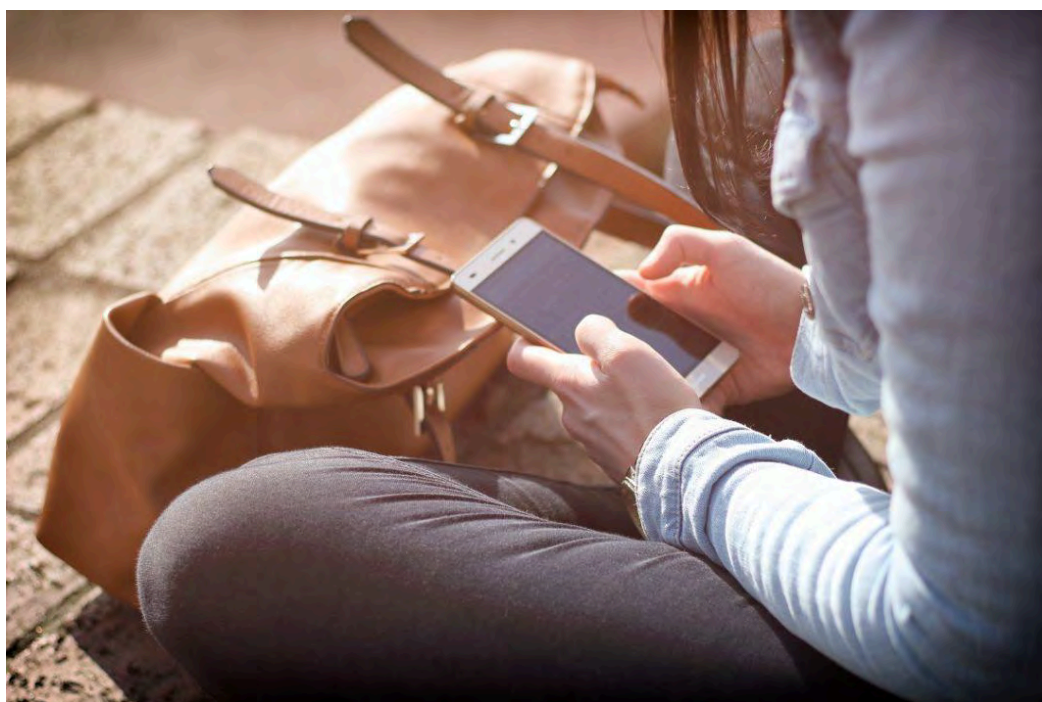


Photo by Tofros.com from Pexels



Imagina que tienes un diario con todos tus secretos y que un día decides deshacerte de él, o hacer lo propio con un álbum de fotos o con ese ordenador en el que tienes multitud de documentos. Seguro que antes los vaciarías o destruirías su contenido. **¿Deberías de hacer lo mismo cuando tiras un móvil?**

## ¿Qué sabe tu celular de ti?

Es algo habitual: **cualquier teléfono que manejas está repleto de información.** El tuyo propio, el de empresa o uno que compraste de forma personal, pero también lo acabaste utilizando en el trabajo. A lo largo de su vida útil, **los teléfonos** van recopilando datos del usuario, que se acumulan con el uso normal. **¿Qué tipo de información puede llegar a almacenar tu móvil?** Según el **Instituto Nacional de Ciberseguridad -INCIBE-**, esta:

- Lugar de residencia, trabajo y detalles de movilidad.
- Información de contactos, con independencia de que sean clientes, compañeros, familia, etc.
- Historial de llamadas, tanto entrantes como salientes, mensajes de voz o llamadas perdidas.
- Conversaciones de mensajería instantánea o chats en redes sociales.
- Historial de navegación, de búsqueda, cookies y páginas en memoria caché.
- Fotos, vídeos y grabaciones de audio.



- Contraseñas almacenadas y acceso a cuentas, ya sean en redes sociales, de acceso a plataformas de pago, cuentas bancarias o cualquier servicio online.
- Acceso a aplicaciones de uso profesional, como gestión de pedidos, albaranes, facturación, etc.
- Acceso a firmas electrónicas y cuentas de correo.

Es decir, se trata de mucha **información a la que podría tener acceso alguien que se haga con tu móvil después de que lo hayas desechado**. ¿Por qué proteges tu teléfono con una contraseña o con un patrón de desbloqueo? Para que nadie acceda a todo lo anterior sin que tú lo sepas, ¿no? Pues algo similar deberías plantearte cuando dejes de utilizarlo y decidas donarlo, venderlo, regalarlo o tirarlo.

## ¿Cómo borrar los datos?

A la hora de limpiar el móvil de todo rastro personal que hayas podido dejar, debes tener en cuenta que **no es suficiente con borrar algunas fotos o unas cuantas aplicaciones**. Aunque lo hagas, esa información podría recuperarse, por lo que la mejor opción es que realices una **restauración del dispositivo a sus valores de fábrica**. Lo que se conoce popularmente como “reseteo”.

Se trata de un borrado total, sin opciones de recuperación. Como el nombre indica, deja el teléfono con tantos datos como tenía cuando salió de la tienda el primer día. Por ello, **antes de ejecutar ese “reseteo”, conviene que guardes en la nube los archivos que te interese conservar**.



Una vez copiados los archivos, estos son los pasos que debes seguir para restaurar los valores de fábrica del teléfono, ya sea un móvil con [sistema operativo IOS](#) o [uno con Android](#).

## Dispositivos Apple IOS

Ve al menú de ajustes, pincha en “General”, accede a “Reestablecer” y ahí selecciona “Borrar contenido y ajustes”.



## Dispositivos Android

Ve al menú de ajustes, pincha en “Sistema”, accede a “Restablecimiento” y ahí elige “Restablecer datos de fábrica”.



## ¿Qué pasa con la tarjeta SIM?

También puede darse el caso de que necesites cambiar la tarjeta SIM de tu operador -es la que permite el intercambio de voz y datos-. Si estás en esa situación, **también deberías deshacerte de ella debidamente** para evitar que alguien

tenga acceso a los datos que almacene. En este caso, el proceso de eliminación es menos sofisticado: **basta con que la destruyas físicamente.**

**Ese mismo proceso de eliminación es el recomendado para las tarjetas SD**, esas que amplían la memoria de algunos dispositivos móviles. Antes de romperla, es recomendable volcar todo su contenido en un nuevo dispositivo -si no quieres perderlo para siempre- y posteriormente borrarlo de la tarjeta.

Medidas sencillas, pero necesarias para no que no comprometan tu información personal o profesional.

## **CÓMO EVITAR QUE TU CELULAR CAUSE UN PROBLEMA DE CIBERSEGURIDAD EN TU AUTO**

Coches y móviles están ahora más unidos que nunca. Pero debes aplicar varias medidas de ciberseguridad para que esa conectividad no termine en un ataque. Estas son las principales recomendaciones a seguir.



Foto: Piqsels.

Lejos quedan los tiempos en los que todo lo que se podía hacer con el móvil dentro del auto era conectarlo al Bluetooth para poder recibir llamadas sin usar las manos.

Con la expansión de la conectividad, tanto en los vehículos como en los smartphones, esas posibilidades se han multiplicado. Surge así **un mundo de posibilidades y servicios que permiten controlar funciones del auto a través del móvil y viceversa.**

Pero como todo lo que tiene que ver con la conectividad informática, esas posibilidades no están exentas de riesgos de ciberseguridad. Un pirata informático podría ‘colarse’ en esas comunicaciones y manipularlas, lo que podría generar numerosos problemas para los ocupantes del vehículo o el dueño del teléfono.

## ¿Cuáles son esas amenazas que podrían afectar a la conexión móvil-auto y qué puedes hacer para evitarlas?

Esto nos han contado desde el Área Técnica de [EUROCYBCAR](#).

## ¿Qué puedes hacer con el móvil en el auto?

Mucho ha cambiado la relación auto-móvil desde que se hizo habitual la conexión por Bluetooth hace una década.

Actualmente, los smartphones pueden interactuar con los vehículos a través de las siguientes tecnologías:

- **Bluetooth:** La forma más extendida. Conecta auto y móvil de forma inalámbrica para poder realizar, entre otras funciones, llamadas manos libres y reproducir música desde el smartphone a través de los altavoces del vehículo.
- **Wifi:** Tener [un punto Wifi a bordo del vehículo](#) permite ofrecer una conexión Internet inalámbrica para conectar smartphones, tablets o cualquier dispositivo que permita acceder a Internet. De esta forma, los pasajeros podrán acceder al correo electrónico, descargarse documentos, reproducir música, ver series o películas, utilizar juegos online... Todos estos sistemas están optimizados para funcionar mientras el auto está circulando, de tal forma que recibas la señal de Internet más intensa y fiable posible -algo que no siempre sucede si usamos la conexión de datos de nuestro propio móvil-. Esta conexión puede realizarse





de dos formas: mediante una tarjeta SIM incluida en el auto, o compartiendo datos desde un teléfono para que el auto amplifique la señal.

- **Android Auto, Apple CarPlay y Mirror Link:** Estos tres sistemas sirven para lo mismo: proyectar en la pantalla central del vehículo ciertas aplicaciones del móvil que podrían ser útiles durante la conducción. Esta conexión puede realizarse de forma física con un cable USB o de forma inalámbrica a través de Bluetooth.
- **Aplicaciones:** La mayoría de marcas ya ofrecen una aplicación para el móvil. Con ella, los propietarios pueden controlar desde su smartphone ciertas funciones del vehículo. Algunas de las más habituales son el encendido y apagado de la climatización o del motor, apertura y cierre de puertas y conocer la posición exacta donde está el auto. Algunas incluso permiten restringir la velocidad máxima a la que circula el automóvil -en caso de que se lo prestes a alguien y no quieras que corra- o aparcarlo de forma remota. Estas apps también suelen ofrecer información sobre el vehículo: consumo, recorridos realizados, historial de mantenimiento, etc.
- **Cargadores móviles inalámbricos:** Después de usar tanto el móvil, es normal quedarse sin batería. Las marcas solucionaban esto con diversos puertos USB repartidos por el habitáculo, pero han empezado a sumar unas bandejas donde el smartphone se recarga de forma inalámbrica al depositarse sobre ellas -siempre que el móvil sea compatible con esta tecnología-.

Si quieres saber qué otras curiosas funciones puedes manejar de tu auto desde el móvil, puedes leer [este artículo](#).

## Riesgos y precauciones

Hasta el momento, todo son ventajas. Esas tecnologías mejoran la comodidad a bordo y brindan interesantes funcionalidades. Pero, como siempre sucede a la hora de hablar de conectividad, hay que tener en cuenta que podemos encontrarnos problemas de ciberseguridad. Y es que un uso descuidado de dichas tecnologías podría desembocar en un ciberataque que comprometa la seguridad de los pasajeros a bordo.

No obstante, hay ciertas medidas que pueden aplicar los conductores y sus acompañantes a la hora de conectar el móvil en el vehículo para evitar esos peligros.

### En el auto

- **Cambia la contraseña del Wifi y del Bluetooth.** Estas tecnologías suelen establecer una clave de seguridad como paso intermedio para permitir la conexión entre auto y móvil. Pero resulta muy conveniente cambiar esa contraseña periódicamente. ¿Por qué? **Si no lo haces, todo dispositivo que se haya conectado alguna vez podrá hacerlo de nuevo sin tu permiso.** Además, esa clave deberá de ser difícil de adivinar. Y cuando no se estén usando,



conviene apagar tanto el Bluetooth como el Wifi para evitar que esas redes sean detectables desde el exterior y que un ciberdelincuente las localice.

- **Protege las tomas USB del auto.** Para que nadie conecte en tu automóvil un dispositivo sin tu permiso, lo mejor es que bloquee los puertos USB con un tapón con llave. De esta forma, solo tú podrás conectar dispositivos en esas tomas y así evitarás que un smartphone infectado con un virus se conecte a tu auto. Por unos 20€, puedes hacerte con un [kit de estos bloqueadores](#) en sitios web como Amazon.
- **Ten el software de tu auto siempre actualizado.** Algunas marcas, como Tesla, envían esas actualizaciones de forma remota gracias a Internet, pero otras las hacen de forma presencial en los talleres oficiales. De una forma o de otra, este método sirve para corregir problemas de seguridad que haya detectado el fabricante, porque en esa nueva versión estará instalado un parche que corrija el problema.

## En la tablet o el móvil

- **Aplicaciones siempre actualizadas.** A la hora de usar la app oficial de una marca, hay que seguir las mismas precauciones que con cualquier otra app móvil. Esto es, descargarla siempre de las tiendas oficiales -como Google Play o App Store- para evitar falsificaciones que puedan contener [malware](#) y tenerlas siempre actualizadas a la última versión -las





actualizaciones son el método que tienen los desarrolladores para corregir vulnerabilidades de seguridad detectadas-.

- **Instala un antivirus.** Los móviles y las tablets, al igual que los ordenadores, pueden infectarse con un virus. Si un dispositivo infectado se conecta posteriormente en el auto, el ataque podría transferirse del primero al segundo. Por tanto, hay que estar seguro de que todo lo que se vincule al vehículo es ciberseguro, y un antivirus aporta tranquilidad en esa labor.
- **Evita comportamientos de riesgo.** Hay muchas formas de caer en la trampa de un ciberdelincuente al usar un móvil o tablet. Por ejemplo, no debes descargar o pinchar en ningún enlace que recibas por correo electrónico si no estás completamente seguro de que el emisor es de confianza -para evitar caer en un ataque de **phishing**-, y no debes conectarte a redes Wifi públicas. Tampoco es recomendable que **anules las restricciones del fabricante**, porque están pensadas para hacer que tu dispositivo funcione correctamente sin riesgos de seguridad.

# EL PROBLEMA DE PRIVACIDAD AL QUE TE ENFRENTAS SI VENDES TU AUTO-Y CÓMO SOLUCIONARLO-

Tu auto sabe mucho sobre ti. Por eso, cuando vayas a deshacerte de él, hay una cuestión que debes de tener en cuenta para no tener más tarde un problema de privacidad.



Una empresa estadounidense -Privacy 4 Cars- que trabaja con concesionarios de autos ha descubierto una realidad preocupante detrás de las ventas de vehículos de segunda mano: en la mayor parte de los concesionarios donde ha

trabajado, **los automóviles en venta aún contenían datos privados de sus anteriores propietarios.**

¿Cómo es eso posible? La respuesta, en realidad, es bastante sencilla. El problema está en los **sistemas de infoentretenimiento** de los autos. Estos equipos, cuyo rasgo más visible suele ser una **gran pantalla en el centro del salpicadero**, gestionan el ordenador de a bordo, el navegador, el equipo de sonido o los elementos de conectividad -teléfono, puertos USB o redes Wifi-.

Dada la variedad y complejidad de funciones que aúnan, **estos sistemas recopilan numerosos datos personales del conductor y sus acompañantes** durante todo el ciclo de vida del auto.

## Todo lo que tu auto sabe sobre ti

Privacy 4 Cars pone el foco, sobre todo, en el **teléfono móvil**. Al conectar el smartphone al vehículo, el primero transmite al segundo diversos datos que permiten al sistema multimedia gestionar el smartphone. Entre las informaciones transferidas, las más habituales son la agenda de contactos, el historial de llamadas y el registro de mensajes. Pero, dependiendo de cómo haya usado el conductor su smartphone en el auto, a esos datos podrían añadirse los correos electrónicos y los mensajes de WhatsApp.

“Cuando las personas conectan su teléfono al automóvil, lo que probablemente no se dan cuenta es que están creando

un mini clon de su teléfono dentro del vehículo”, dijo Andrea Amico, director de Privacy 4 Cars, en declaraciones recogidas por [ABC 7](#).

Incluso se pueden dejar almacenadas las direcciones donde vive, trabaja o visita el usuario, por culpa de que el navegador puede guardar el historial de las localizaciones que se han introducido.

## Cómo hacer un borrado de datos en el auto

Eso no supone un problema mientras el dueño del vehículo sea la misma persona cuyos datos almacena el sistema multimedia. Pero, cuando este se deshace del auto, ya sea vendiéndolo o llevándolo a un desguace, debe **tomar determinadas medidas para borrar de él toda su información personal**. De lo contrario, podría acabar en manos ajenas.

Y, más allá de un vehículo propio, esto mismo sucedería al alquilar o usar un auto ajeno. Quien se suba detrás, podrá ver toda esa información navegando por la pantalla central. ¿La solución? **Borrar esos datos**. Los sistemas multimedia tienen varias opciones para ello. El experto en ciberseguridad [Alejandro Aliaga](#) explicaba cómo hacerlo en este vídeo:

Por otra parte, los expertos en ciberseguridad de [EUROCYBCAR](#) también coinciden en que después de haber vinculado un móvil con el vehículo se debe eliminar el



dispositivo del listado de teléfonos emparejados. **También es conveniente hacer lo propio con los destinos del sistema de navegación...** si es que lo has estado utilizando y has dejado almacenados una serie de 'últimos trayectos'. Incluso hay algunos modelos, como los de Hyundai y Kia, que ya permiten incluso grabar notas de voz: por supuesto, accede al menú correspondiente si has tenido que utilizar esta función.

Otra opción a tener en cuenta, y que puede agilizar todo el proceso, es que desde el sistema [multimedia](#) busques la opción de 'restaurar a los valores de fábrica', una alternativa que seguramente te suene más de dispositivos como móviles u ordenadores, pero que en el caso del vehículo puede servir para borrar información que pueda poner en riesgo tu privacidad.

## **CÓMO BLOQUEAR TODOS TUS DISPOSITIVOS -INCLUSO EL MULTIMEDIA DEL AUTO-**

Cerrar la puerta, bajar la persiana, cerrar la ventana, echar el seguro... tu vida está llena de 'bloqueos' que garantizan tu privacidad y tu seguridad. ¿Por qué también es importante que lo hagas con tus dispositivos electrónicos, incluso los del auto?



Foto: Gerd Altmann en Pixabay.

Si tienes un móvil, una tablet e incluso un ordenador, sabrás que hay diversas manera de ‘bloquearlos’ de tal forma que algún desconocido, **ya sea en un descuido cuando lo dejas desatendido o directamente porque te lo ha robado**, pueda acceder a él y a su contenido.

Porque, queramos o no, perder uno de estos aparatos es ‘doloroso’ desde el punto de vista económico -por tener que volver a comprar uno para reemplazarlo-, **pero sobre todo puede ser preocupante si contiene información sensible**, preocupante, datos de acceso a cuentas bancarias, de correo, de plataformas de compra online...

Además, en el caso de un móvil, ahora quien tiene acceso a un teléfono que no esté protegido por un sistema de bloqueo podría entrar también en aplicaciones que tengas instaladas para controlar tu auto a distancia; sabiendo que algunas de



ellas permiten incluso abrir las puertas a distancia o comprobar tus recorridos, puede que no sea una buena idea dejar el móvil sin ningún tipo de protección.

Bloquear uno de estos aparatos se puede hacer de muchas maneras; por eso, la [OSI](#) ha elaborado una interesante guía que cuenta paso a paso cómo es dicho proceso, haciendo una distinción entre si el dispositivo es [Android o iOS](#).

En el caso de los primeros, el problema es que existen infinidad de marcas que utilizan este sistema operativo, existiendo además diversas versiones de ese Android; en todo caso, la operación para establecer el bloqueo suele coincidir en diversos pasos. En el caso que se ejemplifica, la [Oficina de Seguridad del Internauta](#) ha recurrido a un móvil de la firma Xiaomi.

“Para configurar el **bloqueo de pantalla** en nuestros dispositivos Android deberemos seguir los siguientes pasos, aunque pueden variar dependiendo de nuestra versión de Android y el modelo de nuestro *smartphone*.

