CYBENTIA® GRUPO
CONSULTORA DE INVESTIGACIÓN, CONCIENCIACIÓN Y COMUNICACIÓN ESTRATÉGICA

CURSO NORMATIVA DE CIBERSEGURIDAD EN VEHÍCULOS UNECE/R155

EN COLABORACIÓN CON EL EQUIPO TÉCNICO DE

EUROCYBCAR®
CYBERSECURITY TEST

DOCUMENTACIÓN ALUMNO

Fecha actualización
Abril de 2024

CYBENTIA® GRUPO
CONSULTORA DE INVESTIGACIÓN, CONCIENCIACIÓN Y COMUNICACIÓN ESTRATÉGICA

Sede Central: Vitoria-Gasteiz, Parque
Tecnológico, C/ Hermanos Lumiére 11 CP
01510, Vitoria-Gasteiz, Álava.
Sede Madrid: Parque Científico C/Faraday, 7
-CP 28049, Madrid

T. +34 682 31 89 06
M. formacion@cybentia.com
www.cybentia.com

ÍNDICE DOCUMENTOS

EUROCYBCAR®
CYBERSECURITY TEST

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

Nota: Este informe está basado en la normativa aprobada el 23 de junio de 2020 por la ONU: ECE/TRANS/WP29/2020/79

Diseño y edición: Grupo CYBENTIA

POR QUÉ ERA NECESARIO CREAR UN REGLAMENTO DE CIBERSEGURIDAD PARA VEHÍCULOS

EN VIGOR DESDE EL 22 DE ENERODE 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.

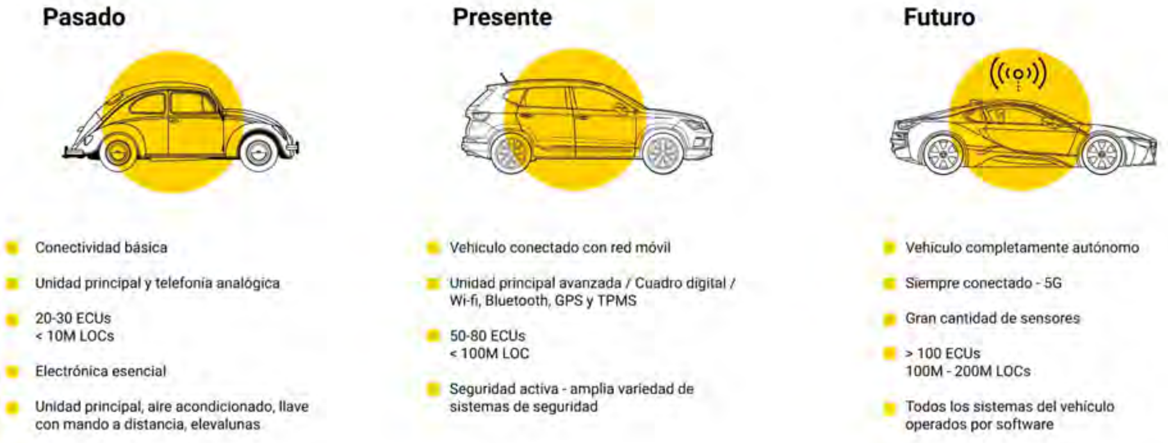
Según EUROCYBCAR, desde 2012 se han documentado más de 550 ciberataques que afectan a modelos de 60 marcas diferentes

• 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.



Pasado

- Conectividad básica
- Unidad principal y telefonía analógica
- 20-30 ECUs
  < 10M LOCs
- Electrónica esencial
- Unidad principal, aire acondicionado, llave con mando a distancia, elevalunas

Presente

- Vehículo conectado con red móvil
- Unidad principal avanzada / Cuadro digital / Wi-fi, Bluetooth, GPS y TPMS
- 50-80 ECUs
  < 100M LOC
- Seguridad activa - amplia variedad de sistemas de seguridad

Futuro

- Vehículo completamente autónomo
- Siempre conectado - 5G
- Gran cantidad de sensores
- > 100 ECUs
  100M - 200M LOCs
- Todos los sistemas del vehículo operados por software