Abriremos la aplicación ‘Ajustes’ -icono con forma de rueda dentada-, que podemos encontrar en el escritorio o en la pantalla de menú, y seleccionaremos la opción ‘Contraseña y seguridad’. Buscaremos la sección de ‘Seguridad’ y, a continuación, ‘Bloqueo de pantalla’.

Si pulsamos sobre ‘Contraseñas’, accederemos a los diferentes tipos de bloqueo de pantalla: Imagen Bloque de pantalla



**Patrón:** consiste en un dibujo trazado uniendo una serie de nueve puntos en forma de un cuadrado de 3×3. Es la opción menos segura, ya que cualquiera puede ver el trazo en la pantalla.

**PIN:** se trata de una clave de al menos 4 dígitos. Te recomendamos no utilizar el mismo PIN de la tarjeta SIM o la del banco.

**Contraseña:** se trata de una clave de al menos 4 dígitos y letras. Debemos utilizar una contraseña difícil de averiguar y única para el dispositivo.

Estas son las opciones universales, pero también hay otras que suelen ser normales en los dispositivos actuales, como:

**Desbloqueo con huella dactilar:** nuestro dispositivo dispone de un lector de huella dactilar. Puede utilizarse para que una o varias huellas dactilares desbloqueen nuestro móvil o tablet simplemente poniendo el dedo sobre el lector de la huella.

**Desbloqueo facial:** nuestro dispositivo es capaz de reconocer rostros mediante la cámara frontal. Podemos añadir nuestro rostro o el de otros usuarios como mecanismo de desbloqueo.

**Desbloquear con dispositivo Bluetooth:** podremos utilizar otro dispositivo inteligente para desbloquear nuestro móvil o tablet, como una pulsera de actividad o reloj inteligente.

Cuando hayamos escogido la opción deseada, preferiblemente las últimas opciones, deberemos seguir los pasos para configurarla e implementarla como mecanismo de desbloqueo. Nuestro dispositivo nos solicitará que configuremos más de un método de desbloqueo para poder utilizarlo en el caso de que el primero falle y como medida de seguridad extra”.

**En cuanto a los dispositivos tipo iPhone**, la **OSI** ha utilizado como ejemplo las opciones que permite un iPhone 11. El proceso de bloqueo que comentan es el siguiente:

Cuando adquirimos un dispositivo de la marca Apple (con el icono de una manzana), como un iPhone (teléfono) o un iPad (*tablet*), nos pedirá establecer un código de 8 cifras para desbloquearlo la primera vez que lo encendamos. Este código será la clave que necesitaremos para desbloquearlo cada vez que lo encendamos a partir de ahora.

En algunos modelos es posible utilizar nuestra **huella dactilar** o incluso el reconocimiento de nuestro **rostro** para proteger nuestro dispositivo. Podemos configurar estas medidas de bloqueo/desbloqueo siguiendo estos pasos:

“1. Accederemos a **‘Ajustes’** (icono de una rueda dentada), que podemos encontrar en el escritorio, y seleccionamos **ID de Apple > Contraseña y seguridad > Cambiar contraseña**. Desde aquí podremos cambiar la clave a una más robusta, estableciéndola como mínimo de 8 caracteres, incluyendo al menos una mayúscula, una minúscula y un número; por ejemplo: Milph0ne11.

2. Dentro de '**Ajustes**' buscaremos las opciones **Touch ID** o **Face ID** (en los modelos más nuevos). Dentro podremos:

- Activar el desbloqueo del iPad/iPhone.
- Añadir una nueva huella o nuestro rostro con alguna modificación.
- Solicitar el código -contraseña- como medida de seguridad adicional.

3. También podremos configurar el tiempo que el dispositivo estará inactivo antes de activarse el bloqueo automático. Para ello, iremos a **Ajustes > Pantalla y brillo**, donde encontraremos la opción de '**Bloqueo automático**'.

## ¿Y qué puedes 'bloquear' en un auto?

Todavía no es lo habitual... y, de hecho, lo normal es que quien tenga acceso al interior de un vehículo pueda conectar el dispositivo multimedia y navegar a su antojo por todas sus funciones y menús. Sin embargo, ya empieza a haber soluciones interesantes para que eso no suceda, tal y como nos han explicado desde el Área Técnica de [EUROCYBCAR](#).



Por ejemplo, muchos de los modelos de Toyota y Lexus ya cuentan con el llamado ‘modo portero’; no es algo muy sofisticado o complejo, **pero sí que permite bloquear el acceso al sistema introduciendo un código PIN de cuatro dígitos**. En el caso de estos autos, el proces para llevarlo a cabo es acceder a la zona de ‘configuración’, después en ‘vehículo’ y ahí aparece la opción ‘modo portero’.



Muy parecida es la solución que ofrece Ford con el denominado 'Modo Valet' dentro de sus sistemas **multimedia Sync3**, siendo el principio de funcionamiento muy parecido, tal y como recoge el manual de instrucciones del vehículo:

**“El modo de valet le permite bloquear el sistema. No se podrá acceder a ninguna información hasta que el sistema se desbloquee con el PIN correcto. Si selecciona el modo de valet, aparece una ventana emergente que le indica que debe introducir el código de cuatro dígitos para activar o desactivar dicho modo. Puede usar cualquier PIN que elija, pero debe usar ese mismo PIN para desactivarlo. El sistema le pedirá que introduzca el código”.**

Evidentemente, aquí la 'pega' es que si por un casual olvidas la clave, tendrás que acudir al concesionario para que te reestablezcan el dispositivo -evidentemente, aquí no hay una opción que te envíe un mail para cambiar el PIN, como cuando olvidas una contraseña de alguna de tus cuentas en redes sociales-. En cualquier caso, ¿cómo lo activas? Accediendo al menú de los 'ajustes', una vez en él deslizando hacia la pantalla de la derecha y ahí aparece el icono de 'Modo Valet'.



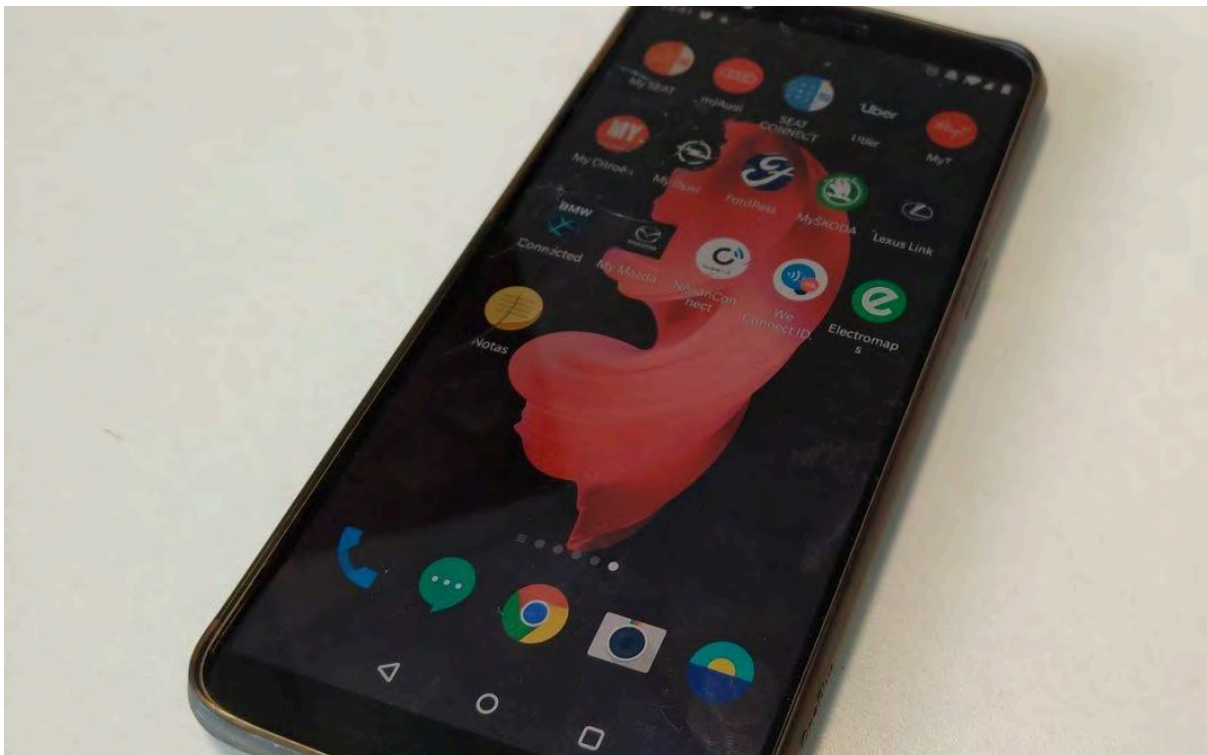


También se ofrece un ‘modo seguro’ en los modelos de Jaguar y Land Rover; incluso, este modo ofrece funciones ampliadas, en el sentido de que cuando se activa, además de bloquearse el acceso a muchas de las funciones del sistema multimedia, también se ‘condena’ el acceso al maletero. Todo esto está pensado, por ejemplo, para cuando el usuario deja el vehículo a un aparcamiento. **Además, el sistema de Jaguar-Land Rover permite crear códigos PIN temporales, así como uno permanente o PIN ‘maestro’.**

Acceder al modo valet del Jaguar se realiza de la siguiente manera: desde la pantalla principal de ‘inicio’, deslizando hacia el lado derecho encuentras las llamadas ‘funciones extra’. Allí, con el icono de una llave encuentras el acceso a ‘Modo seguro’: si accedes a él, ya podrás activarlo.

# CÓMO SABER SI LA APP DE UNA MARCA DE AUTOMÓVILES ES DE FIAR

Una de las formas más evidentes de la conectividad entre coche y usuario es... a través de la app para el móvil. Como en cualquier otro programa que te descargas en el teléfono, siempre es bueno seguir unos consejos de ciberseguridad.



Nuestro compañero “Jaime” -nombre ficticio- decide que quiere bajarse la app de su banco para realizar ciertas



operaciones de manera cómoda y desde cualquier sitio. Encuentra un enlace que le lleva al lugar donde descargárela, **lee la pequeña descripción que incluye y todo parece cuadrar con que esa es la app de su entidad bancaria.**

Nada más bajársela, Jaime comienza a probarla y a operar con ella; lo primero que le piden son múltiples datos, personales o bancarios, pero nuestro protagonista no sospecha, porque entiende que su oficina del banco también maneja esa información. Sin embargo, pasados unos días, recibe una llamada de la persona de confianza con la que trata **cada vez que acude a su sucursal de confianza y le comenta que está percibiendo extraños movimientos en su cuenta**, con numerosas compras seguidas y en pequeñas cuantías en establecimientos de dudosa ‘reputación’.

Jaime dice que él lo único que ha hecho es bajarse la app del banco pero que aún no ha operado con ella... y es entonces cuando tanto el empleado del banco como nuestro protagonista caen en la cuenta: la app que se descargó, a pesar de imitar la apariencia e imagen corporativa de la de su banco, en realidad es un aplicación que suplanta la identidad de la original, con el objetivo de que los usuarios ‘piquen’ dejen sus datos... y se les pueda robar información, dinero...

No sólo eso: **bajarse una app ‘ilegal’ o maliciosa -aunque sea sin darnos cuenta- puede tener más repercusiones**, como la de perder la garantía del fabricante del dispositivo, no poder actualizarse -debido a que no son oficiales, sino piratas- o, como comentábamos, ser víctimas de un hackeo.

Esta situación, aunque ficticia, es más real de lo que parece; y puede suceder con una app bancaria, pero también con una app para conocer gente, hacer compras on-line o, por qué no, ‘comunicarte’ con tu coche. Ahora que estas apps se están poniendo más de moda que nunca con lo vehículos conectados, no está de más repasar los consejos que da la OSI -Oficina de Seguridad del Internauta- a la hora de instalarse una app en el móvil. Y es que **“a veces, si lo descargamos del primer sitio que veamos, podemos terminar siendo infectados por algún tipo de virus que ponga en peligro nuestra privacidad”**, aseguran desde este organismo.

## Consejos sencillos para aplicar siempre

Prácticamente todos los teléfonos ya vienen con un acceso a las aplicaciones oficiales de la marca -Google Play para los [Android](#) y App Store para los iPhone-; unas tiendas que disponen de sus propios métodos de ciberseguridad con el fin de que no haya allí apps peligrosas o maliciosas, pero como destacan [desde la OSI](#), no es algo infalible y siempre puede haber apps que se cuelen. **Y es ahí donde tienen que entrar las medidas que sigan los usuarios.**

**La primera es mirar el número de descargas que tiene la aplicación**, lo cual siempre ayuda a distinguir cuál es la app oficial y no la fraudulenta, porque la primera se habrá descargado muchísimas más veces. **La segunda** es mirar lo que opinan otros usuarios: los comentarios y valoraciones son interesantes para saber si la app es útil, si funciona

bien, si hay algo 'raro' detrás... y las encontrarás en el apartado 'puntuaciones y opiniones'. **Como tercera medida**, comprueba quién ha creado la aplicación; es decir, visita la página web de la empresa que la haya creado o echa un vistazo en Google para conocer quién está detrás. Encontrarás el nombre en el aparato de 'Contacto del desarrollador' o en 'Ficha técnica'.

**En cuarto lugar**, y bastante importante -incluso en las apps legítimas- es revisar los permisos que solicita la aplicación al instalarse. Y es que cuando te la bajas, y antes de que la abras, te solicitará diversos permisos para funcionar -que pueden ir desde acceso a tus fotos y contactos hasta conexión a Internet-, pero también otros que quizá estén de más. Como ejemplo, [la OSI](#) asegura que si te bajas una app para editar fotos es normal que te pida acceso a las que tengas almacenadas en el móvil y al control de la cámara... pero que una aplicación para consultar el tiempo no debería tener acceso a la cámara bajo ningún concepto.

## **CIBERSEGURIDAD EN CAMIONES: PROBLEMAS Y SOLUCIONES**

La tecnología de los vehículos pesados no se difunde tanto, pero tienen incluso más que los turismos. Por eso, también han ido apareciendo

vulnerabilidades que los ponen en el punto de mira de los crackers.



Foto: Piqsels.

Si la ciberseguridad es una cuestión importante en los coches, **más aún debería serlo en los camiones**. Y es que estos vehículos son más complejos tecnológicamente, lo que se traduce en **mayor probabilidad de recibir un ciberataque**.

“La complejidad es el peor enemigo de la seguridad”, afirman Marko Wolf y Robert Lambert. Ambos investigadores de ciberseguridad publicaron [un estudio](#) en el que recogían **los motivos que hacían a los camiones más vulnerables que los turismos**.

Esas causas son muy variadas, y se pueden resumir en:



- **Necesita mayor conectividad para funcionar.** La idea de que en el futuro haya hileras de camiones autónomos que se dejen llevar guiados por un camión 'líder', cada vez más cercana, solo es posible si todos los participantes de la caravana están bien comunicados entre sí. Y no hace falta irse al futuro: las aplicaciones de gestión de flotas ya permiten intercambiar datos entre el vehículo y la central. Además es habitual que los camiones monten y desmonten accesorios según las necesidades del trabajo a desarrollar. Si esos accesorios están digitalizados, podrían convertirse en propagadores de virus de camión a camión.
- **Son más caros.** Estos gigantes de la carretera tienen un precio equivalente al de un superdeportivo y, encima, su capacidad de carga les hace llevar en cada viaje miles de euros de mercancías. Un botín con ruedas muy apetecible para los criminales.
- **No paran.** Se dice que un camión pierde dinero cada minuto que está parado. Por eso, las empresas los tienen en ruta el máximo tiempo posible, por lo que llegan a hacer kilometrajes al año impensables para un turismo. Y más tiempo de uso implica más posibilidades de ser atacado.

Teniendo en cuenta esas circunstancias, la conclusión de Wolf y Lambert es clara: **“es urgente la necesidad de ciberseguridad”** en este tipo de vehículos.

## ¿Quiénes amenazan a los vehículos pesados?

Debido a la importancia que tienen los camiones al ser parte fundamental de la economía de un país, pueden ser muchos los interesados en atacarlos. Según nos han expuesto los expertos del Área Técnica de [EUROCYBCAR](#), son **tres los grupos que podrían querer crackear a un vehículo pesado**.

El primero de ellos serían los **cibercriminales**. El típico cracker que busca aprovecharse de una vulnerabilidad para ganar dinero o infligir daño a la empresa. Puede atacar un camión o a toda la flota buscando un rescate o dañar la reputación de la empresa. Sus motivaciones pueden llegar incluso al terreno del espionaje industrial.

El siguiente grupo que consideran desde [EUROCYBCAR](#) son los **terroristas, los estados o los activistas**. En este caso, el interés no es realizar el crackeo en sí, sino enviar un mensaje a través de él, que puede ser político o ideológico.

Por último, queda un colectivo que puede sorprender a primera vista: el de **los propietarios**. ¿Por qué querría el dueño de un camión piratear su propio vehículo? No pienses en esta posibilidad como una forma de hacerse daño a ellos mismos, sino como una forma de hacer trampas. Es lo que ocurrió hace año y medio, cuando conocimos el caso de [una empresa que manipuló los tacógrafos](#) que equipaban los vehículos de su flota para poder ahorrarse los descansos



periódicos que son obligatorios por ley -y necesarios por seguridad-. El caso terminó en los juzgados.

## Algunas medidas de ciberseguridad para camiones

Las soluciones que proponen en sus textos tanto Wolf y Lambert como los expertos de [EUROCYBCAR](#) para proteger los vehículos pesados contra los crackers son bastante similares.

Ambos documentos ven conveniente **establecer medidas a lo largo de todo el ciclo de vida del camión**, para que ningún aspecto quede al azar. No sirve con protegerlo de fábrica, sino que hay que establecer procesos para que garantizar que ninguna de las posibles variables a las que se pueden enfrentar estos vehículos en su periodo activo cause un ciberataque.

Este aspecto ha pasado de ser una petición de los expertos a **un imperativo legal**. Y es que los camiones, al igual que otros tipos de vehículos, deberán cumplir [la norma de ciberseguridad de UNECE WP.29](#), que se aplicará en la UE a partir de julio de 2022 y establece que los vehículos deberán certificar su ciberseguridad a lo largo de todo su ciclo de vida.

Esas soluciones pasarían por **instalar protecciones en todos los sistemas informáticos del camión**, desde las centralitas hasta los servidores en la nube a la que llegan los



datos que emite el vehículo. Por tanto, sus componentes deben de ser ciberseguros por diseño.

Tampoco hay que olvidar algunos riesgos específicos de los camiones. En este aspecto se incluye el hecho de que su actividad va ligada a una empresa. Por tanto, la compañía propietaria deberá **contar -y aplicar- con una política de ciberseguridad adecuada**. Tendrá que saber gestionar la ciberseguridad y tomar medidas específicas para evitar los peligros de un ecosistema conectado como es un sistema de gestión de flotas.

## **CÓMO USAR TU MÓVIL Y TABLET EN EL AUTO DE FORMA SEGURA**

¿Quieres escuchar tu música favorita en el coche? ¡Claro! ¿Tener navegación GPS? ¡También! Y lo puedes lograr conectando un dispositivo móvil al vehículo. Pero si no sigues estos consejos, también tendrás en el viaje un ciberataque.



Subir al coche y conectar el smartphone o la tablet es una acción cada vez más habitual. Y es que **los coches de hoy en día permiten disfrutar de algunas funciones de un dispositivo móvil** sin tener que manejarlos conduciendo -lo cual sería una temeridad-.

## Coche y móvil se fusionan

Ya hace tiempo que está extendida la **vinculación entre vehículo y teléfono mediante Bluetooth**. Ese avance logró que el conductor pudiera hacer llamadas de voz sin tener que levantar las manos del volante.