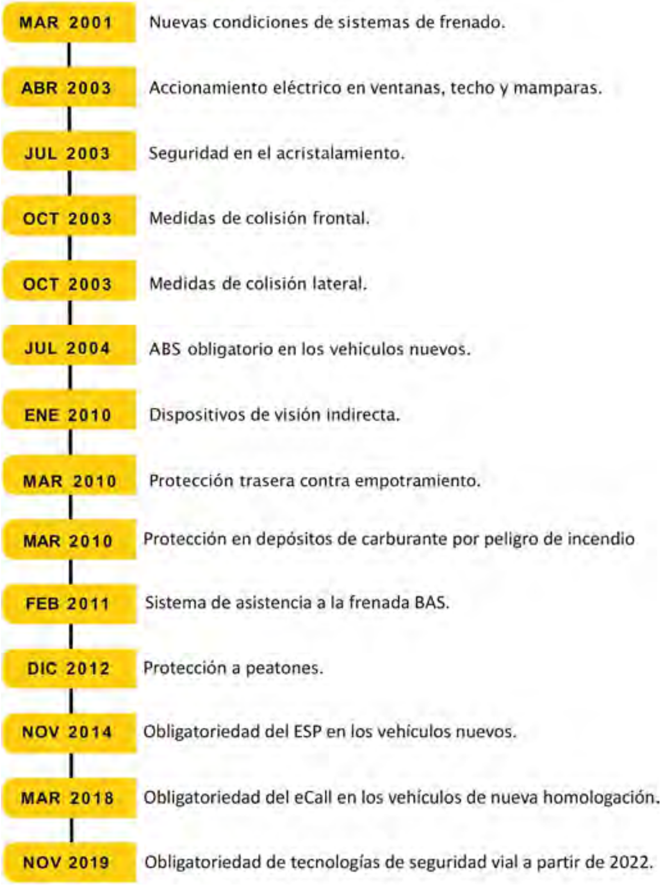
LOC: Lines of Code (Líneas de código) **100M:** Millones **ECU:** Electronic Control Unit (Unidad de control electrónica)

https://www.informationisbeautiful.net/visualizations/million-lines-of-code/
https://site.ieee.org/connected-vehicles/ieee-connected-vechicles/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 obli- gatorios en el equipamiento de los coches los siguientes sistemas de seguridad:

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



MAR 2001	Nuevas condiciones de sistemas de frenado.
ABR 2003	Accionamiento eléctrico en ventanas, techo y mamparas.
JUL 2003	Seguridad en el acristalamiento.
OCT 2003	Medidas de colisión frontal.
OCT 2003	Medidas de colisión lateral.
JUL 2004	ABS obligatorio en los vehiculos nuevos.
ENE 2010	Dispositivos de visión indirecta.
MAR 2010	Protección trasera contra empotramiento.
MAR 2010	Protección en depósitos de carburante por peligro de incendio
FEB 2011	Sistema de asistencia a la frenada BAS.
DIC 2012	Protección a peatones.
NOV 2014	Obligatoriedad del ESP en los vehículos nuevos.
MAR 2018	Obligatoriedad del eCall en los vehículos de nueva homologación.
NOV 2019	Obligatoriedad de tecnologías de seguridad vial a partir de 2022.

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

Fuentes (del gráfico): Noticias coches. http://www.noticias.coches.com - Dirección General de Tráfico. Disponible en: http://revista.dgt.es/es/reportajes/2018/04ABRIL/0404ecall-obligatorio-a-partir-del-31-de-marzo.shtml#.X4ATvmgzbIU

LAS NORMATIVAS QUE LA UNIÓN EUROPEA TOMA DE NACIONES UNIDAS

Y la úlima 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.

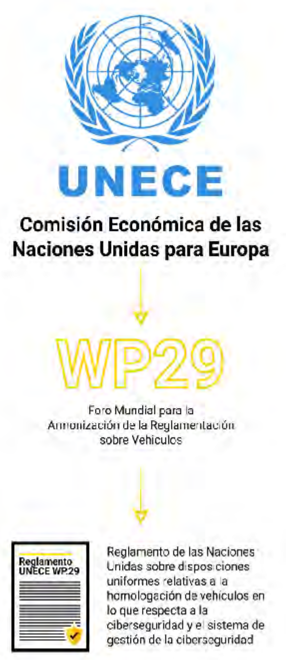
Dentro de UNECE existe el citado Foro Mundial para la Armonización de las Regulaciones de Vehículos -WP29-.

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- .


UNECE
Comisión Económica de las Naciones Unidas para Europa
WP29
Foro Mundial para la Armonización de la Reglamentación sobre Vehículos
Reglamento UNECE WP29
Reglamento de las Naciones Unidas sobre disposiciones uniformes relativas a la homologación de vehículos en lo que respecta a la ciberseguridad y el sistema de gestión de la ciberseguridad

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 ci- berseguridad 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/
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
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
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

2013

OCTUBRE

“Una revista española publica un reportaje sobre los riesgos de ciberseguridad en los coches”

“Un hacker podría matarte mientras conduces”. Así titula la revista Autofácil –creada y dirigida por Azucena Hernández– el reportaje publicado en el número 156, en el que alerta sobre los riesgos de ciberseguridad que afectan a los sistemas electrónicos de los vehículos. Afirma que algunas vulnerabilidades podrían poner en peligro la vida de los pasajeros si un ciberdelincuente se aprovecha de ellas.

2016

ENERO

“Guía de ciberseguridad para sistemas de vehículos ciberfísicos J3061_201601”[9]

Elaborada por la SAE. En ella se dan unas recomendaciones prácticas que proporcionan orientación sobre cómo establecer un alto nivel de ciberseguridad en los sistemas de los vehículos. Este texto se convertirá en el estándar ISO/SAE 21434, que aún está en fase de desarrollo y cuya última versión es un borrador no aprobado que aún está sujeto a cambios.

MARZO

“Los vehículos motorizados, cada vez más vulnerables a los ciberataques”[10]

El FBI emite un comunicado en el que avisa de que la creciente conectividad de los vehículos conlleva amenazas a la ciberseguridad. El texto pone algunos ejemplos de ciberataques que se podrían llevar a cabo sobre automóviles.

OCTUBRE

“Las mejores prácticas de ciberseguridad para vehículos modernos”

Elaborada por la NHTSA. Es una guía no vinculante para mejorar la ciberseguridad de los vehículos a motor.

2017

ENERO

“Ciberseguridad y resiliencia de automóviles inteligentes”

Elaborado por ENISA. El objetivo de este estudio es identificar buenas prácticas que garanticen la seguridad de los coches inteligentes frente a las ciberamenazas. El estudio enumera los activos sensibles presentes en los automóviles inteligentes, así como las correspondientes amenazas, riesgos, factores de mitigación y posibles medidas de seguridad a implementar.

JULIO

“El equipo fundador de EUROCYBCAR realiza el primer test de ciberseguridad a un vehículo”

Durante tres meses un equipo compuesto por hackers, ingenieros y probadores de coches realizaron las primera prueba de ciberseguridad a un vehículo fabricado en España para comprobar el nivel de ciberseguridad que ofrece un vehículo. El resultado reveló que la ciberseguridad era el gran olvidado de las marcas de coches, a pesar de que afecta a la vida de las personas.

AGOSTO

“Los principios clave de la ciberseguridad del vehículo para vehículos conectados y automatizados”

Elaborada por el Gobierno Británico. Es una guía que resume los 8 principios para la obtención de una buena ciberseguridad en el sector de la automoción.

2018

JULIO

“El Centro Vasco de Ciberseguridad crea el primer grupo de trabajo sobre ciberseguridad y automoción”

Tras la inauguración del Centro Vasco de Ciberseguridad –BCSC–, que dirige Javier Diéguez, se promueve la creación de un grupo de trabajo compuesto por los Centros de Investigación Tecnalia, Vicomtech e Ikerland, el BCSC y los fundadores de EUROCYBCAR.

2018

“En el evento internacional 12ENISE se descubre la importancia de la ciberseguridad para la movilidad”

Durante el 12ENISE -Encuentro Internacional de Seguridad de la Información que organiza el Instituto de Ciberseguridad de España (INCIBE)-, por primera vez, se habla de las amenazas y vulnerabilidades de ciberseguridad que deben considerarse en el automóvil. La ponencia la imparte Azucena Hernández, actual CEO de EUROCYBCAR.

DICIEMBRE

“PAS 1885:2018” [14]

Elaborada por el Grupo BSI (que está designado por el Gobierno del Reino Unido como el organismo nacional de normalización): Establece principios fundamentales sobre cómo proporcionar y mantener ciberseguridad en relación con la reducción de amenazas y daños a productos, servicios y sistemas dentro de ecosistemas de transporte inteligente cada vez más conectados y colaborativos.