Pero **la llegada de los smartphones convirtió a los móviles en un aparato más útil e inteligente**. Ya no servían solo para hacer llamadas: ahora también podían hacer algunas funciones muy interesantes para un viaje en coche, como **reproducir música** o hacer las veces de GPS.

¿Cómo integrarlas en un vehículo para utilizarlas de forma segura? Por ejemplo, a través de aplicaciones como [Android Auto](#) o [Apple CarPlay](#), o de la toma USB.

Y como la conectividad de los coches está aumentado, también lo hacen las formas de conectar los dispositivos móviles: ya es posible que los vehículos y los smartphones estén unidos por [wifi](#), [aplicaciones](#)... Incluso puedes [controlar funciones del automóvil desde el propio teléfono](#).

¿Todo ventajas? En principio sí... **hasta que llega un ciberdelincuente**. Los coches son vulnerables y los teléfonos también, así que su combinación podría hacer que un ciberataque pasase de uno al otro.

## Consejos para un uso seguro

Hay una serie de precauciones que los usuarios pueden tomar para minimizar los riesgos, ya sea en el dispositivo móvil para evitar que un ataque pase al vehículo al vincularlos o en el propio automóvil para protegerse de lo que llegue de fuera.

### En el coche

- **Protege las tomas USB del coche.** Si se conecta un móvil infectado con un ciberataque a ellas, este se podría descargar en el vehículo. Esto podría pasar también con un pen drive. Para que nadie conecte en



tu automóvil un dispositivo sin tu permiso, lo mejor es que bloques los puertos USB con un tapón con llave. De esta forma, solo tú podrás conectar dispositivos en esas tomas y así evitarás ciberriesgos. Por unos 20€, puedes hacerte con un [kit de estos bloqueadores](#) en sitios web como Amazon.

- **Cambia la contraseña del wifi.** Algunos coches ofrecen una red wifi interna para dar Internet a los dispositivos de los pasajeros. Una forma de establecer esta conexión es mediante una contraseña que viene por defecto en el coche. Un buen procedimiento de ciberseguridad sería que cambiases esta contraseña periódicamente. ¿Por qué? **Si no lo haces, todo dispositivo que se haya conectado alguna vez podrá hacerlo de nuevo sin permiso.**

## En la tablet o el móvil

- **Instala un antivirus.** Los programas maliciosos no afectan solo a ordenadores. Algunas apps están diseñadas para infectar smartphones y tabletas.
- **Cuidado con las estafas.** El mayor uso de dispositivos móviles por los usuarios ha aumentado el número de intentos de fraude a través de este canal. Permanece alerta.
- **Protege tu dispositivo** para que en caso de robo o pérdida puedas recuperarlo o al menos evitar que otros accedan a tu información.



- **Precaución al conectarte** a redes wifi públicas. Los crackers pueden generar redes que te den Internet... pero que a la vez te roben tus datos. También hay que tener cuidado al vincularse a otros dispositivos a través del Bluetooth.
- **No anules las restricciones del fabricante.** Éstas están pensadas para hacer que tu dispositivo funcione correctamente sin riesgos de seguridad.
- Si tu dispositivo móvil es Android, puedes [instalarte CONAN mobile](#) que te permite **conocer el estado de seguridad de tu dispositivo.**

## No solo ciberseguridad

Si vas a usar un dispositivo móvil en el coche, **asegúrate de hacerlo solo si no conduces o si están debidamente conectados** para que no tengas que usarlos físicamente. De nada sirven estos consejos de ciberseguridad si tienes un accidente por una distracción. Recuerda cuidar también la seguridad física.

## LAS PREGUNTAS MÁS



# FRECUENTES SOBRE CIBERSEGURIDAD

La ciberseguridad genera bastantes incógnitas por ser una materia relativamente nueva.

¿Cuáles son las dudas más habituales que nos genera? Te decimos cuáles son... y las respondemos.



Foto: Piquesels.

Google es el mayor confesor que tenemos en nuestra vida digital. Él lo sabe todo porque a él le preguntamos cuando tenemos alguna duda, así que se convierte indirectamente en **una herramienta muy útil para analizar qué es lo que más nos intriga sobre un tema.**

Nosotros, como no podía ser de otra manera, hemos querido saber **qué es lo que más preguntamos los españoles a Google en cuestión de ciberseguridad**. Para ello, hemos utilizado la página web [Also Asked](#), en la que introduciendo una palabra, muestra cuáles son las preguntas más habituales que la gente hace en Google sobre ese término.

En el caso de la ciberseguridad, las preguntas más habituales entre los españoles son cuatro. A continuación, te mostramos cuáles son... y también las respondemos, para salir de dudas.

## ¿Qué es la ciberseguridad?

La pregunta básica sobre ciberseguridad es... saber qué significa ese término. La ciberseguridad se podría definir como **las medidas que hay que tomar para proteger cualquier sistema informático de ciberataques**. Esos sistemas informáticos abarcan [desde los móviles](#) que llevamos en el bolsillo [hasta los coches](#). Todos esos objetos pueden estar en el punto de mira de un ciberdelincuente.

## ¿Cuáles son los elementos de la ciberseguridad?

La seguridad informática no está compuesta solo por un ámbito. **Para lograr una completa protección, hay varios aspectos que hay que cuidar**, que son los siguientes:





- **Seguridad de la aplicación.** Son todas aquellas características que equipa el software de una aplicación informática para evitar ciberataques. Por ejemplo, un mecanismo de seguridad instalado en una aplicación de correo electrónico para evitar que un cracker pueda acceder a la información almacenada.
- **Seguridad de información.** Las medidas que permiten resguardar y proteger la información que utiliza una organización o usuario.
- **Seguridad de la red.** Es habitual que empresas con un número importante de empleados que trabajan delante de un ordenador conecten de alguna forma todos sus equipos para que puedan compartir recursos. Pero eso puede suponer un peligro: si uno de las computadoras conectadas sufre un ciberataque, sus consecuencias podrían extenderse por toda la red. Por eso, la seguridad en la red es el conjunto de prácticas que adopta una organización para evitar riesgos en su red informática.
- **Recuperación ante desastres.** Hasta ahora, todos los elementos estaban enfocados a evitar incidentes. Pero la ciberseguridad 100% no existe, así que hay que tener un plan para reponerse de las consecuencias si finalmente un cracker logra atacarnos. Suelen centrarse en recuperar el correcto funcionamiento y acceso a todos los sistemas informáticos y datos afectados por el ciberataque.
- **Seguridad operacional.** Establecer protocolos para que los procesos rutinarios de una compañía en los que se usen sistemas informáticos no acaben en una



brecha de ciberseguridad. Es decir, que un trabajador no pueda exponer con sus acciones a un ciberataque a la empresa en la que trabaja.

- **Educación del usuario final.** De nada sirve crear el dispositivo mejor protegido contra ciberataques del mundo si luego la persona que lo usa incurre en conductas de riesgo. Por eso, es clave que el usuario final de un producto informático sepa identificar potenciales ciberataques como el phishing –[aquí](#) te contamos cómo puedes identificarlo- y tenga claro qué no debe hacer para no poner su equipo en peligro.

## ¿Cuánto gana un especialista en ciberseguridad?

Es importante señalar que no hay una única profesión relacionada con la ciberseguridad, sino que pueden **desempeñarse múltiples puestos... con múltiples remuneraciones**. Según [Infoempleo](#), un especialista en ciberseguridad puede dedicarse a:

- Administrador de seguridad de sistemas y redes.
- Consultor de seguridad y hacking ético.
- Arquitecto de sistemas de seguridad.
- Director de proyectos de Ciberseguridad.
- Analista de informática forense.
- Gestor de protección de datos.
- Ingeniero de control de Ciberseguridad.



- Arquitecto de análisis de riesgos.
- Ingeniero de ventas de Ciberseguridad.
- Perito judicial tecnológico.

El mismo portal calcula que los especialistas en ciberseguridad ganan cada año de media entre 30.000 y 60.000 euros. Los puestos con peor remuneración serían los que conllevan menos responsabilidad y experiencia, como los técnicos de seguridad -unos 28.000 euros anuales- o los técnicos de redes -24.000 euros-. En el otro extremo se situarían los directores de los sistemas de información, con un sueldo anual entorno a los 60.000 euros.

## ¿Qué estudiar para dedicarse a la ciberseguridad?

Si te interesa este mundillo y quieres enfocar tu trayectoria profesional a él, estás de enhorabuena. La digitalización cada vez afecta a más ámbitos, por lo que los ámbitos donde hay que trabajar la ciberprotección aumentan -el mundo del automóvil es un [ejemplo de ello](#)-. Así que este tipo de profesionales están muy demandados, y esa tendencia [irá al alza](#) en los próximos años.

¿Te interesa trabajar en este ámbito?

Desde [Educaweb](#) recomiendan empezar por adquirir unos **conocimientos básicos en informática**. Estos se pueden alcanzar a través de ciclos formativos de grado superior o estudios universitarios de informática o telecomunicaciones.

También recomiendan especializarse estudiando másteres o cursos de ciberseguridad.

Esa formación serviría de base, pero Educaweb también recomienda sumar conocimientos específicos sobre:

- Entornos tecnológicos: SCADA, mobility, servidores, Smart Grid y otras arquitecturas tecnológicas.
- Análisis forense: sistemas de archivos, adquisición de evidencias, timeline, análisis de memoria, file carving, reconstrucción de ficheros, criptografía, etc.
- Análisis de malware: ASM x86/x64, determinación de funciones, métodos de infección y persistencia, desinfección de malware, ingeniería inversa/reversing, criptografía. Todo ello enfocado a diferentes tipos de formatos: PE, PDF, SWF, MS Office, APK, etc.
- Análisis y evaluación de vulnerabilidades técnicas para el descubrimiento y explotación de vulnerabilidades tanto en servidores como en puestos: test de intrusión, análisis forense, etc.
- Gestión de incidentes: sistemas operativos, networking, IDS, IPS, FW, análisis de logs, análisis de tráfico en red.

Además, para mejorar la empleabilidad, es recomendable obtener algunas de las certificaciones más demandadas del ámbito, como **CCNP, CCSA, CCNA, F5 LTM, Palo Alto CNSE, SANS SEC-401, CISSP y CEH**.

# ¡CUIDADO CON EL USB! TODO LO QUE PODRÍA PASARTE CON UNO... Y CÓMO EVITARLO

Robo de información, secuestro de equipos o descargas eléctricas. Los crackers saben cómo atacar tu coche con un pen drive. Y nosotros, cómo evitarlo.



*Imagen de StockSnap en Pixabay*

Uno de nuestros [expertos nos contaba en una ocasión](#) que los puertos USB de su coche están tapados. Pero no con un tapón normal que tenga por finalidad proteger la conexión del polvo o de cualquier elemento externo. El tapón de Demonito sólo se puede quitar... ¡con llave! De esta forma, se asegura



de que nadie conecte ningún dispositivo a través de esas tomas sin su conocimiento. ¿**Qué riesgos tiene el puerto USB de un coche** para que un hacker decida tomar esta medida?

## **Puerta de entrada para los “malos”**

Sí, pueden ciberatacar tu coche a través de las múltiples tomas USB que llevan los coches modernos. **Algo tan cotidiano** como que te descargues música en tu ordenador, introducirla luego en un pen drive y, posteriormente, conectar éste en tu coche para reproducir las canciones **podría suponer una amenaza para tu vehículo**. ¿Cómo? Si un cracker ha introducido software malicioso dentro de esa lista de reproducción que, de forma inocente, has descargado, al conectar el pen drive al coche, el virus infectaría los sistemas de tu vehículo.

Hace unos años, se demostró que varios modelos de Mazda y Subaru eran **crackeables a través del USB**. Todo el ataque se desarrollaba simplemente introduciendo un pen drive infectado con el malware en la toma del salpicadero del coche. Con esa acción, se desarrollaba el ataque **sin necesidad de que el inocente usuario realizase ninguna acción**.

¿Qué consigue un cracker con esto? **Piensa en toda la información que dispone de ti tu coche conectado**. Datos personales, contactos, hábitos..., todo eso sería accesible a un cracker. Pero no solo tu información está en riesgo. Hay

ciberataques que **pueden dirigirse a los sistemas de funcionamiento de tu coche y manipularlos**. Tomar el control de la dirección o frenos; abrir y cerrar las puertas; o detener el motor son riesgos que pueden entrar por el USB. Y tú que solo querías escuchar música en el coche...

Los riesgos que pueden llegar a través del USB son muchos. Hay hasta un tipo de pen drive, llamado USB killer, cuya única función es soltar una descarga eléctrica sobre el equipo anfitrión -el coche en este caso- al conectarlo. ¿El resultado? La destrucción del hardware, entre ello, los sistemas operativos de un coche. Además, el peligro no está solo en los pen drives. Cualquier dispositivo que se conecte mediante USB –*smartphones, tablets...*- puede contener un vector de ataque.

¿Se puede solucionar esto de alguna manera? En el mercado existen algunas opciones para prevenir el ciberataque, en concreto mediante aparatos que hacen de ‘barrera’. Cabe señalar que **ninguna ofrece garantía en caso de que el mecanismo de defensa falle** y se cuele un ciberataque a pesar de emplearlos. Los fabricantes justifican esta decisión porque en un crackeo intervienen varios factores externos, que no siempre pueden ser controlados y auditados

## La solución de fábrica...

...no existe, al menos de momento. Lo ideal sería que el coche saliese de la línea de montaje con **sus puertos USB**



**ya protegidos** frente a estas amenazas. Pero, de momento, esta opción no está disponible. Hay herramientas como el authUSB Safe Door que lo harían posible si las marcas apostasen por integrarlas en el diseño y fabricación del vehículo.

El Safe Door tiene el tamaño de un router y protege cualquier tipo de ordenador -también los del coche- de aquellos dispositivos USB que puedan contener ciberataques. Esa herramienta **analiza si un instrumento de almacenamiento es seguro o no antes de descargar la información** -y, por tanto, el ciberataque en caso de contenerlo- en el equipo anfitrión. Así, se cierra la puerta a, por ejemplo, un pen drive infectado con un virus.

**Puede detectar los tres tipos de vectores de ataque posibles:** a nivel software -virus-, hardware -vectores de robo de información o infección de equipos y redes- y eléctrico -los ya mencionados USB killers-.

De estar implementado este dispositivo en los coches desde el propio proceso de fabricación de los vehículos, todos los conectores USB del vehículo estarían vinculados con el Safe Door. Por ello, el usuario solo tendría que conectar un pen drive en el coche y esperar al resultado del análisis, según afirman los responsables de authUSB. Ese análisis podría mostrarse al dueño del vehículo de una forma tan sencilla como un juego de luces verde y roja en el salpicadero, por ejemplo. **Si aparece una luz roja, el pen drive no es seguro** y la información que contenga no se descargaría para proteger el vehículo. En cambio, si la luz es verde, su

uso es seguro y el Safe Door sí dejaría paso a la información de forma automática.

Sabiendo que aún no es posible que los coches vengan con ello instalado de fábrica, quizá algún conductor se podría plantear adquirir este dispositivo de forma personal. Sin embargo, por el momento, tanto el precio -a partir de 900€, según los años de actualizaciones que se decidan contratar- como el enfoque del producto están destinados a empresas con un equipamiento informático muy grande. Así, solo a industrias o grandes oficinas sí les saldría rentable la compra -a través de [la web de authUSB](#)- de una unidad para vincular en red sus diversos ordenadores con el Safe Door.

## Dos formas de evitar estos ataques

Si quieres una solución asequible para proteger tu coche de crackeos, aquí tienes dos opciones. A diferencia del Safe Door, ninguno de estos productos defiende a la vez de los tres tipos de ciberataques que existen -de software, de hardware y eléctrico, ya mencionados anteriormente-, sino que protegen de alguno de ellos.

### USB DEFENDER

**De qué te protege:** Alquilas un coche y conectas el móvil para cargarlo. Viajas en tren y haces lo propio cuando te quedas sin batería. Enchufas tu dispositivo a un cargador público en un aeropuerto. Nadie puede asegurarte que un

cracker haya alterado esos puertos para robarte los datos que almacenas en tus aparatos nada más enchufarlos.

**Cómo funciona:** USB Defender actúa de intermediario entre el cargador público y tu dispositivo. Así, te permite cargar el móvil, la tablet o cualquier otro aparato con puerto USB, sin transmitir datos.



**Lo mejor:** Su funcionamiento es muy sencillo y su precio, asequible. Puede adquirirse [a través de Amazon](#) por unos 7 euros.

**Lo peor:** Si necesitas descargar datos de un dispositivo a otro, no podrás hacerlo, ya que funciona cortando el canal de transmisión de datos en ambos sentidos. Solo permite cargar tu dispositivo.

## TEST SHIELD

**De qué te protege:** Del USB killer, un pequeño aparato, similar a un USB, que, al enchufarlo a un dispositivo, lanza una descarga eléctrica que funde componentes, como la placa base, inutilizando el ordenador o el móvil al que se conecta. Se comercializó en 2015 – y va ya por su versión 3.0, que cuesta 54,95 euros. Inicialmente estaba pensado para que los fabricantes testaran la seguridad de sus equipos contra USB killers-

**Como funciona:** debes conectar el [Test Shield](#) al puerto USB, y el pen drive que quieras comprobar si es seguro, al Test Shield. A continuación, y con cuidado, comprueba si al unir los cables que salen del test shield saltan chispas. Si es así, estarás ante un USB killer, por lo que no debes conectarlo al ordenador bajo ningún concepto.

**Lo mejor:** Solo cuesta 14,95 euros y, si habitualmente conectas a tu ordenador USB desconocidos, es una buena forma de hacerlo de forma segura.

**Lo peor:** solo sirve para testar si un pen drive es un USB Killer, pero no protege contra malware -virus-.

# ECALL: QUÉ HACE CON TUS DATOS EL SISTEMA QUE SALVA VIDAS

Este sistema, obligatorio en todos los coches nuevos, promete reducir los fallecidos en carretera. Pero, para eso, necesita saber muchos datos de tu coche. ¿En qué lugar queda tu privacidad? ¿Qué datos usa el eCall y para qué los emplea?



Salvará 1.500 vidas al año. Por eso, todos los vehículos nuevos que se fabriquen en la Unión Europea desde hace año y medio deben equiparlo. Se trata del [eCall](#), un sistema

que permite a los ocupantes de los coches **avisar al 112 mediante un botón** si han sufrido un accidente. Pero su gran ventaja es que, **si los pasajeros no lo pueden activar** como consecuencia de las lesiones, **el propio sistema dará el aviso** a los servicios de emergencia **de forma automática**.

## ¿A qué datos accede el eCall?

Para que pueda funcionar, **el eCall debe transmitir determinada información** de forma automática y, por tanto, debe tener acceso a ella. Silvia Díaz y Xisco Martínez, Delegados de Protección de Datos -DPD- del [Instituto Internacional de Privacidad y Seguridad de la Información](#) -IIPSI- explican que **esos datos son**:

- Posición del vehículo: latitud y longitud geográfica, así como las dos últimas posiciones del coche y la diferencia entre éstas y la posición actual.
- Datos de control: si la activación ha sido automática o manual, si se trata de un test o una llamada de emergencia real, la clase del vehículo, el dígito binario o la fiabilidad de la posición.
- Hora del accidente y dirección del viaje.
- Número de chasis -VIN-: número de 17 dígitos para la identificación inequívoca del vehículo.
- Tipo de transmisión: eléctrica, diésel, gasolina o GLP.
- Número de pasajeros: basado en el número de cinturones de seguridad abrochados.



Además, los expertos aclaran que **el sistema no almacena ningún dato personal del propietario del coche**. De esa forma, no será necesario actualizar los datos, por ejemplo, al vender el coche de segunda mano.

Gracias a la información que recopilan, los servicios de emergencia podrán evaluar y gestionar la situación. Pero también puede poner sobre aviso a los conductores que se preocupen por la [ciberseguridad en sus automóviles](#). Entonces, ¿cómo se gestiona la privacidad en este sistema?

## “Un serio debate”

“**El eCall ha desencadenado un serio debate en torno a la privacidad de los datos**” afirman los DPD del IIPSI. Tanto es así que, incluso, se retrasó la aprobación del sistema en 2015, por un debate “en torno a la privacidad en los pasillos del parlamento de la UE” añaden.

Eso fue debido a que “**las voces más críticas ven en el sistema una amenaza potencial a la privacidad de los conductores**”. De hecho, “fabricantes y aseguradoras ya han mostrado gran interés en [la información que potencialmente se recopile](#) a través del sistema” explican.

## ¿Qué hace con la información?

Sin embargo, ese escenario aún no ha llegado y **el actual eCall protege trata mejor a los datos de los usuarios**.



“Solo se activa en caso de accidente grave. El resto del tiempo permanece inactivo” aclaran Díaz y Martínez. Es decir, que “durante la conducción habitual del vehículo no se produce ninguna actividad de seguimiento -para controlar la posición del automóvil o los datos de conducción- ni de transmisión de datos”.

Además, los expertos del IIPSI detallan que desde las instituciones europeas se ha legislado para **obligar a los fabricantes a eliminar “de forma permanente” los datos recopilados a través del eCall**. Ni siquiera los servicios de emergencia “podrán transmitir los datos a terceros sin el consentimiento explícito del propietario del vehículo” continúan.

## ¿Anularlo?

Si aún así el usuario no se fía y quiere desactivar este sistema en su coche, debe saber que “podría perder la capacidad de circular por la Unión Europea”, además de que “el seguro podría incluso anular su cobertura” si se descubre el engaño. Tampoco sería fácil anular el eCall: “Es virtualmente imposible debido a la conexión del sistema con otros sistemas internos del vehículo” concluyen Díaz y Martínez.

# LAS COSAS QUE NUNCA TE VA A PEDIR TU MARCA

Para comprar un vehículo, tienes que dar muchos datos personales para formalizar el contrato. Pero no te los pueden pedir de cualquier forma. Así que deberías sospechar si se dan las siguientes circunstancias. Podrían haber suplantado a la marca.



*Photo by Caleb Oquendo from Pexels*

Los **datos personales** se han convertido en **un bien muy codiciado**. Por eso, no deberías de difundirlos alegremente. Ni tampoco al primero que te los pida, aunque te insista

diciendo que son de una empresa de la que eres cliente, como tu marca de coches.

Gracias al [Reglamento General de Protección de Datos](#), hay procedimientos establecidos para pedirte legalmente y con garantías tu información privada. Todo lo que no sean los canales establecidos debería encenderte las alarmas ante un posible caso de suplantación con el objetivo de sacarte tus valiosos datos.

¿Qué cosas son las que deberían hacerte sospechar?

## No des datos personales por teléfono...

Hace cerca de un año, medios de Puerto Rico [informaron](#) de que la filial de Toyota en el país caribeño había detectado **una serie de llamadas telefónicas fraudulentas a sus clientes**.

Cuando descolgaban el teléfono, el estafador pedía a las víctimas información personal, intentando persuadirlas diciendo que llamaban en nombre de Toyota. El fabricante de automóviles ha denunciado que ellos no habían hecho esas llamadas, sino que es habían suplantado. Además, aclaró que ellos **nunca pedirían información de forma telefónica**, por lo que aconseja no dar información confidencial por esta vía.

Ese consejo es extrapolable a España. **No es conveniente que proporciones información personal tuya en caso de**

**que llamen por teléfono.** No es la política que aplican las empresas y lo más probable es que se trate de un delincuente que quiera hacerse con tus datos para fines nada beneficiosos para ti.

## **...ni por correo electrónico**

La misma máxima se puede aplicar también en caso de que recibas un correo de una marca de coches solicitándote información personal. **La mayoría de empresas nunca contactarán contigo por esta vía para pedirte datos.**

¿El problema? Los ciberdelincuentes hacen muy bien su trabajo y dedican mucho tiempo a imitar la estética de correos corporativos de un compañías auténticas para que confíes en ellos y piques. **Es el famoso [phishing](#), uno de los ciberataques más habituales en el mundo.**

Pero hay una serie de **pistas que pueden ayudarte a diferenciar un correo electrónico verdadero de uno de [phishing](#).** Estos son los consejos que [publica](#) ESET en su blog:

- ¿El mensaje realmente demuestra que el remitente sabe algo acerca tuyo y, ante todo, ya tienes relaciones comerciales con él? La falta de personalización puede ser un claro indicativo. Si el mail empieza por “Estimado cliente”, sospecha. Pero que el texto incluya algún dato tuyo no quiere decir



que lo tengas que dar por bueno automáticamente. Deberías pasar a las siguientes pistas.

- No te fíes de los archivos y vínculos insertados. Los primeros podrían contener un virus que se ejecute al descargarlos y los segundos te pueden llevar a un sitio web peligroso. Un truco puede ser que pases el cursor sobre el enlace para que aparezca la dirección web y que así puedas comprobar si te dirige a un sitio fiable o no. Y debes sospechar de los vínculos acortados.
- No caigas en las amenazas. “Si no proporciona los datos en 24 horas, su cuenta será cancelada”. Pocas compañías querrían perder tan rápido a un cliente. No te precipites por leer algo así.
- ¿Tiene faltas de ortografía o está mal redactado? Los primeros correos de phishing se caracterizaban por tener fallos muy evidentes en su escritura. Este aspecto ha mejorado últimamente, pero si ves un mail corporativo con ellos, sospecha.

## **CÓMO PUEDES EVITAR -SIN SER UN EXPERTO- QUE UN CRACKER CONTROLE TU AUTO**

El mundo que abren los coches conectados es también un intercambio constante de información entre entorno y vehículo, lo que sin duda atraerá a los astutos ciberdelincuentes.





**A mayores avances tecnológicos siempre habrán mayores conocimientos sobre cómo funcionan esas herramientas**, y los que los utilicen para interés personal o para saltarse la ley deberán trabajar de manera cada vez más discreta y meticulosa. Una vez conocido esto, de la mano de la revista de automóviles estadounidense Car and Driver se le brindan al lector una serie de [advertencias y consejos](#) para que pueda sobrellevar el riesgo que se le plantea si es poseedor de un coche conectado, o si prevé obtenerlo en un futuro a corto plazo.

## **Actuaciones correctas para evitar ciberataques**

**Para comenzar no hay nada más importante que situar y asimilar el problema**, que es el siguiente: si se posee un

coche “inteligente”, la tecnología que lleva incorporada siempre podrá ser pirateada de alguna manera, y está claro que a mayores capacidades digitales mayor lo será también el riesgo de ciberataque. Una vez conocido esto, **el primer consejo es tan simple como estar alerta y fijarse en posibles fallos o funcionamientos anormales de esos sistemas.**

El segundo recuerda a cualquier otra tecnología conectada, y es **la necesidad de actualizar el sistema siempre para que se mantenga con las últimas funcionalidades y sus rendimientos.** Muchos de esos “parches” son precisamente para tapar lagunas de ciberseguridad, previamente detectadas por los fabricantes y consideradas como de riesgo por ser altamente aprovechables por parte de ciberdelincuentes.

**Le sigue un control adecuado de los dispositivos USB -Universal Serial Bus- mediante su escaneo antes de incorporarlos al coche.** Pocas dudas caben de que este es el sistema clásico de ataques cibernéticos, su “caballo de Troya”, así que una revisión del antivirus puede ahorrar sustos y detectar a tiempo softwares maliciosos listos para crackear el vehículo, o todo aquello en lo que se instalen nada más establecer contacto.

El cuarto es algo que pocos hacen, y es el hecho de **desactivar Bluetooth y la Wifi cuando no se esté utilizando para alguna funcionalidad del automóvil.** Quizás una actualización reciente no evite que un tercero no deseado se cuele a través de las puertas que implican las



conexiones, por ejemplo si se aprovechara la nueva tecnología que implica el **5G**. Cabe añadir que no se le debe ofrecer a la ligera el servicio de conexión propio a alguien, a no ser que sea de la más absoluta confianza y cercanía.

Se debe hablar de extremar la precaución a la hora de conectar cualquier cosa al OBD2, un escáner que implica un sistema de diagnóstico del motor. Para ser más claros, **este puerto de comunicaciones se utiliza para programar, codificar o diagnosticar todo dispositivo electrónico que incorpore el vehículo**; así que deben conocerse su ubicación y sus distintas aplicaciones. Como advertencia añadida, algunas compañías de seguros venden dispositivos que a su vez se adaptan al anterior y explican los hábitos del conductor, pensados para adaptar los precios de los seguros en base a ello. A cambio de una buena manera de ahorrar, el dueño del vehículo conectado ofrecerá más posibilidades a los crackers para atacar e incluso controlar su coche.

## **El mando del coche, vulnerable como el que más**

También se deben **vigilar las descargas que se realizan o que uno se plantea realizar**. Se debe aclarar que los “smartphone” o “teléfonos inteligentes” adquieren cada vez más funcionalidades, destronando a otros dispositivos, y el mando del coche es uno de esos que poco a poco se ve relevado de su puesto. Esto quiere decir que **si un teléfono inteligente es atacado con éxito, todo aquello a lo que**

**esté conectado podría verse comprometido**, y eso podría incluir a un coche de última generación.

Asegurarse de que no roben la señal proveniente de las **llaves del coche** es otra recomendación importante, algo básico pero crucial si además las mismas controlan más funciones del automóvil, algo común en vehículos conectados. Puede sonar surrealista, pero **no se recomienda abrir las puertas del coche a distancia en lugares que no se controlen**, ya que de no hacerse manualmente con la clavija física del objeto quizás alguien se aproveche y tome el control de manera astuta y sigilosa.

Como complemento del consejo anterior, se debe cuidar y proteger en todo momento el mando del transporte. Más allá de llevarlo siempre en el bolsillo o en el bolso, **lo idóneo es guardarlo en lugares donde se sepa que un cracker no puede encontrarlo ni acceder a él a distancia**. Para facilitar la labor, hoy se encuentran disponibles ciertas bolsas especiales que bloquean toda posibilidad de ciberataque o duplicado del mando del coche.

## La batalla de hackers contra crackers

Adicionalmente a los consejos, se quiere añadir que **muchos fabricantes de coches han decidido tomar cartas en el asunto** y **contratar a hackers** como guías y guardianes que eviten los ataques malintencionados de terceros. Por el bien de no sólo la seguridad de sus dispositivos, sino también de los softwares para el control, las marcas han reaccionado y

ya incorporan a sus plantillas a expertos con los mismos conocimientos que los crackers, pero que sin duda cuentan con mejores intenciones, y de paso más legales.

Lo que más les ha podido llevar a actuar de esta manera es el hecho de que **ante un daño material o físico a sus clientes, lo más probable es que sean los propios fabricantes que les han vendido el modelo crackeado los que deban responder legalmente**, y ello supondría tanto pérdidas cuantiosas en sus ganancias como en su buena reputación.

## **CÓMO ENFRENTARSE AL RANSOMWARE, EL MAYOR ENEMIGO DE LAS EMPRESAS**

Este crackeo es la principal amenaza de ciberseguridad para cualquier organización. ¿Qué hay detrás de estos ataques y qué se puede hacer para combatirlos? Varios expertos reflexionan sobre ello.



Foto: Píqsels.

El **ransomware** supone un auténtico quebradero de cabeza para las organizaciones, ya sean instituciones públicas o empresas privadas. Informe tras informe, no dejan de sucederse las estadísticas que señalan a este ciberataque -con el que los crackers **bloquean un sistema informático o sus datos para pedir un rescate**— como uno de los más preocupantes y extendidos actualmente. Por ejemplo, desde ESET apuntan a que probablemente sea la amenaza más peligrosa a la que se enfrentan las empresas, sea cual sea su tamaño.

Es por eso que **el ransomware tuvo un notable protagonismo dentro del X Foro de la Ciberseguridad organizado por ISMS Forum**, que se ha celebrado este jueves. De hecho, fue el plato fuerte de la mesa redonda titulada ‘El mayor riesgo para cada organización’ -en velada referencia al ransomware-.



## Los ciberdelincuentes van a por las empresas

En dicha charla, Jenko Gaviglia, de HelpSystems, señaló **dos problemas importantes en relación con el ransomware**. El primero de ellos, que este ataque está creciendo mucho con respecto al año anterior. ¿El segundo? Que ha cambiado. Estos ataques antes iban a por los usuarios particulares, pero ahora solo les usan como método para llegar a las empresas para las que trabajan. “Primero van a por el sistema de un usuario, con eso acceden al sistema de la empresa, se quedan ahí dentro un tiempo y después empiezan a atacar a toda la empresa”, explicó Gaviglia.

**Y el motivo de que ahora los ciberdelincuentes se hayan centrado en las empresas no es otro que el dinero.** “¿Y dónde está el dinero? En las empresas, por eso van a por ellas”, aseguró Jonathan Gándara, de Votorantim Cimentos. Por eso, cree el ransomware ha llegado para quedarse. Irá cambiando, pero siempre seguirá ahí porque es rentable.

**Este tipo de delincuencia ya ha sufrido una gran evolución.** Gándara afirmó que se ha especializado mucho porque va a la par con la tecnología: cuanto más y mejores sistemas de encriptación hay, más los usan los ciberdelincuentes para atacar empresas. Es decir, los mismos sistemas que usan los hackers para proteger información son empleados por los malos para secuestrarla.



También coincidió con esa teoría de la evolución Jonathan Rendal, de FireEye. Este experto declaró durante la mesa redonda del evento de ISMS Forum que **los crackers cada vez saben hacer cosas más peligrosas y silenciosas**. Señaló que incluso pueden permanecer ocultos dentro de los sistemas informáticos de la empresa víctima, esperando el momento adecuado para cometer el ataque. Y afirmó que en Europa pasan 66 días de media desde que se infiltran en las redes de una empresa hasta que son detectados.

Por eso, Alexis Serrano, de BeyondTrust, cree que hay que centrarse en **evitar que los ciberdelincuentes hagan daño una vez hayan entrado en los sistemas**. Hay que proteger la información con medidas para hacerla inaccesible, porque, opina Serrano, si un grupo criminal quiere entrar en el sistema informático, lo va a lograr.

## Una cuestión de dinero

Los cuatro participantes en la mesa redonda también hablaron del dinero que pagan las empresas para recuperar la normalidad tras un ciberataque. **El rescate más caro que habían visto pagar** ascendía a 1,9 millones de euros. Una cifra que parece incluso discreta si se compara con los cinco millones de dólares -4,1 millones de euros- que se rumorea que **pagó Colonial Pipeline** por recuperar la operatividad de su red de oleoductos en EE.UU. tras sufrir recientemente un ataque por ransomware.

“La gente paga porque el ransomware está bloqueando la operativa de la empresa. Es perder o pagar”, sentenció Serrano.

Y es que tener totalmente bloqueada la actividad empresarial puede suponer mayores pérdidas que el precio del chantaje. Por ejemplo, Forward Air, una empresa de transporte aéreo y terrestre, **tuvo que interrumpir sus operaciones** durante varios días por un ataque a su sistema informático. ¿El resultado? Unas **pérdidas estimadas de 7,5 millones de dólares** -algo más de seis millones de euros-.

## ¿Alguna marca de coches ha sufrido ransomware?

De momento, **no hay confirmación oficial** por parte de ninguna marca de coches de haber sido afectada por un ataque de ransomware.



No obstante, hay ciertas dudas con [el problema informático que sufrió Kia](#) a principios de año. Los servidores informáticos de la filial norteamericana de la marca tuvieron problemas para funcionar correctamente durante varios días del mes de febrero. La afección **paralizó los concesionarios y la aplicación móvil** que usan los propietarios. Bleeping Computer [lo atribuyó](#) a un ciberataque de ransomware -incluso cifró en 20 millones de dólares el rescate exigido-, pero Kia, que reconoció las interrupciones en el servicio, negó que la causa fuera un crackeo.

Sin embargo, en la industria auxiliar del automóvil sí se han visto ya algunos casos de ransomware. Uno de los más recientes fue [el sufrido por NameSouth](#), una empresa estadounidense de recambios de automóviles. En este suceso, los ciberdelincuentes lograron sacar del sistema informático de NameSouth 3GB de archivos confidenciales. Tras la sustracción, los crackers pidieron un rescate a la empresa para recuperar los documentos. Al no recibir pago alguno, los crackers **publicaron la información en un blog de la Internet oscura**.

## ¿Qué hacer para evitar el ransomware?

[Pablo F. Iglesias](#), consultor de Presencia Digital y Reputación Online, piensa que toda organización debería “**tener un sistema de alerta temprana implementado que nos alerte de potenciales filtraciones**“. Esto protegería a las empresas contra casos de ransomware y filtrado de información



confidencial. Además, como pautas generales, el experto recomienda:

- **Establecer controles de seguridad efectivos** que analicen el tráfico y actividades potencialmente sospechosas dentro de las fronteras de la organización, y bloqueen accesos según salten las alarmas. Por ejemplo, sistemas inteligentes de detección, sistemas de gestión de incidentes de seguridad, cortafuegos, honeypots....
- **Contar con una política de compliance correctamente aplicada** -no vale solo con tenerla, hay que cumplirla...- que evite, por ejemplo, que un usuario infectado pueda exponer todos los recursos de la organización y no únicamente los que compete a sus labores.
- **Cifrar la información sensible y forzar el tratamiento de dicha información mediante canales cifrados.** Con ello se logra que, aunque un ataque tenga éxito, “no puedan recompartir los datos en texto plano como parece que ocurrió en este caso” afirma Iglesias.

Por último, el experto también cree conveniente **formar en competencias digitales a los empleados**, ya que el 95% de los ciberataques a empresas entran por **un fallo humano**.

# LOS TRANSPORTISTAS AÚN NO ESTÁN CONCIENCIADOS CON LA CIBERSEGURIDAD

Las empresas de transporte cada vez sufren más ciberataques. Pero un estudio de Continental muestra que estas compañías aún no dedican la suficiente atención ni los recursos para estar protegidas.



Foto: Pigsels.

Un estudio realizado por [Continental](#) pone de manifiesto que las empresas dedicadas al transporte por carretera aún **no están lo suficientemente concienciadas de la importancia que tiene la ciberseguridad en su trabajo.**

Resulta llamativo, ya que en este sector **se están implementando en los últimos años un creciente número de soluciones de conectividad**. Con ellas, las empresas logran mejorar la eficiencia y reducir el coste de sus procesos. “Sin embargo, la conectividad también aumenta los riesgos de ciberataques en las compañías de transporte”. explica el Dr. Mathias Dehm, director en Continental de Investigación y Procesos para la Seguridad de Productos.

De hecho, el sector del transporte fue **el tercero más atacado durante 2019**. **Un informe** que IBM publicó hace cuatro años reveló que las empresas de transporte sufrieron uno de cada 10 ataques registrados por dicha compañía.

## Las empresas se sienten protegidas

Pero, paradójicamente, el estudio de Continental -titulado “Vehículos Comerciales: Ciberseguridad y Digitalización”- muestra que las empresas de transporte se sienten a salvo: **dos tercios de los encuestados se consideran protegidos contra ciberataques**. Y todo ello a pesar de que **solo la mitad de las empresas dispone de mecanismos de seguridad para protegerse**, ya sean crackeos contra sus vehículos o contra los sistemas de gestión de flotas.

Esa sensación de seguridad ha llevado a las compañías a confiarse. Por eso, **tres cuartas partes de los encuestados no planean realizar más inversiones en ciberseguridad en los próximos 6/12 meses**.