2019

MARZO

“Nace el primer medio de investigación y concienciación de motor y ciberseguridad del mundo”

El medio de comunicación HackerCar, dirigido por Javier García, consigue que periodistas, probadores de coches y hackers trabajen en equipo para testar los coches de una forma nunca vista.

JULIO

“EUROCYBCAR realiza la segunda evaluación técnica de ciberseguridad a un vehículo”

En su laboratorio de Vitoria-Gasteiz, EUROCYBCAR somete a un vehículo fabricado en España al Test EUROCYBCAR: el único test en el mundo que mide el nivel de ciberseguridad de un coche basándose en dos parámetros: de qué forma protege la vida y la privacidad de las personas que viajan a bordo.

2019

NOVIEMBRE

“La ciberseguridad aplicada a la automoción”

El Real Instituto de Elcano publica un artículo de investigación, firmado por Ana Ayerbe -Tecnalia-, en el que se analizan los riesgos de ciberseguridad en los automóviles, las formas de enfrentarse a ellos y qué iniciativas existen en el mundo, citando a EUROCYBCAR, como la única empresa en España que mide la ciberseguridad de los vehículos.

DICIEMBRE

“Por primera vez en el mundo, una institución somete a un vehículo de su flota a un test de ciberseguridad”

El Gobierno Vasco somete a uno de los vehículos de su Parque Móvil al Test EUROCYBCAR para conocer las cibervulnerabilidades a las que se exponen las autoridades que viajan a bordo de dichos vehículos.

2020

Reglamento ECE/TRANS/WP29 /2020/79

Normativa desarrollada por la UNECE WP29 que exigirá que los vehículos cuenten con un certificado de ciberseguridad que acredite que están protegidos frente a ciberataques para poder homologarse.

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://hackercar.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

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 cíberseguridad”.

FASES DE DESARROLLO DE LA NORMA

2018

Septiembre

Comienza la discusión sobre los riesgos de la ciberseguridad que presentan los vehículos.

2019

Junio-agosto

Fases de pruebas con autoridades y fabricantes voluntarios para comprobar la solidez y preparar el borrador.

Septiembre

Decisión de GRVA (Grupo de trabajo sobre vehículos automatizados / autónomos y conectados) sobre el contenido de regulación.

2020

Marzo

Publicación del borrador final.

23 de junio

Aprobación del reglamento final.

2021

Enero 2021

Entrada en vigor. El reglamento estará disponible para su aplicación en los Estados miembros de UNECE. La Unión Europea, Corea del Sur y Japón ya han confirmado que lo aplicarán en sus territorios, como se detallará más adelante.

2022

Julio

La normativa comienza a ser de obligatoria aplicación en todos los modelos de nueva homologación.

2024

Febrero

La ONU amplía el ámbito de aplicación de la normativa también a motocicletas, scooter y bicicletas eléctricas de más de 25 km/h.

Julio

La normativa comienza a ser de obligatoria aplicación en todos los modelos nuevos que estén a la venta o se fabriquen para regiones como la UE

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 protege 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

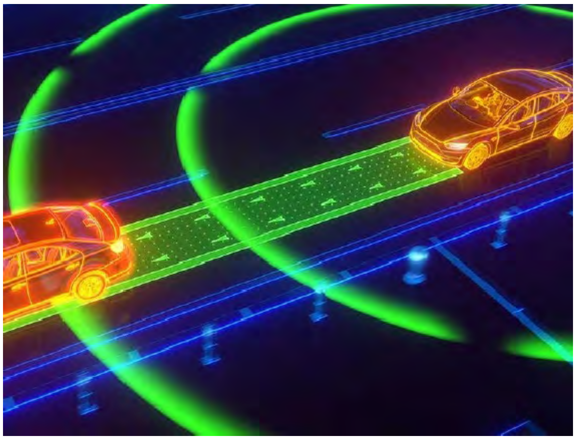
EL CSMS DEBE PROTEGER A LOS VEHÍCULOS CONTRA 70 AMENAZAS DE CIBERSEGURIDAD ESPECÍFICAS, SEGÚN LA NORMATIVA UNECE/R155

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 proporcionan. 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