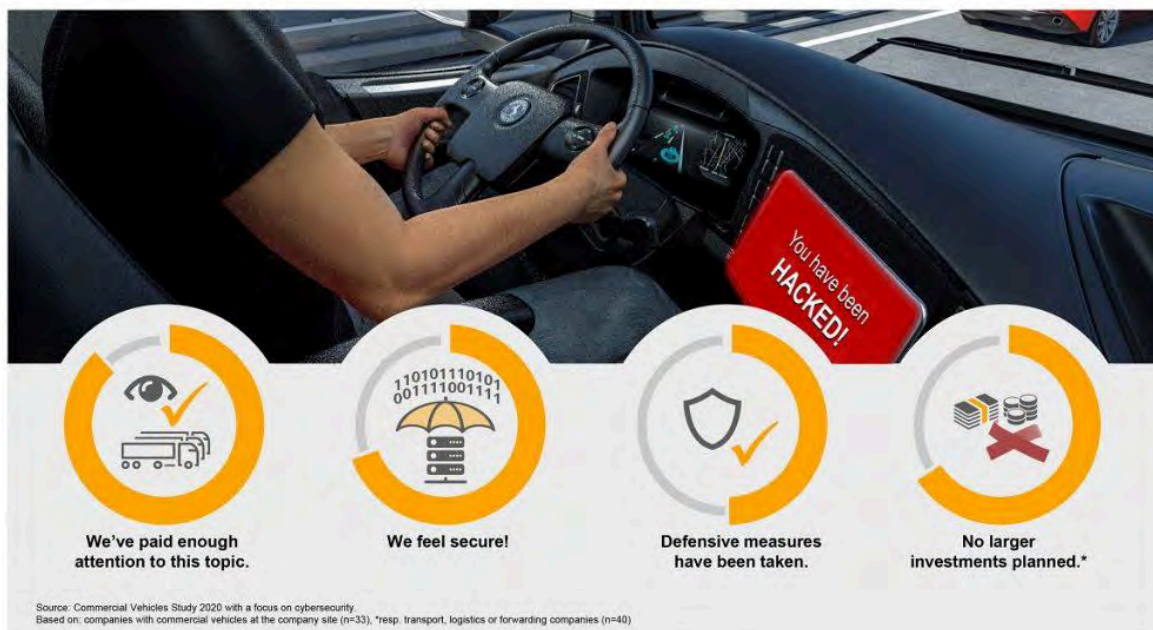


Foto: Continental

Pero esta tendencia podría cambiar cuando, en el futuro, las empresas de transporte y logística sufran aún más ciberataques por estar más digitalizadas. “La ciberseguridad protege los beneficios que se obtienen de la digitalización, lo que es vital para los vehículos industriales, por lo que **merece una mayor atención**”, afirma Gilles Mabire, director en Continental de la Unidad de Negocio de Vehículos y Servicios Comerciales.

## Las empresas pequeñas dudan

Además, el estudio, para el cual se entrevistó a expertos alemanes de diferentes asociaciones y autoridades, además de a empresas de transporte por carretera y proveedores de servicios tecnológicos, muestra **un aspecto clave a la hora de tratar la ciberseguridad** entre los transportistas: depende de si es una pequeña o una gran empresa.

“Existe **una gran brecha entre las grandes compañías y las pequeñas**. Las grandes empresas pueden desarrollar estrategias, contratar especialistas en sistemas informáticos y en ciberseguridad de automoción, así como establecer sus propias unidades cibernéticas. Pero las más pequeñas, a menudo, carecen de la conciencia y de los medios financieros para hacerlo”, dice Dehm.

Por eso, el estudio hace un llamamiento al **desarrollo de soluciones de ciberseguridad que sean asequibles** para todas las compañías.

## **Ciberseguridad total**

Además, el informe explica que las empresas no deben conformarse solo con comprar un software de protección. Las medidas de ciberseguridad deben establecerse con una visión holística del problema. Por eso, se debe **realizar una inversión continua en esta materia**.

“Además de los propios camiones, la ciberseguridad también afecta a toda la infraestructura informática, incluidos los sistemas de gestión de flotas o la organización del trabajo. De ser posible, estas áreas de responsabilidad deberían agruparse ‘en un todo’ para que todas los interfaces entre las áreas sean cubiertas”, señala Mathias Dehm de Continental.

# CÓMO AYUDA LA TECNOLOGÍA A LAS EMPRESAS DE TRANSPORTE

El mundo del transporte está encontrando en la tecnología a un gran aliado. ¿Cuáles son las posibilidades y los cambios que está propiciando? Pudimos escuchar algunas ideas en el Cybertech América Latina.



El mundo del transporte, del reparto y la logística está sufriendo una revolución gracias a la tecnología. Hay nuevos sistemas permiten [simplificar y optimizar procesos](#), además de hacerlos más seguros, y eso redunda en mayor eficiencia y efectividad a la hora de trabajar.



Esas fueron algunas de las conclusiones que se pudieron extraer durante la celebrada Cybertech América Latina. Se trata de un evento anual que reúne a instituciones académicas, gubernamentales, tecnológicas y comerciales con el objetivo de conectar al mundo de la innovación cibernética para combatir los riesgos de ciberseguridad.

Dentro de esa cita, a la que se pudo asistir en formato de videoconferencia, tuvo lugar una charla dedicada al transporte y las comunicaciones, bajo el título de “Ciberseguridad para el transporte y las comunicaciones: mantenerse conectados física y digitalmente”. En ella participaron diversos ponentes procedentes del mundo del transporte y la logística, como **Ilan Shatz**, fundador del [Grupo Aura](#), **Maxim Rebolledo**, consultor de la [Autoridad del Canal de Panamá](#), **Carlos Carbone**, director de operaciones de [DHL Express Panamá](#), y **Franklin Trujillo**, gerente de transporte en [Palacios&Asociados](#).

Ellos explicaron algunas de **las oportunidades que brinda la tecnología al sector del transporte**.

Para Carbone, “la tecnología ayuda a que las entregas puerta a puerta sea más eficiente”.

Ejemplo de esto es lo que comenta EAE [en su blog](#): la constante evolución que sufren los **dispositivos GPS** permiten recopilar y transferir informaciones en tiempo real a otros dispositivos interconectados. En cuanto al reparto, EAE destaca el avance que supondrán los combustibles alternativos y el **uso de drones y dispositivos no**

**tripulados**, los cuales serán un aliado imprescindible de empresas de paquetería y **reparto de corta distancia**.

Por su parte, Trujillo comentó algunos retos y oportunidades que brindará la tecnología a la seguridad logística en América Latina. El experto destacó que uno de los mayores problemas que hay en varios países, como México o Colombia, es el narcotráfico, ya que **las mafias asaltan a camioneros**. Una de las formas que Trujillo sugiere **para corregir ese problema es compartimentar el flujo de la información**. Es decir, que los miembros de la red logística solo tengan acceso a los datos del proceso que les afectan a ellos en concreto. De esta forma, se minimizan las fugas de información que puedan llegar a oídos de los narcotraficantes.

## ¿CÓMO DE VULNERABLES SON LOS COCHES A LOS ATAQUES?

¿Qué pasa si varios juristas analizan un coche conectado? Pues que descubren grietas que pueden conducir a posibles fallos de ciberseguridad... y qué lleva a los ciberdelincuentes a aprovecharlas.



Foto: Elviss Raiļis Bitāns de Pexels

La Universidad Estatal de Michigan -MSU- ha publicado un estudio en la que se analiza **la tecnología de los coches inteligentes desde el punto de vista social**.

El informe, recogido en [Science Daily](#), muestra que algunas tecnologías de conectividad de los automóviles, como el Wifi, el [puerto USB](#), pueden ser una **puerta de entrada para que los ciberdelincuentes penetren en los sistemas de los vehículos**. Una vez dentro, podrían acceder a toda la información e incluso modificarla.

“El riesgo con los vehículos no son solo los [datos personales](#), aunque eso sigue siendo una preocupación real” afirma Thomas Holt, profesor de justicia penal en MSU.

“Digamos que el automóvil está comprometido y un pirata informático altera ciertos sistemas de alerta que le dicen al conductor cuando **la presión de las ruedas es baja** o que los sistemas sensoriales de los frenos de emergencia no se activan. Eso podría provocar la pérdida de vidas” añade el investigador.

## Claves de la ciberseguridad de los coches

Holt descubrió que, **para que un criminal actúe, se deben unir tres factores**: un delincuente motivado, un objetivo adecuado y la falta de un tutor.

Los dos primeros factores parecen claros, pero **¿qué o quién es un tutor y por qué carecen los coches de él?**

La teoría aplicada para la investigación considera que los tutores son **los responsables de los sistemas afectados**. Y el estudio declara que “no hay nadie técnicamente responsable de los sistemas informáticos centrales” de los vehículos.

Holt explicó que, en la industria automotriz tradicional, un fallo en el equipo llevaría a **la retirada del vehículo para solucionar el problema**. Sin embargo, la seguridad cibernética es completamente diferente.

“Es crítico pensar más allá de los umbrales y los retiros del mercado porque la seguridad cibernética no es un problema recuperable, sino que requiere actualizaciones constantes de

parches del sistema, instalaciones y nuevos códigos escritos”, dijo Holt. “Esto es más complicado, pero debe ser un proceso de tutor activo”.

Y, para lograrlo, Holt propone que las marcas saquen **actualizaciones de sus sistemas informáticos que los usuarios se puedan descargar**. De esta manera, los clientes no tendrían que ir al taller para que el mecánico les instale la última versión del software, con las correcciones necesarias para las vulnerabilidades descubiertas. Algo que ya hacen los fabricantes de smartphones y algunos [fabricantes de coches como Tesla](#).

“No podemos esperar que todos los propietarios de vehículos vayan a un concesionario cada vez que haya una actualización de seguridad” añade Holt.

Pero tampoco serviría de nada que los fabricantes creasen esas actualizaciones online si luego [el usuario no las descarga](#). Por eso, el investigador concluye que los dueños de los coches “serán los responsables de proteger sus vehículos y a ellos mismos” descargando las actualizaciones.

## ¿VOLVERÁ A PONERSE DE MODA LA BARRA EN EL VOLANTE?

Hace unos años, una de las medidas disuasorias más importantes de cara a evitar el robo de nuestro coche era recurrir a una barra metálica que impidiese mover el volante. Ahora



puede que ese gadget se vuelva a poner de moda; ¿la razón?



Foto: Pexels en Pixabay.

Como es lógico, no se trata de una moda estética, sino que una vez más, hablamos de una solución sencilla puede evitar que nos roben el coche. No es algo infalible, pero sí una medida para que un ladrón se fije en otro modelo antes que en el nuestro.

Este tipo de antirrobo se pueden localizar en cualquier centro del automóvil, pero **también en tiendas online con precios que van entre los 15 y los 30 euros**. Algunos ejemplos son los modelos de Buygoo [por 16,99 euros](#), el Auto Companion [por 16,07 euros](#), o el Blockauto, por 29,50 euros.

Pero la pregunta importante es... ¿por qué se van a poner de moda este tipo de dispositivos? Para evitar el posible incremento en el robo de vehículos dotados de sistemas de acceso y arranque manos libres; **un dispositivo cada vez más extendido, pero muy utilizado en modelos de alta gama.**

Este sistema funciona de la siguiente manera: se trata de un dispositivo con la clásica forma del mando a distancia de apertura de puertas del coche... pero que, en este caso, basta con llevar encima -en el bolso, un bolsillo, en la mochila...- **para que el coche ‘detecte’ nuestra presencia cuando estamos cerca del vehículo.**

De esta forma, cuando pongamos la mano en alguna de las manecillas de las puertas, el vehículo desbloqueará los seguros de las puertas y podremos acceder al interior para, a continuación, arranca el motor, normalmente con pulsar un botón.

Todo esto es posible **porque coche y llave están en constante comunicación... pero lo hacen ‘en voz bajita’** de tal forma que esta tecnología sólo funciona cuando ambos elementos están cerca y eso es lo que garantizaba, en parte, la seguridad de este dispositivo.

Pero, **¿qué sucedería si llave y coche entendiesen que están cerca... aun estando a una distancia considerable el uno del otro?** Que alguien que no fuese el dueño del coche podría ‘aprovecharse’ para estar en medio, subirse al vehículo, ponerlo en marcha o llevárselo.



¿Y cómo se puede lograr que coche y llave “se hablen en alto”? **Con unos amplificadores y retransmisores de señal... que es el método que está empezando a extenderse en países como Reino Unido o Estados Unidos.** ¿Y cuál es el modus operandi que se está utilizando? Las cámaras de seguridad han registrado muchos de estos robos, y en la mayoría de ellos siempre solían coincidir una serie de factores.

En primer lugar, **suele producirse en viviendas tipo chalet con el coche de los propietarios aparcado junto a la vivienda.** En segundo, en la sustracción del vehículo intervienen dos personas: una de ellas se coloca cerca de la puerta del conductor con uno de los aparatos de amplificación y retransmisión de la señal mientras que la otra se aproxima a la vivienda y comienza a mover el aparato por las paredes de la vivienda.



Foto:

¿El objetivo? **Que el dueño del coche haya dejado las llaves del vehículo en algún lugar dentro de la casa pero cercano a la puerta de entrada** o alguna de las paredes que den hacia el lugar de la calle donde está aparcado el coche.

De ser así, y por el funcionamiento de esos amplificadores, coche y llave pensarán que están próximos, de tal manera que al delincuente que esté cerca de la puerta del vehículo le basta con poner la mano en la manecilla de la puerta para que los seguros se desbloqueen.

## Cuestión de pocos segundos

Otra característica de este tipo de sustracciones es que el robo de los coches apenas conlleva unos pocos segundos o, como mucho, un par de minutos. Y, como decíamos, no es un caso aislado, sino que ya se han registrado varios casos. **Por poner algunos ejemplos, unos delincuentes logran robar dos Lexus durante una noche**, y a los mismos propietarios, la familia Downey, en la localidad candiense de Ottawa, en el año 2018.

Los robos se producen justo en la misma puerta del domicilio de los propietarios de los coches, lo que parece mostrar que se trata de un crackeo de los vehículos llevado a cabo mediante el sistema de retransmisión de señal de la llave remota de los vehículos.

Más recientemente, en 2020, un ladrón recurre a un **sistema de relevos para amplificar la señal de las llaves remotas**

y **acceder a los vehículos aparcados** en la entrada de las casas, todas ellas en la localidad de Peterborough, en Reino Unido. El método empleado le funciona en coches como **un Nissan Juke**, un Volvo XC60 o un Ford Mondeo, entre otros -pero de anteriores generaciones-.

Otro caso más, esta vez en Irlanda y también este año, **muestra cómo los ladrones consiguen hacerse con un BMW Serie 6** que está aparcado con la entrada de la casa de su propietario, en el Condado de Down -Irlanda-. Al parecer, los delincuentes emplean el método de ampliar la señal de la llave remota, que se encuentra dentro de la vivienda.

## ¿CÓMO PUEDES SABER SI TE ESTÁN CIBERATACANDO?

Entrenar es la clave para mejorar cualquier habilidad. ¿Existe alguna forma de aprender a diferenciar qué es un ciberataque de lo que no lo es? Sí: esta plataforma de aprendizaje.



Photo by Jonathan Borba from Pexels

Un día, llega a tu **correo electrónico** corporativo un mensaje de una fuente desconocida. ¿Lo abres o no? ¿Descargas los documentos adjuntos? Cuidado, porque podría ser un ciberataque y la liarías si le haces caso. O podría ser un auténtico mail del trabajo y te pondría en problemas con tu jefe si pasas de él.

**¿Cómo puedes diferenciar un ciberataque de lo que no lo es?**

Lo mejor es que estés entrenado para cuando llegue ese momento.

Una solución para estar alerta es **Attack Simulator**. Es una plataforma de aprendizaje en ciberseguridad que ofrece servicios de **concienciación, entrenamiento y formación**

de todos sus clientes de forma automatizada y sencilla que acaba de actualizarse.

¿Cómo funciona? **Envía de forma automática diversos tipos de ciberataques simulados.** Con estos ensayos -que tienen lugar directamente en el ordenador- se puede concienciar, formar y mantener en alerta al personal de una compañía sobre los riesgos de la red y los ciberataques. Es decir, si se está habituado a tratar con ataques simulados día a día, sabrá reconocer uno de verdad y actuar para bloquearlo.

Algunos de los ataques simulados son:

- **Ransomware:** Un **secuestro informático**. Es un programa malicioso que secuestra el equipo infectado y no deja que se use con normalidad. Normalmente, el atacante pide un rescate económico para desbloquearlo.
- **Phishing:** Un tipo de ataque que busca engañarte -usualmente a través de un correo electrónico que suplanta a una empresa- para que le des tus datos personales.
- **Malware:** Cualquier software maligno.
- **Exploits:** Acceder a un sistema informático de forma no autorizada, o bloquearlo o tomar su control.
- **Privacidad.**
- **Fraude.**

Según informa **INGECOM**, distribuidor de Attack Simulator en España, las actualizaciones que incluye esta nueva versión



se basan en las sugerencias de los partners y se ha creado una nueva consola con un nuevo diseño más intuitivo y amigable.

## Los crackers entran por el correo electrónico

“Hace tiempo que sabemos que **el correo electrónico es el principal vector de infección**, pero eso unido al gran incremento de ataques de ransomware ‘empresarial’, así como de suplantación de identidad y robo de credenciales, entre otros, está haciendo evidente la necesaria e ineludible concienciación de los usuarios en las empresas” señala Carles Gil, Country Manager de Attack Simulator.

“Los recientes ataques de los últimos meses han dejado claro que, a pesar de las tecnologías defensivas y otros motivos, **los ciberdelincuentes están llegando a los usuarios finales**, dejando la seguridad, la productividad y la reputación de las empresas y entidades, en muchos casos, pendientes de un solo clic. Attack Simulator fue concebido específicamente para ayudar a las personas y a las empresas a evitar esos posibles clics” concluye el directivo.

# CÓMO TE ESPÍAN SIN DARTE CUENTA... Y CÓMO EVITAR QUE LO HAGAN

Los ciberataques están a la orden del día y cualquiera puede ser víctima de ellos. No pienses que nadie va a poner el foco en ti: los crackers no hacen ascos a nadie. Estas son las formas más habituales de atacarte.



“¿Quién va a querer **espiarme a mí si no soy nadie importante ni mis datos valen nada?**” Es la pregunta habitual que reciben los expertos en ciberseguridad cuando intentan concienciar a algún usuario sobre la importancia de [mantener una serie de rutinas para proteger su privacidad](#) y evitar así ser víctima de un ciberataque.



Sin embargo, pensar así supone no tener en cuenta los riesgos reales. **“Cualquier usuario es importante para un ciberdelincuente**, ya sea como objetivo de una extorsión o con fines incluso más peligrosos, como convertir su dispositivo en el elemento desde el que lanzar un ataque y convertirle, por tanto, no sólo en víctima sino también en colaborador involuntario del delincuente” explican desde ESET, una empresa especializada en ciberseguridad.

## Las puertas de entrada

Hay **diversas formas de espiar al usuario de un dispositivo móvil**. Incluso de espiar a otra persona que no sea el propio usuario -como la aplicación de La Liga, que [usaba el micrófono de los smartphones](#) para detectar bares que emitiesen partidos de fútbol sin permiso-. Según ESET, **estos son las vías de entrada más utilizadas por los ciberdelinquentes para infectar dispositivos** de usuarios desprevenidos:

- **Correo electrónico:** un clásico que no pasa de moda y que en 2023 volvió a ser uno de los principales medios por los que se propaga el [malware](#). Ya sea mediante ficheros adjuntos, como una hoja de cálculo que contiene una supuesta factura o un currículum enviado en formato PDF, o utilizando enlaces dentro del cuerpo del mensaje que redirigen a webs o descargas maliciosas, esta técnica sigue funcionando tan bien como lo hacía hace años.



- **Aplicaciones troyanizadas:** la introducción de software espía en aplicaciones supuestamente inofensivas es otro clásico imperecedero. Con esta forma de ataque, cuando el usuario se descarga la app, descarga también el programa malicioso que contiene, infectando así su dispositivo. Los delincuentes han adaptado esta técnica a los dispositivos móviles, llegando incluso a colocar sus creaciones en tiendas de aplicaciones oficiales como Google Play.
- **Webs maliciosas:** pueden existir webs maliciosas o vulneradas, preparadas por los delincuentes y que descargan automáticamente malware en nuestro ordenador o dispositivo móvil aprovechándose de alguna vulnerabilidad no solucionada. Esta técnica es especialmente peligrosa si se combina con el envío de un enlace mediante alguno de los otros medios mencionados en este apartado.
- **Redes sociales:** el punto de encuentro para los usuarios también es un posible punto de propagación de amenazas. Aprovechándose de su popularidad, los delincuentes crean campañas para engañar a los usuarios con titulares llamativos o utilizando los sistemas de mensajería interna.
- **Mensajería instantánea:** WhatsApp o Telegram son aplicaciones instaladas en cientos de millones de dispositivos, así que no es de extrañar que sean uno de los vectores de infección más peligrosos actualmente. La rápida capacidad de propagación que tienen las amenazas en forma de enlaces o adjuntos

maliciosos a través de estas aplicaciones no pasa desapercibida para los criminales.

## ¿Qué pueden hacerte?

Una vez revisados cuales son los principales vectores de ataque, **las amenazas más recurrentes** con las que los ciberdelincuentes atacan a la privacidad de los usuarios con fines ilícitos se pueden resumir en:

- **Keylogger:** uno de los malware más clásicos, especializado en robar credenciales. Este tipo de programas registra las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un fichero o enviarlas a través de internet. Se suele utilizar para acceder a perfiles de redes sociales, cuentas de correo o incluso aplicaciones de banca online y espiar información personal, la de nuestros contactos o incluso realizar una suplantación de identidad.
- **Remote Access Tool -RAT-:** sirven para controlar desde la distancia un dispositivo. Si bien la mayoría de veces se utilizan estas herramientas con un buen propósito -como en departamentos de soporte técnico-, los delincuentes pueden llegar a instalarlas en los equipos de sus víctimas y, a partir de ahí, espiar no solo el contenido de su disco o lo que están viendo por la pantalla -como hacía recientemente el malware Varenky-, sino también activar la cámara o el micrófono.



- **Redes WiFi comprometidas:** aunque la seguridad de muchos de los servicios online y aplicaciones ha mejorado considerablemente en los últimos años, esto no significa que debemos bajar la guardia a la hora de conectarnos a una red WiFi que no sea de confianza. Los delincuentes siguen teniendo la capacidad de espiar nuestras comunicaciones si no nos andamos con cuidado por lo que se recomienda evitarlas y utilizar una solución VPN.
- **Robos de credenciales:** las credenciales de acceso a los servicios online son un bien muy preciado por los delincuentes, por lo que siguen usándose con frecuencia páginas de phishing -suplantando la identidad de empresas o servicios reales- junto con otras técnicas. Además, existen bases de datos de millones de credenciales con las que los delincuentes trafican y que sirven para acceder a las cuentas de usuarios de todo el mundo, robando información confidencial o incluso realizando chantajes. Por ello se recomienda configurar, siempre que sea posible, el doble factor de autenticación.
- **SIM Swapping:** Los ataques de este tipo han estado aumentando de forma preocupante en los últimos meses, especialmente en Estados Unidos. Los delincuentes consiguen obtener datos personales de sus víctimas y se hacen pasar por ellas para conseguir un duplicado de la tarjeta SIM. Con este duplicado, los delincuentes pueden suplantar la identidad de sus víctimas y acceder a varias cuentas online solicitando una recuperación de su cuenta. Mediante esta técnica se consiguen evadir la

protección ofrecida por el doble factor de autenticación basado en SMS -utilizado sobre todo en las transferencias bancarias-, por lo que se recomienda utilizar otros métodos de doble autenticación, como son el uso de aplicaciones dedicadas o el reconocimiento biométrico.

## Toma precauciones

“En general, **con una serie de precauciones sencillas**, como desconfiar de mensajes no esperados, procedentes de remitentes desconocidos, con informaciones erróneas o llenas de faltas de ortografía, y con la instalación de una solución de seguridad y la actualización de las aplicaciones y sistema operativo de nuestros dispositivos, **los delincuentes tendrán más complicado atentar contra nuestra privacidad**”, afirma [Josep Albors](#), responsable de concienciación e investigación en ESET España.

# ¿QUÉ PRECIO PODRÍAN TENER LOS DATOS DE TU COCHE EN EL MERCADO NEGRO?

Desde información privada sobre tu agenda de contactos hasta la posibilidad de ayudar en la ejecución de un secuestro. Un coche conectado encierra información muy valiosa para los crackers, como tus rutas y horarios.



**Juan Díez, experto en ciberseguridad del Instituto Nacional de Ciberseguridad español, declaró para el medio**



digital 'Última Hora' que **la venta de historiales médicos en la *darkweb* fluctúa desde los 35 hasta los 900 euros.**

Comparados con la venta de datos de tarjeta de crédito, que no suelen superar la decena de euros, la de Juan Díez es una declaración que **pone de manifiesto cuál es la moneda actual más valiosa: los datos.**

En esta era de la movilidad, donde los **vehículos conectados se han convertido en el día a día de la industria**, surge una inquietante pregunta: **¿podrían nuestros vehículos ser el próximo objetivo de la *darkweb*?** Podemos asumir -pues es una realidad- que **los coches actuales analizan y almacenan una gran cantidad de datos sensibles que podrían poner en peligro nuestra privacidad**, además de convertirse en una mina para los *crackers*.

Un **cracker** que consiguiera hacerse con los datos de un **vehículo podría conocer las rutas más comunes de la víctima, los destinos más frecuentados, sus horarios de conducción en su cotidianidad** -a qué hora va y regresa del trabajo-, **la agenda de su teléfono, las credenciales de cualquier aplicación que esté vinculada al sistema multimedia**, el manejo del vehículo: frenazos, acelerones, poco respeto a las indicaciones viales... Incluso, en las situaciones más estrafalarias, si el coche cuenta con cámaras *on-board*, podría hacerse hasta con dichas grabaciones.



## ¿Cómo podrían robar los datos de tu vehículo?

Aprovechando **vulnerabilidades en sistemas de info-entretenimiento poco seguros**, los ciberdelincuentes podrían acceder a datos almacenados en el vehículo.

También, podrían **atacar a través de intercepciones de comunicaciones entre vehículo y las redes**, en las cuales una falta de cifrado robusto en la comunicación entre vehículo y servidores podría permitir la interceptación de datos.

Los *crackers* podrían acceder **a través de la red interna del vehículo mediante ataques remotos, aprovechando debilidades en la seguridad de las comunicaciones inalámbricas**. Otra posibilidad sería la de aprovechar para introducir malware en las actualizaciones periódicas que lanzan las compañías para sus modelos -como las que debes hacerle a tu móvil cada cierto tiempo-, o suplantación de la **identidad de fuentes seguras para provocar que el vehículo se comuniquen con fuentes maliciosas en lugar de servidores legítimos**. Las aplicaciones móviles vinculadas al vehículo son otro gran punto de entrada, ya que suelen gestionar directamente información sensible entre el propietario y el propio coche.

Si bien es complicado establecer el precio al que estos datos podrían venderse, obtener información de este calibre sobre **vehículos oficiales de dirigentes políticos o de personajes públicos podría estimarse cerca de la decena de miles de euros**. Para vehículos de ciudadanos de a pie,

el precio rondaría el baremo que tienen los informes médicos, pudiendo acercarse al millar de euros, en caso de conocerse una información muy delicada de la persona a través de su coche.



*Imagen generada por la Inteligencia Artificial Bing*

## La importancia de ciber-proteger tu vehículo

Por razones como esta, **la ciberseguridad en la movilidad se vuelve tan capital en los últimos años. Normativas como la UNECE/R155** han querido adelantarse a que situaciones así se vuelvan recurrentes y obligará a que, a partir de julio del 2024, todos los vehículos que se fabriquen en y para Europa cumplan con unos requisitos mínimos de ciberseguridad, contando con una certificación de

ciberseguridad que acredite que la persona no encuentra vulnerados sus derechos de privacidad.

España se encuentra entre las naciones pioneras en este campo, con **empresas como la vasca EUROCYBCAR**, que ha desarrollado el primer test que mide la ciberseguridad del vehículo y emite un certificado acorde a la UNECE. Pues no solo la privacidad puede verse vulnerada por ataques hacia los vehículos.

Si es tu primera vez en **HackerCar**, **puede que no conozcas los peligros de seguridad que suponen los crackeos**: un mensaje al propietario sobre el mal estado de unos neumáticos que están correctos; forzar a la parada del vehículo y accionar las ventanillas o las puertas del vehículo; movimientos bruscos del volante; comportamientos anómalos de algunos sistemas del vehículo; movimientos inesperados del volante e incluso mal funcionamiento de los frenos...

Aún así, es **clave recordar la importancia de que el usuario también colabore con una serie de medidas**: cambiar las contraseñas de fábrica, desconectar el Wi-Fi si no se está utilizando, actualizar el software del vehículo cuando se lo indique el fabricante, desconectar sistemas o tecnologías cuando no las utilice -como el Wi-Fi-, eliminar la agenda de contactos del sistema **Bluetooth** o asegurarse de que los dispositivos que vincule al vehículo sean seguros.



# **Las mejores prácticas de ciberseguridad para vehículos modernos**

***Pre-Final***

# Cybersecurity Best Practices for the Safety of Modern Vehicles

*Release 2022*



U.S. Department of Transportation  
**National Highway Traffic Safety  
Administration**

# 2022 Update Release Notes

- Reorganized for readability.
- Recent industry standards such as ISO/SAE 21434 have been considered for applicability to NHTSA’s guidance regarding appropriate corporate processes.
- Recommendations have been enumerated and updated based on best available research results, industry standards, real world incidents, general cybersecurity knowledge, and in response to comments on the 2016 draft document.
  - Throughout this document, “General best practices” elements are enumerated using the [G.n<sub>i</sub>] convention and “Technical best practices” elements are enumerated using the [T.n<sub>j</sub>] convention, where n<sub>i</sub>, and n<sub>j</sub> respectively represent the “i<sup>th</sup>” and “j<sup>th</sup>” element of the general and technical best practices covered in this document. NHTSA adopted this approach to make it easier for readers to follow and comment on recommendations within this best practice document.

## Table of Contents

|        |                                                                              |    |
|--------|------------------------------------------------------------------------------|----|
| 1.     | Purpose of This Document .....                                               | 1  |
| 2.     | Scope .....                                                                  | 1  |
| 3.     | Background.....                                                              | 2  |
| 4.     | General Cybersecurity Best Practices.....                                    | 3  |
| 4.1    | Leadership Priority on Product Cybersecurity .....                           | 4  |
| 4.2    | Vehicle Development Process with Explicit Cybersecurity Considerations ..... | 4  |
| 4.2.1  | Process .....                                                                | 4  |
| 4.2.2  | Risk Assessment .....                                                        | 5  |
| 4.2.3  | Sensor Vulnerability Risks.....                                              | 5  |
| 4.2.4  | Unnecessary Risk Removal .....                                               | 5  |
| 4.2.5  | Protections.....                                                             | 6  |
| 4.2.6  | Inventory and Management of Software Assets on Vehicles .....                | 6  |
| 4.2.7  | Penetration Testing and Documentation .....                                  | 6  |
| 4.2.8  | Monitoring, Containment, Remediation .....                                   | 7  |
| 4.2.9  | Data, Documentation, Information Sharing .....                               | 7  |
| 4.2.10 | Continuous risk monitoring and assessment .....                              | 7  |
| 4.2.11 | Industry best practices.....                                                 | 8  |
| 4.3    | Information Sharing .....                                                    | 8  |
| 4.4    | Security Vulnerability Reporting Program .....                               | 9  |
| 4.5    | Organizational Incident Response Process .....                               | 9  |
| 4.6    | Self-Auditing.....                                                           | 11 |
| 4.6.1  | Process management documentation .....                                       | 11 |
| 4.6.2  | Review and audit.....                                                        | 11 |
| 5.     | Education.....                                                               | 12 |



|       |                                                                           |    |
|-------|---------------------------------------------------------------------------|----|
| 6.    | Aftermarket/User Owned Devices.....                                       | 12 |
| 6.1   | Vehicle manufacturers .....                                               | 12 |
| 6.2   | Aftermarket device manufacturers.....                                     | 12 |
| 7.    | Serviceability.....                                                       | 13 |
| 8.    | Technical Vehicle Cybersecurity Best Practices.....                       | 13 |
| 8.1   | Developer/Debugging Access in Production Devices .....                    | 13 |
| 8.2   | Cryptographic Credentials .....                                           | 14 |
| 8.3   | Vehicle Diagnostic Functionality.....                                     | 14 |
| 8.4   | Diagnostic Tools .....                                                    | 15 |
| 8.5   | Vehicle Internal Communications .....                                     | 15 |
| 8.6   | Event Logs .....                                                          | 16 |
| 8.7   | Wireless Paths into Vehicles.....                                         | 16 |
| 8.7.1 | Wireless Interfaces.....                                                  | 16 |
| 8.7.2 | Segmentation and Isolation Techniques in Vehicle Architecture Design..... | 16 |
| 8.7.3 | Network Ports, Protocols, and Services .....                              | 17 |
| 8.7.4 | Communication to Back-End Servers.....                                    | 17 |
| 8.7.5 | Capability to Alter Routing Rules.....                                    | 17 |
| 8.8   | Software Updates / Modifications.....                                     | 17 |
| 8.9   | Over-the-Air Software Updates .....                                       | 18 |
|       | Appendix .....                                                            | 19 |
|       | Terms and Descriptions .....                                              | 19 |

## 1. Purpose of This Document

This document from the National Highway Traffic Safety Administration (NHTSA) updates the Agency's non-binding and voluntary guidance to the automotive industry for improving motor vehicle cybersecurity. NHTSA encourages vehicle and equipment manufacturers to review this guidance to determine whether and, if so, how to apply this guidance to their unique systems.

Vehicles are cyber-physical systems<sup>1</sup> and cybersecurity vulnerabilities could impact safety. NHTSA has made vehicle cybersecurity an organizational priority, and it is important for automotive industry suppliers and manufacturers to do so as well. This includes proactively adopting and using available guidance, such as this document, as well as existing standards and best practices. Prioritizing vehicle cybersecurity also means establishing internal processes and strategies to ensure systems will be safe under expected real-world conditions, including in the presence of potential vehicle cybersecurity threats. The automotive cybersecurity environment is dynamic and is expected to change continually and quickly.<sup>2</sup>

NHTSA believes the voluntary best practices described in this document provide a solid foundation for developing a risk-based approach to cybersecurity challenges, and describes important processes that can be maintained, refreshed and updated effectively over time to serve the needs of the automotive industry.

## 2. Scope

This document is intended to cover cybersecurity issues for all motor vehicles<sup>3</sup> and motor vehicle equipment (including software)<sup>4</sup> and is therefore applicable to all individuals and organizations designing and manufacturing vehicle electronic systems and software. These entities include, but are not limited to,

---

<sup>1</sup> National Science Foundation defines cyber-physical systems (CPS) as engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components, available at [https://www.nsf.gov/funding/pgm\\_summ.jsp?pims\\_id=503286](https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286).

<sup>2</sup> Chetan Sharma Consulting suggests that as of quarter 1 in 2019, AT&T estimated that the total number of connected vehicles on the AT&T network in the U.S. market is 32 million vehicles. *See* <http://www.chetansharma.com/publications/us-mobile-market-update-q1-2019/>.

<sup>3</sup> "Motor vehicle" means a vehicle driven or drawn by mechanical power and manufactured primarily for use on public streets, roads, and highways. 49 U.S.C. § 30102(a)(7).

<sup>4</sup> "Motor vehicle equipment" means—

(A) any system, part, or component of a motor vehicle as originally manufactured;

(B) any similar part or component manufactured or sold for replacement or improvement of a system, part, or component, or as an accessory or addition to a motor vehicle; or

(C) any device or an article or apparel, including a motorcycle helmet and excluding medicine or eyeglasses prescribed by a licensed practitioner, that—

(i) is not a system, part, or component of a motor vehicle; and

(ii) is manufactured, sold, delivered, or offered to be sold for use on public streets, roads, and highways with the apparent purpose of safeguarding users of motor vehicles against risk of accident, injury, or death. *See* 49 U.S.C. § 30102(a)(8).

small and large volume motor vehicle and motor vehicle equipment designers, suppliers, manufacturers, modifiers, and alterers.

While the cybersecurity recommendations in this document have broad applicability, the implementation by all sizes and tiers of automotive entities would be expected to vary among them. Importantly, all individuals and organizations involved in the design, manufacturing, assembly and maintenance of a motor vehicle have a critical role to play with respect to vehicle cybersecurity. The security of a system is measured by its weakest link. Organizations within the automotive supply chain should set clear cybersecurity expectations for their suppliers that are consistent with the best practices outlined in this document and support their own verified implementation.

### **3. Background**

In 2016, NHTSA issued “Cybersecurity Best Practices for Modern Vehicles,”<sup>5</sup> which described NHTSA’s non-binding guidance to the automotive industry for improving motor vehicle cybersecurity. This document provides an update to those practices based on knowledge gained through research and industry activities over the past six years. Since 2016, both NHTSA and the automotive industry have continued to invest in and collaborate on the critical vehicle safety implications of cybersecurity. Additionally, industry organizations took a number of proactive steps that include increased industry membership and participation in the Automotive Information Sharing and Analysis Center (Auto-ISAC), publication of industry best practices documents, and development of new voluntary standards.

This document builds upon the progress industry and NHTSA have made since 2016 and considers the emerging voluntary standards, such as the International Standards Organization (ISO)/SAE International (SAE) Final Draft International Standard (FDIS) 21434, “Road Vehicles – Cybersecurity engineering.”<sup>6</sup> The ISO/SAE 21434 standard is a consensus of expert recommendations from 82 companies and 16 nations addressing important subjects such as:

- Cybersecurity organization and governance;
- Cybersecurity engineering throughout the lifecycle; and
- Post-production processes.

In addition, the Auto-ISAC, through its members, developed a series of Best Practice Guides as resources<sup>7</sup> to the industry on a range of important vehicle cybersecurity issues including:

- Incident Response;
- Collaboration and Engagement with Appropriate Third Parties;
- Governance;
- Risk Assessment and Management;
- Awareness and Training;

---

<sup>5</sup> National Highway Traffic Safety Administration (2016), *Cybersecurity Best Practices for Modern Vehicles*, available at: [https://www.nhtsa.gov/staticfiles/nvs/pdf/812333\\_CybersecurityForModernVehicles.pdf](https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf).

<sup>6</sup> ISO/SAE 21434:2021 *Road vehicles – Cybersecurity engineering*, available at: <https://www.iso.org/standard/70918.html> and <https://www.saemobilus.sae.org>

<sup>7</sup> Auto-ISAC, available at: <https://automotiveisac.com/best-practices/download-best-practice-guides/>.

- Threat Detection, Monitoring and Analysis; and
- Security Development Lifecycle.

ISO/SAE 21434 and the Auto-ISAC best practice guides provide additional resources to the automotive industry to help organizations strengthen their organizational and vehicular cybersecurity practices and implement product cybersecurity best practices and voluntary standards.

## 4. General Cybersecurity Best Practices

NHTSA’s policy and research focus on practices and solutions that are expected to result in strengthening vehicles’ electronic architectures to protect against potential attacks and to help ensure vehicle systems take appropriate and safe actions, even when an attack is successful.

A layered approach to vehicle cybersecurity, an approach which assumes some vehicle systems could be compromised, reduces the probability of an attack’s success and mitigates the ramifications of unauthorized vehicle system access.

[G.1<sup>8</sup>] The automotive industry should follow the National Institute of Standards and Technology’s (NIST’s) documented Cybersecurity Framework,<sup>9</sup> which is structured around the five principal functions “Identify, Protect, Detect, Respond, and Recover,” to build a comprehensive and systematic approach to developing layered cybersecurity protections for vehicles.

This approach should:

- Be built upon risk-based prioritized identification and protection of safety-critical vehicle control systems;
- Eliminate sources of risks to safety-critical vehicle control systems where possible and feasible;
- Provide for timely detection and rapid response to potential vehicle cybersecurity incidents in the field;
- Design-in methods and processes to facilitate rapid recovery from incidents when they occur; and
- Institutionalize methods for accelerated adoption of lessons learned (e.g. vulnerability sharing) across the industry through effective information sharing, such as participation in the Auto-ISAC.

---

<sup>8</sup> Throughout this document, “General best practices” elements are enumerated using the [G.n<sub>i</sub>] convention and “Technical best practices” elements are enumerated using the [T.n<sub>i</sub>] convention, where n<sub>i</sub> and n<sub>i</sub> respectively represent the “i<sup>th</sup>” and “j<sup>th</sup>” element of the general and technical best practices covered in this document.

<sup>9</sup> The current version of this document, at the time of publication, is: Matthew P. Barrett, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (National Institute of Standards and Technology, NIST, April 16, 2018), and is available at: <https://doi.org/10.6028/NIST.CSWP.04162018>.

## 4.1 Leadership Priority on Product Cybersecurity

It is essential for automotive industry suppliers and manufacturers to create corporate priorities and foster a culture prepared and able to handle increasing cybersecurity challenges associated with motor vehicles and motor vehicle equipment.

Emphasizing the importance of cybersecurity from the leadership level down to the staff level demonstrates the seriousness of effectively managing cybersecurity risks and will help the organization better prioritize cybersecurity throughout product development. This emphasis enables a proactive cybersecurity culture to follow from the leadership positions within the organization. In addition, it facilitates the product development cycle to consider cybersecurity protections early in the design phases. Along these lines,

- [G.2] Companies developing or integrating vehicle electronic systems or software should prioritize vehicle cybersecurity and demonstrate executive management commitment and accountability by:
  - [a] Allocating dedicated resources within the organization focused on researching, investigating, implementing, testing, and validating product cybersecurity measures and vulnerabilities;
  - [b] Facilitating seamless and direct communication channels through organizational ranks related to product cybersecurity matters; and
  - [c] Enabling an independent voice for vehicle cybersecurity-related considerations within the vehicle safety design process.

For example, companies can demonstrate leadership priority by taking actions such as appointing a high-level corporate officer who is directly responsible and accountable for product cybersecurity and providing this executive with appropriate staff, authority, and resources.<sup>10</sup>

## 4.2 Vehicle Development Process with Explicit Cybersecurity Considerations

Cybersecurity considerations encompass the full lifecycle of the vehicle, which includes conception, design, manufacture, sale, use, maintenance, resale, and decommissioning. Organizations have more flexibility to design in protections, as well as functionality that can facilitate containment and recovery solutions, early in the development process.

### 4.2.1 Process

- [G.3] The automotive industry should follow a robust product development process based on a systems-engineering approach with the goal of designing systems free of

---

<sup>10</sup> ISO/SAE 21434 [RQ-05-01] requires that “The organization shall define a cybersecurity policy that includes: b) the executive management’s commitment to manage the corresponding risks.” Further ISO/SAE 21434 annexes provide further guidance on nurturing a strong cybersecurity culture.

unreasonable safety risks, including those from potential cybersecurity threats and vulnerabilities.

#### 4.2.2 Risk Assessment

[G.4] This process should include a cybersecurity risk assessment step<sup>11</sup> that is appropriate and reflects mitigation of risk for the full life-cycle of the vehicle.

[G.5] Safety of vehicle occupants and other road users should be of primary consideration when assessing risks.

#### 4.2.3 Sensor Vulnerability Risks

An emerging area of cybersecurity is the potential manipulation of vehicle sensor data. It is prudent for manufacturers to consider that vehicle systems and their behavior could be influenced through sensor signal manipulation in addition to traditional software/firmware modifications.

[G.6] Manufacturers should consider the risks associated with sensor vulnerabilities and potential sensor signal manipulation efforts such as GPS spoofing,<sup>12</sup> road sign modification,<sup>13</sup> Lidar/Radar jamming and spoofing,<sup>14</sup> camera blinding,<sup>15</sup> and excitation of machine learning false positives.<sup>16</sup>

#### 4.2.4 Removal or Mitigation of Safety-Critical Risks

[G.7] Any unreasonable risk to safety-critical systems should be removed or mitigated to acceptable levels through design, and any functionality that presents an unavoidable and unnecessary risk should be eliminated where possible.

---

<sup>11</sup> A risk assessment process is described in clause 15 of ISO/SAE 21434. The work product [WP-09-02] “Threat analysis and risk assessment” results from requirements [RQ-09-03] and [RQ-09-04] which pull from several clause 15 sections.

<sup>12</sup> DefCon 23 – Lin Huang and Qing Yang – *Low cost GPS Simulator: GPS Spoofing by SDR*. 2015 Video of the talk: <https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20video/>

<sup>13</sup> McAfee Labs, *Model Hacking ADAS to Pave Safer Roads for Autonomous Vehicles* 2020, available at: <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/model-hacking-adas-to-pave-safer-roads-for-autonomous-vehicles/>.

<sup>14</sup> Mark Harris, IEEE Spectrum Sept 4, 2015, *Researcher Hacks Self-driving Car Sensors*.

<sup>15</sup> Petit, J. et al., “Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR.” 2015, available at: <https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers-wp1.pdf>.

<sup>16</sup> Tencent Keen Security Lab, *Experimental Security Research of Tesla Autopilot* 2019, available at: [https://keenlab.tencent.com/en/whitepapers/Experimental\\_Security\\_Research\\_of\\_Tesla\\_Autopilot.pdf](https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Research_of_Tesla_Autopilot.pdf).

#### 4.2.5 Protections

- [G.8] For remaining functionality and underlying risks, layers of protection<sup>17</sup> that are appropriate for the assessed risks should be designed and implemented.
- [G.9] Clear cybersecurity expectations should be specified and communicated to the suppliers that support the intended protections.<sup>18</sup>

#### 4.2.6 Inventory and Management of Hardware and Software Assets on Vehicles

- [G.10] Suppliers and vehicle manufacturers should maintain a database of their operational hardware and software components<sup>19,20</sup> used in each automotive ECU, each assembled vehicle, and a history log of version updates applied over the vehicle's lifetime.
- [G.11] Manufacturers should track sufficient details related to software components,<sup>21</sup> such that when a newly identified vulnerability is identified related to an open source or off-the-shelf software,<sup>22</sup> manufacturers can quickly identify what ECUs and specific vehicles would be affected by it.

#### 4.2.7 Cybersecurity Testing and Vulnerability Identification

- [G.12] Manufacturers should evaluate all commercial off-the-shelf and open-source software components used in vehicle ECUs against known vulnerabilities.<sup>23,24,25</sup>
- [G.13] Manufacturers should also pursue product cybersecurity testing, including using penetration tests, as part of the development process.<sup>26</sup>
- [G.14] Test stages should employ qualified testers who have not been part of the development team, and who are highly incentivized to identify vulnerabilities.

---

<sup>17</sup> See the appendix's Terms and Definitions entry for "Layered Protections"

<sup>18</sup> ISO/SAE 21434 Clause 7 "Distributed Cybersecurity Activities" discusses customer- supplier relationships and various recommendations for how to manage cybersecurity risks among these entities, including the interactions, dependencies, and responsibilities between customers and suppliers for cybersecurity activities.

<sup>19</sup> This is also referred to as a software bill of materials (SBOM), which is a list of components in a piece of software, including assembled open source and commercial software components.

<sup>20</sup> Multistakeholder Process on Promoting Software Component Transparency, 83 Fed. Reg. 110 (June 4, 2018).

<sup>21</sup> These details could include: the licenses that govern those components, the versions of the components used in the codebase, and their patch status.

<sup>22</sup> A good example would be the vulnerability associated with the Transport Layer Security(TLS) implementations in OpenSSL 1.0.1 before 1.0.1g in the Heartbleed vulnerability: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-0160>.

<sup>23</sup> MITRE Common Vulnerabilities and Exposures (CVE) may be found at: <https://cve.mitre.org/>.

<sup>24</sup> NIST's National Vulnerability Database may be found at: <https://nvd.nist.gov/>.

<sup>25</sup> ISO/SAE 21434's [RQ-06-21] and clause 6 in general discuss the integration of off-the-self components.

<sup>26</sup> ISO/SAE 21434 recommends penetration testing as part of [RC-10-12] the cybersecurity validation requirements and recommendations.



- [G.15] A vulnerability analysis should be generated for each known vulnerability assessed or new vulnerability identified during cybersecurity testing. The disposition of the vulnerability and the rationale for the how the vulnerability is managed should also be documented.<sup>27</sup>

#### 4.2.8 Monitoring, Containment, Remediation

- [G.16] In addition to design protections, the automotive industry should establish rapid vehicle cybersecurity incident detection and remediation capabilities.<sup>28</sup>
- [G.17] Such capabilities should be able to mitigate safety risks to vehicle occupants and surrounding road users when a cyber-attack is detected and transition the vehicle to a minimal risk condition, as appropriate for the identified risk.

#### 4.2.9 Data, Documentation, Information Sharing

- [G.18] Manufacturers should collect information on potential attacks,<sup>29</sup> and this information should be analyzed and shared with industry through the Auto-ISAC and other sharing mechanisms.<sup>30</sup>
- [G.19] Manufacturers should fully document any actions, design choices, analyses, supporting evidence, and changes related to its management of vehicle cybersecurity.
- [G.20] All related work products should be traceable within a robust document version control system.<sup>31</sup>

#### 4.2.10 Continuous risk monitoring and assessment

- [G.21] Companies should use a systematic and ongoing process to periodically re-evaluate risks and make appropriate updates to processes and designs due to changes in the vehicle cybersecurity landscape, as appropriate.

---

<sup>27</sup> As specified in ISO/SAE 21434 work product 5 clause 8 ([WP-08-05]) (vulnerability analysis) should be generated for each vulnerability identified during cybersecurity testing. The management of the vulnerability should meet requirement [RQ-08-07].

<sup>28</sup> Described in clause 13 of ISO/SAE 21434, “Operations and Maintenance”

<sup>29</sup> ISO/SAE 21434 clause section 8.3 “Cybersecurity Monitoring” describes monitoring activities and potential sources of information.

<sup>30</sup> For example, US-CERT at the Cybersecurity & Infrastructure Security Agency (CISA)

<sup>31</sup> For example, the vehicle development recommendations included in ISO/SAE 21434 and the “work products” summarized in annexes of ISO/SAE 21434.

#### 4.2.11 Industry best practices

[G.22] Best practices for secure software development should be followed, for example as outlined in NIST publications<sup>32 33</sup> and ISO/SAE 21434.<sup>34</sup>

Due to the dynamic and continuously evolving nature of cybersecurity, it is important for the members of the automotive industry to stay abreast of the available cybersecurity guidance, best practices, design principles, and standards based on or published by SAE International, ISO, Auto-ISAC, NHTSA, Cybersecurity Infrastructure Security Agency (CISA), NIST, industry associations, and other recognized standards-setting bodies, as appropriate. Further,

[G.23] Manufacturers should actively participate in automotive industry-specific best practices and standards development activities through recognized standards development organizations and the Auto-ISAC.

[G.24] As future risks emerge; industry should collaborate to expediently develop mitigation measures and best practices to address new risks.

### 4.3 Information Sharing

In late 2014, in alignment with Executive Order 13691, “Promoting Private Sector Cybersecurity Information Sharing,” (EO 13691),<sup>35</sup> NHTSA began encouraging the industry<sup>36</sup> to create the Auto-ISAC.<sup>37</sup> The automotive industry established the Auto-ISAC in late 2015 and it became fully operational on January 19, 2016. The Auto-ISAC is authorized by EO 13691 to facilitate industry’s cybersecurity-related information sharing among its members. Government entities, including NHTSA, are not members of the Auto-ISAC. NHTSA does not participate in or access the information sharing that takes place within Auto-ISAC.

As of early-2022, Auto-ISAC membership includes 64 organizations. NHTSA recommends:

[G.25] Members of the extended automotive industry (including, but not limited to, vehicle manufacturers, automotive equipment suppliers, software developers, communication

---

<sup>32</sup>Black P., Badger M., Guttman B., Fong E., NISTIR 8151 *Dramatically Reducing Software Vulnerabilities: Report to the White House Office of Science and Technology Policy*.

<sup>33</sup> Dodson D., Souppaya M., Scarfone K., *Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework*

<sup>34</sup> ISO/SAE 21434 clause 10 discusses software development practices.

<sup>35</sup> Executive Order 13691 *Promoting Private Sector Cybersecurity Information Sharing* encourages the development and formation of Information Sharing and Analysis Centers.

<sup>36</sup> NHTSA Report to Congress: “Electronic Systems Performance in Passenger Motor Vehicles” December 2015, available at: <https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/electronic-systems-performance-in-motor20vehicles.pdf>.

<sup>37</sup> McCarthy, C., Harnett K., Carter A., & Hatipoglu, C., *Assessment of the information sharing and analysis center model* 2014, available at: <https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/812076-assessinfosharingmodel.pdf>.

services providers, aftermarket system suppliers, and fleet managers) are strongly encouraged to:

[a] Join the Auto-ISAC;

[b] Share timely information concerning cybersecurity issues, including vulnerabilities, and intelligence information with the Auto-ISAC.

[G.26] Members of the Auto-ISAC are strongly encouraged to collaborate in expeditiously exploring containment options and countermeasures to reported vulnerabilities, regardless of an impact on their own systems.

#### 4.4 Security Vulnerability Reporting Program

It is important for the members of the automotive industry to make information reporting to them easy by the security researcher community and the general public. A vulnerability reporting program can assist in identifying cybersecurity vulnerabilities. These programs have been effective in other sectors and would benefit the motor vehicle industry.

[G.27] Automotive industry members should create their own vulnerability reporting policies and mechanisms.<sup>38 39</sup>

Such policies would provide external cybersecurity researchers with guidance on how to confidentially report vulnerabilities to organizations that design and/or manufacture vehicle systems.

#### 4.5 Organizational Incident Response Process

It is not possible to anticipate all future attacks. Therefore, it is prudent to prepare the organization, its processes and staff to effectively handle incidents if—and when—they occur.

[G.28] Members of the automotive industry should develop a product cybersecurity incident response process.<sup>40</sup> This process should include:

---

<sup>38</sup> ISO/SAE 21434's [RQ-05-02] suggests the organization shall establish and maintain rules and processes regarding vulnerability disclosure. ISO/SAE 21434 also notes that the rules and processes regarding vulnerability disclosure can be specified in ISO 29147, *Information Technology Security Techniques Vulnerability Disclosure*.

<sup>39</sup> The Cybersecurity and Infrastructure Security Agency (CISA) has "Binding Operational Directive 20-01" that discusses vulnerability disclosure. Available at: <https://cyber.dhs.gov/bod/20-01/>

<sup>40</sup> Auto-ISAC's "Incident Response" best practice provides additional guidance, available at: <https://automotiveisac.com/best-practices/download-best-practice-guides/>

- [a] A documented incident response plan;<sup>41</sup>
  - [b] Clearly identified roles and responsibilities within the organization;<sup>42</sup>
  - [c] Clearly identified communication channels and contacts outside the organization;<sup>43</sup> and
  - [d] Procedures for keeping this information, [G.28[a]-[c]], up to date.
- [G.29] Organizations should develop metrics to periodically assess the effectiveness of their response process.
- [G.30] Organizations should document the details of each identified and reported vulnerability, exploit, or incident applicable to their products.<sup>44</sup>
- [G.31] The nature of the vulnerability and the rationale for how the vulnerability is managed should be documented.
- [G.32] Commensurate to assessed risks, organizations should have a plan for addressing newly identified vulnerabilities on consumer-owned vehicles in the field, inventories of vehicles built but not yet distributed to dealers, vehicles delivered to dealerships but not yet sold to consumers, as well as future products and vehicles.

Even when a new vulnerability may not be considered safety-critical and may not warrant an immediate fix on its own, it is good practice to apply known remedies to identified vulnerabilities during new software release cycles.

Additionally, the response process should include reporting all incidents, exploits, and vulnerabilities to the Auto-ISAC<sup>45</sup> as soon as possible. This is also recommended for companies who may not yet be a member of Auto-ISAC. *[Restated G.23[b]]*

- [G.33] Any incidents should also be reported to CISA/United States Computer Emergency Readiness Team (US-CERT) in accordance with the US-CERT Federal Incident Notification Guidelines.<sup>46</sup>

---

<sup>41</sup> While “incident response plan” is not specifically one of ISO/SAE 21434’s work products, the more general [WP-05-01] “Cybersecurity Rules and Processes” should include appropriate organizational information, while specific incidents might be described in [WP-08-04] “Cybersecurity Event Evaluation.””

<sup>42</sup> ISO/SAE 21434’s [RQ-05-03] requires that “The organization shall assign and communicate the responsibilities to achieve and maintain cybersecurity.”

<sup>43</sup> ISO/SAE 21434 section 8.3 “Cybersecurity Monitoring” and [RQ-08-01] discuss potential external sources of information.

<sup>44</sup> Described in clause 8 of ISO/SAE 21434.

<sup>45</sup> Information can be directed to the Auto-ISAC via [analyst@automotiveisac.com](mailto:analyst@automotiveisac.com).

<sup>46</sup> US-CERT Federal Incident Notification Guidelines, available at: <https://us-cert.gov/incident-notification-guidelines>.

[G.34] Industry members should periodically conduct and participate in organized,<sup>47</sup> cyber incident response exercises.

Participation in organized exercises tests the effectiveness of an organizations' disclosure policy operations and incident response processes. Further, it facilitates appropriate revisions based on lessons learned.

## 4.6 Self-Auditing

Documentation and document control are vital for establishing a clear and controlled process for managing software and related vulnerability risks.

### 4.6.1 Process management documentation

[G.35] The automotive industry should document the details related to their vehicle cybersecurity risk management process<sup>48</sup> to facilitate auditing and accountability.

[G.36] Further, such documents should be retained through the expected life span of the associated product.

[G.37] Documents should follow a robust version control protocol<sup>49 50</sup>, and should be revised regularly as new information, data, and research results become available.

### 4.6.2 Review and audit

[G.38] The automotive industry should establish procedures for internal review of its management and documentation of cybersecurity-related activities.

These activities will assist companies in better understanding their cybersecurity practices and determining where their processes could benefit from improvement.

[G.39] The automotive industry should consider carrying out organizational and product cybersecurity audits annually.<sup>51</sup>

---

<sup>47</sup> For example, DHS' bi-annual "CyberStorm" exercise. See <https://www.cisa.gov/cyber-storm-securing-cyber-space>.

<sup>48</sup> NHTSA strongly encourages developing the "work products" described in ISO/SAE 21434.

<sup>49</sup> ISO/SAE 21434's requirement [RQ-05-11] discusses a quality management system that encompasses change management and configuration management.

<sup>50</sup> ISO/SAE 21434 requirement [RQ-06-12] states: "The work products identified in the cybersecurity plan shall be subject to configuration management, change management, requirements management, and documentation management".

<sup>51</sup> ISO/SAE 21434 requires an organization cybersecurity audit in requirement 17 clause 5 ([RQ-05-17]). The automotive industry should consider carrying out an "organizational cybersecurity audit report" ([WP-05-03]).

A public version of audit reports would be informative to stakeholders and consumers and can assist in demonstrating the organization's commitment to product cybersecurity.

## 5. Education

Continually educating the existing workforce and educating the workforce of the future are crucial steps that will assist industry with improving the cybersecurity posture of motor vehicles. Cybersecurity educational activities should not be limited to the current workforce or technical individuals but should also enrich the future workforce and non-technical individuals. NHTSA encourages the automotive industry to work with universities to develop curriculums that further skillsets useful across a range of practical security applications, including the field of vehicle cybersecurity.

[G.40] Vehicle manufacturers, suppliers, universities, and other stakeholders should work together to help support educational efforts targeted at workforce development in the field of automotive cybersecurity.<sup>52</sup>

## 6. Aftermarket/User Owned Devices

User owned devices, designed and manufactured by third parties, could present unique cybersecurity challenges.

### 6.1 Vehicle manufacturers

The automotive industry should consider that consumers may bring aftermarket devices (e.g., insurance dongles) and personal equipment (e.g., mobile phones) into vehicles and connect them to vehicle systems through the interfaces manufacturers provide (cellular data, IEEE 802.11 wireless local area network (Wi-Fi), Bluetooth, USB, OBD-II port, etc.).

[G.41] The automotive industry should consider the risks that could be presented by user owned or aftermarket devices when connected with vehicle systems and provide reasonable protections.

[G.42] Any connection to a third-party device should be authenticated and provided with appropriate limited access.

### 6.2 Aftermarket device manufacturers

Aftermarket device manufacturers should consider that their devices connect with cyber-physical systems that may impact the safety-of-life. Even though the primary purpose of the system may not be safety-related (e.g., a telematics device collecting fleet operational data), depending on the vehicle system architecture, if not properly protected the device could be used as proxy to influence the behavior of

---

<sup>52</sup> For instance, the SAE CyberAuto Challenge <https://www.sae.org/attend/cyberauto>, the Cyber Truck Challenge <https://www.cybertruckchallenge.org/> as well as NHTSA's efforts to fund and develop cybersecurity curricula

safety-critical systems in vehicles. Aftermarket devices could be connected to a variety of vehicle types with varying levels of cybersecurity protections on the vehicle side of the interface. Therefore,

[G.43] Aftermarket device manufacturers should employ strong cybersecurity protections on their products.

## **7. Serviceability**

An average motor vehicle remains on the roads for over a decade and needs regular maintenance and occasional repair to operate safely while in service.

[G.44] The automotive industry should consider the serviceability of vehicle components and systems by individuals and third parties.

[G.45] The automotive industry should provide strong vehicle cybersecurity protections that do not unduly restrict access by alternative third-party repair services authorized by the vehicle owner.

NHTSA recognizes the balance between third party serviceability and cybersecurity is not necessarily easy to achieve. However, cybersecurity should not become a reason to justify limiting serviceability. Similarly, serviceability should not limit strong cybersecurity controls.

## **8. Technical Vehicle Cybersecurity Best Practices**

The following technical vehicle cybersecurity best practices present various fundamental protection techniques based on what NHTSA has learned through its internal applied research as well as from stakeholder experiences shared with NHTSA and the public. These recommendations do not form an exhaustive list of actions necessary for securing automotive computing systems, and all items may not be applicable in each case.

### **8.1 Developer/Debugging Access in Production Devices**

Software developers have considerable access to ECUs. Such ECU access might be facilitated by an open debugging port, through a serial console, or an open IP port on the vehicle's Wi-Fi network. However,

[T.1] Developer-level access should be limited or eliminated if there is no foreseeable operational reason for the continued access to an ECU for deployed units.

[T.2] If continued developer-level access is necessary, any developer-level debugging interfaces should be appropriately protected to limit access to authorized privileged users.

Merely physically hiding connectors, traces, or pins intended for developer debugging access should not be considered a sufficient form of protection.



## 8.2 Cryptographic Techniques and Credentials

The suitability of cryptographic techniques can change in response to a variety of factors. One significant factor is computing innovation. For this reason:

[T.3] Cryptographic techniques should be current and non-obsolescent for the intended application.<sup>53</sup>

While the selection of appropriate cryptographic techniques is an important design criterion, it should be noted that implementation issues often determine any system's security.

Cryptographic credentials help mediate access to vehicle computing resources and back-end servers. Examples include passwords, public key infrastructure (PKI) certificates, and encryption keys.

[T.4] Cryptographic credentials that provide an authorized, elevated level of access to vehicle computing platforms should be protected from unauthorized disclosure or modification.

[T.5] Any credential obtained from a single vehicle's computing platform should not provide access to other vehicles.<sup>54</sup>

## 8.3 Vehicle Diagnostic Functionality

Vehicle diagnostic features provide utilities to support repair and serviceability of vehicles; however, if not appropriately designed and protected, they could be leveraged to compromise vehicle systems.

[T.6] Diagnostic features should be limited, as much as possible, to a specific mode of vehicle operation which accomplishes the intended purpose of the associated feature.

[T.7] Diagnostic operations should be designed to eliminate or minimize potentially dangerous ramifications if they were misused or abused outside of their intended purposes.

For example, a diagnostic operation that may disable a vehicle's individual brakes<sup>55</sup> could be restricted to operate only at low speeds. In addition, this diagnostic operation could be prohibited from disabling all brakes at the same time, and/or the duration of such diagnostic control action could be time limited.

---

<sup>53</sup> NIST regularly updates the Federal Information Processing Standards (FIPS) 140 Series "Security Requirements for Cryptographic Modules" that provides guidance on appropriate cryptographic techniques.

<sup>54</sup> In <https://github.com/sgayou/subaru-starlink-research/blob/master/doc/README.md>, Scott Gayou describes his efforts to hack an infotainment system.

<sup>55</sup> Miller C., Valasek C., *Adventures in Automotive Networks and Control Units*, 2014, available at: [http://illmatics.com/car\\_hacking.pdf](http://illmatics.com/car_hacking.pdf).

- [T.8] The use of global symmetric keys and ad-hoc cryptographic techniques for diagnostic access should be minimized.<sup>56</sup>

Public key cryptography techniques are more secure than symmetric keys valid across multiple vehicles.<sup>57</sup>

## 8.4 Diagnostic Tools

In the past, researchers have reverse engineered diagnostic tools to obtain authentication keys and perform sensitive operations such as re-flashing firmware.<sup>58</sup>

- [T.9] Vehicle and diagnostic tool manufacturers should control tools' access to vehicle systems that can perform diagnostic operations and reprogramming by providing for appropriate authentication and access control.<sup>59</sup>

## 8.5 Vehicle Internal Communications

Critical safety messages are those that could directly<sup>60</sup> or indirectly<sup>61</sup> impact safety-critical vehicle control systems' operations.

- [T.10] When possible, critical safety signals should be transported in a manner inaccessible through external vehicle interfaces.

For example, providing an ECU's critical sensors with dedicated transport mechanisms would eliminate the risks associated with spoofing signals on common data busses such as CAN. A segmented communications bus may also mitigate the potential effects of interfacing insecure aftermarket devices to vehicle networks.

- [T.11] Employ best practices for communication of critical information over shared and possibly insecure channels. Limit the possibility of replay, integrity compromise, and spoofing. Physical and logical access should also be highly restricted.

---

<sup>56</sup> Hogan G., *Flashing ECU Firmware Updates from a Web Browser* Talk at DefCon 27: Car Hacking Village, Las Vegas. Video of the talk may be found at: <https://media.defcon.org/DEF%20CON%2027/DEF%20CON%2027%20villages/>. Mr. Hogan describes reverse engineering enciphered firmware updates.

<sup>57</sup> Miller C., Valasek C., *Adventures in Automotive Networks and Control Units*, 2014, available at: [http://illmatics.com/car\\_hacking.pdf](http://illmatics.com/car_hacking.pdf). The paper describes efforts to discover fixed, universal keys from diagnostic software and use them.

<sup>58</sup> Miller C., Valasek C., *Adventures in Automotive Networks and Control Units*, 2014, available at: [http://illmatics.com/car\\_hacking.pdf](http://illmatics.com/car_hacking.pdf).

<sup>59</sup> ISO/SAE 21434 requirement [RQ-05-14] states that "Tools that can impact the cybersecurity of an item, system or component shall be managed."

<sup>60</sup> For example, a control command message sent to a traction control actuator, if spoofed, could apply the vehicle's brakes without a driver's or a legitimate vehicular safety system's intent.

<sup>61</sup> For example, a vehicle speed estimate message, if spoofed, could cause the distributed vehicle controllers relying on that information to misunderstand the moving state of the vehicle (e.g., stationary versus moving).

## 8.6 Event Logs

In-vehicle networks and connected services produce data that can support detection of unauthorized attempts to access vehicle computing resources.

[T.12] A log of events sufficient to reveal the nature of a cybersecurity attack or successful breach and support event reconstruction should be created and maintained.

[T.13] Such logs that can be aggregated across vehicles should be periodically reviewed to assess potential trends of cyber-attacks.

## 8.7 Wireless Paths into Vehicles

Wireless interfaces into vehicle systems create new attack vectors that could potentially be remotely exploited. Unauthorized wireless access to vehicle computing resources could scale rapidly to multiple vehicles without appropriate controls.<sup>62</sup>

### 8.7.1 Wireless Interfaces

[T.14] Manufacturers should treat all networks and systems external to a vehicle's wireless interfaces as untrusted and use appropriate techniques to mitigate potential threats.

### 8.7.2 Segmentation and Isolation Techniques in Vehicle Architecture Design

[T.15] Network segmentation and isolation techniques should be used to limit connections between wireless-connected ECUs and low-level vehicle control systems, particularly those controlling safety critical functions, such as braking, steering, propulsion, and power management.

Privilege separation with boundary controls is important to improving the security of systems.<sup>63</sup> Logical and physical isolation techniques can be used to separate processors, vehicle networks, and external connections, as appropriate, to limit and control pathways from external threat vectors to cyber-physical features of vehicles.

---

<sup>62</sup> For example, vehicle systems could expose vulnerable services to other participants in a Wi-Fi network if they trust that Wi-Fi encryption systems are, by themselves, secure. (Blackhat 2020 – Lipovsky R. and Svorencik S. – Kr00k: Serious Vulnerability Affected Encryption of Billion+ Wi-Fi Devices. Paper available at <https://i.blackhat.com/USA-20/Thursday/us-20-Lipovsky-Kr00k-Serious-Vulnerability-Affected-Encryption-Of-Billion-Wi-Fi-Devices-wp.pdf>.)

<sup>63</sup> Some strategies are described in *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies*, Department of Homeland Security, September, 2016, available at [https://www.us-cert.gov/sites/default/files/recommended\\_practices/NCCIC\\_ICS-CERT\\_Defense\\_in\\_Depth\\_2016\\_S508C.pdf](https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf).

- [T.16] Gateways with strong boundary controls, such as strict whitelist-based filtering of message flows between different network segments, should be used to secure interfaces between networks.

### 8.7.3 Network Ports, Protocols, and Services

Any software listening on an internet protocol (IP) port opens an attack vector that may be exploited. Network services such as telnet,<sup>64</sup> dbus,<sup>65</sup> and the Android Debugger<sup>66</sup> have been discovered by port scan on the networks of production vehicles. Recommended practices to address potential vulnerabilities related to network ports include:

- [T.17] Eliminating unnecessary internet protocol services from production vehicles.
- [T.18] Limiting the use of network services on vehicle ECUs to essential functionality only; and,
- [T.19] Appropriately protecting services over such ports to limit use to authorized parties.

### 8.7.4 Communication to Back-End Servers

- [T.20] Manufacturers should use appropriate encryption and authentication methods in any operational communication between external servers and the vehicle.<sup>67</sup>

### 8.7.5 Capability to Alter Routing Rules<sup>68</sup>

- [T.21] Manufacturers should plan for and create processes that could allow for quickly propagating and applying changes in network routing rules to a single vehicle, subsets of vehicles, or all vehicles connected to the network.

## 8.8 Software Updates / Modifications

Automotive software architecture is distributed and complex, and the automotive industry has long included the ability to update automotive ECU firmware in their vehicles to address in field issues and

---

<sup>64</sup> Computest Report, *The Connected Car-- Ways to get unauthorized access and potential implications*, 2018, available at: <https://www.computest.nl/en/knowledge-platform/rd-projects/car-hack/>

<sup>65</sup> Miller C., Valasek C., *Remote Exploitation of an Unaltered Passenger Vehicle*, 2015, available at: <http://illmatics.com/Remote%20Car%20Hacking.pdf>.

<sup>66</sup> Android Debug Bridge description may be found here: <https://developer.android.com/studio/command-line/adb>

<sup>67</sup> Allgemeiner Deutscher Automobil-Club (ADAC), "Security Holes in BMW Connected Drive" 2015 (English title as reported by Google translate), available at: <https://www.adac.de/rund-ums-fahrzeug/ausstattung-technik-zubehoer/assistentensysteme/sicherheitsluecken-bmw-connected-drive/>.

<sup>68</sup> A demonstrated security vulnerability in 2015 allowed general access to affected vehicles over the Internet. A quick initial fix carried out by the wireless carrier blocked packets directed to the vulnerable port. (Miller C., Valasek C., *Remote Exploitation of an Unaltered Passenger Vehicle*, 2015, available at: <http://illmatics.com/Remote%20Car%20Hacking.pdf>.)

system upgrades. The risks associated with unauthorized use of these mechanisms needs to be considered and addressed.

[T.22] Automotive manufacturers should employ state-of-the-art techniques for limiting the ability to modify firmware to authorized and appropriately authenticated parties.

Limiting an attacker's ability to modify firmware makes it more challenging for malware to be installed on vehicles. The use of digital signing techniques may prevent an automotive ECU from booting modified/unauthorized and potentially damaging firmware images. In addition, firmware updating systems which employ signing techniques could prevent the installation of a damaging software update that did not originate from an authorized source.

An attacker may use software update mechanisms to place older, more vulnerable software on a targeted device. This practice is called a firmware version rollback or downgrade attack.<sup>69 70</sup>

[T.23] Manufacturers should employ measures to limit firmware version rollback attacks.

## 8.9 Over-the-Air Software Updates

Over-the-air (OTA) refers to a software update distribution method which uses wireless transmission. Manufacturers that design-in and offer OTA software update capability on their vehicles should:

[T.24] Maintain the integrity of OTA updates, update servers, the transmission mechanism, and the updating process in general.<sup>71,72</sup>

[T.25] Take into account, when designing security measures, the risks associated with compromised servers, insider threats, men-in-the-middle attacks, and protocol vulnerabilities.

---

<sup>69</sup> Chen Y. et al. "Downgrade Attack on TrustZone" available at:<https://arxiv.org/ftp/arxiv/papers/1707/1707.05082.pdf>... CVE-2015-6639

<sup>70</sup> "OnePlus OTA Downgrade Vulnerability" Aleph Research Advisory available at: <https://alephsecurity.com/vulns/aleph-2017008>

<sup>71</sup> Bar R., *Hacking into Automotive Clouds*, talk at DefCon 27 Car Hacking Village, Las Vegas, 2019. Video of the talk: <https://media.defcon.org/DEF%20CON%2027/DEF%20CON%2027%20villages/>.

<sup>72</sup> Rodgers M., Hahaffey K. *How to Hack a Tesla Model S*, talk at DefCon 23, Las Vegas, 2015. Video of the talk: <https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20video/>.

## Appendix

### Terms and Descriptions

**Application Programming Interface (API)** is an interface that defines interactions between two software entities. Usually, the goal of an API is to provide an abstraction layer that hides complexity while providing specified functionality.

**Attack** is an intentional action designed to cause harm.

**Attack Surface** is the set of interfaces (the “attack vectors”) where an unauthorized user can try to inject or extract data from a system or modify a system’s behavior.

**Attack Vector** refers to the interfaces or paths an attacker uses to exploit a vulnerability. For instance, an exploit may use an open IP port vulnerability on a variety of different attack vectors such as Wi-Fi, cellular networks, IP over Bluetooth, etc. Attack vectors enable attackers to exploit system vulnerabilities, including the human element.

**Authentication** is the process of verifying identity, especially a user, code creator or source of data.

**Automotive** refers to “of, relating to, or concerned with motor vehicles in general.”

**Back-end Server** are network-based computing resources that provide a variety of services to mobile devices such as cars and phones.

**Binary image** or **firmware image** refers to the sequence of bytes that comprises the software, both code and data, running on vehicle electronics.

**Controller Area Network (CAN)** is a dominant serial communication network protocol used for intra-vehicle communication.

**Credential** is some subset of cryptographic keys, username or password used to authenticate.

**Cybersecurity** is the measures taken to protect a computer or computer system against an attack.

**Debug** is the activity of discovering errors in software and hardware that leads to unspecified system functionality including erroneous behavior.

**Digital signing** is a mathematical technique that ensures message authenticity, integrity, and non-repudiation. Signature validation proves to the recipient the sender’s identity, the message has not been modified during transmission, and only the signing key holder could have generated the signature (given the key has not been compromised).

**Electronic Architecture** is the general framework that provides power and communications for devices within a vehicle.

**Electronic Control Unit (ECU)** is an embedded system that provides a control function to a vehicle's electrical system or subsystems through digital computing hardware and associated software.

**Encryption** is an operation that converts information to a form that is readable only to an authorized party.

**Exploit** refers to an action that takes advantage of a vulnerability in order to cause unintended or unanticipated behavior to occur on computer software and/or hardware. An example of an exploit would be using a buffer overflow to execute privileged code on a target.

**Firmware** refers to compiled code and data running in an environment dominated by electrical, physical interfaces.

**Global Symmetric Keys** are symmetric cryptographic keys that are applied to multiple, or an entire population of devices.

**Incident** is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system on a vehicle computing platform using an exploit.

**Layered Protections** are internal cybersecurity protections that assume the compromise of other vehicle computing resources.

**Over-The-Air (OTA)** is a software update distribution method which uses wireless transmission.

**Privilege Separation** is a technique in which computing resources are divided into parts which are limited to the specific privileges they require in order to perform a specific task.

**Public Key Infrastructure (PKI)** refers to a set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

**Recovery** is the timely restoration of systems or assets affected by cybersecurity incidents.

**Safety-Critical Vehicle Control Systems** are vehicle systems which can apply control inputs to steering, throttle or brake.

**Software** refers to the instructions and data that reside on an embedded system, such as an automotive electronic control system, that implements dedicated functions and manage system resources (e.g., system input/outputs (I/O) to execute those functions). Software may take a variety of different forms. For example, in some cases "software" may refer to source code while in some cases it may take the form of a binary image consisting of a file system and compiled binary.

**Spoofing** refers to using a communications channel with the intent of misrepresenting the source of a message.

**Service Set Identifier (SSID)** is a string that functions as the name of a Wi-Fi network.



**Telematics** refers to the integration of telecommunications and informatics for intelligent applications in vehicles, such as fleet management.

**Transport Layer Security** (TLS) is a common set of cryptographic protocols used to secure communications over IP networks. TLS secures communications between web clients and servers.

**Vulnerability** is a weakness in a system or its associated networks, system security procedures, internal controls, or implementation that could be exploited to obtain unauthorized access to system resources. For instance, an open diagnostic port on an ECU is a vulnerability.

**Whitelist-based Filtering** is a policy that uses a list of allowed messages to pass valid messages while not passing invalid messages.

**Wi-Fi** is a common name for a wireless local area network (WLAN) defined by IEEE 802.11.