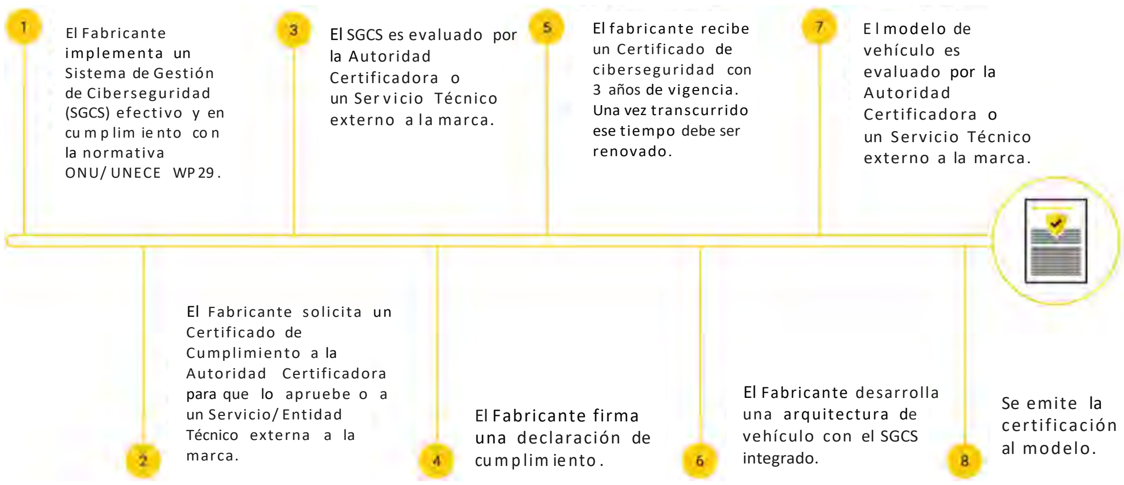
Para que un modelo de vehículo obtenga el certificado de ciberseguridad que acredite que cumple con los requisitos establecidos por la ONU, los fabricantes deberán someterlo a unas evaluaciones. Hasta ahora, los OEMs contrataban a empresas de consultoras de ciberseguridad para auditar de forma puntual 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



1 El Fabricante implementa un Sistema de Gestión de Ciberseguridad (SGCS) efectivo y en cumplimiento con la normativa ONU/ UNECE WP29.

2 El Fabricante solicita un Certificado de Cumplimiento a la Autoridad Certificadora para que lo apruebe o a un Servicio/ Entidad Técnico externa a la marca.

3 El SGCS es evaluado por la Autoridad Certificadora o un Servicio Técnico externo a la marca.

4 El Fabricante firma una declaración de cumplimiento.

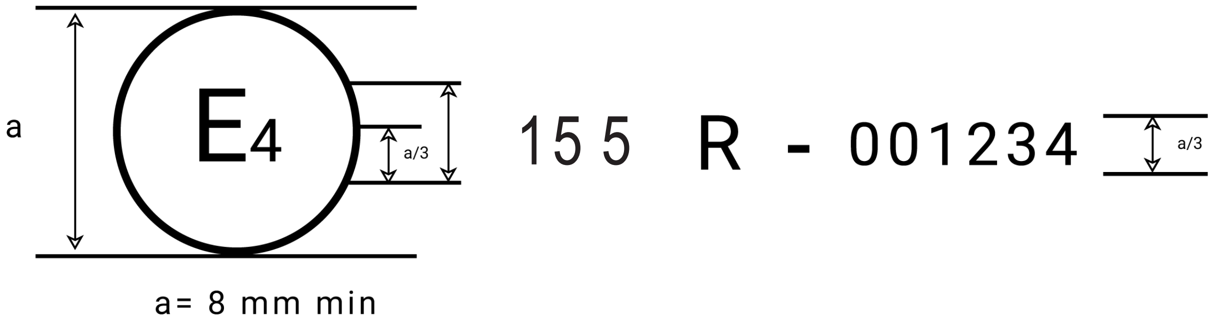
5 El fabricante recibe un Certificado de ciberseguridad con 3 años de vigencia. Una vez transcurrido ese tiempo debe ser renovado.

6 El Fabricante desarrolla una arquitectura de vehículo con el SGCS integrado.

7 El modelo de vehículo es evaluado por la Autoridad Certificadora o un Servicio Técnico externo a la marca.

8 Se emite la certificación al modelo.

En inglés: 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. Disponible en https://www.unece.org/fileadmin/DAM/trans/main/wp29/wp29regs/2017/E-ECE-TRANS-505-Rev.3e.pdf



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.

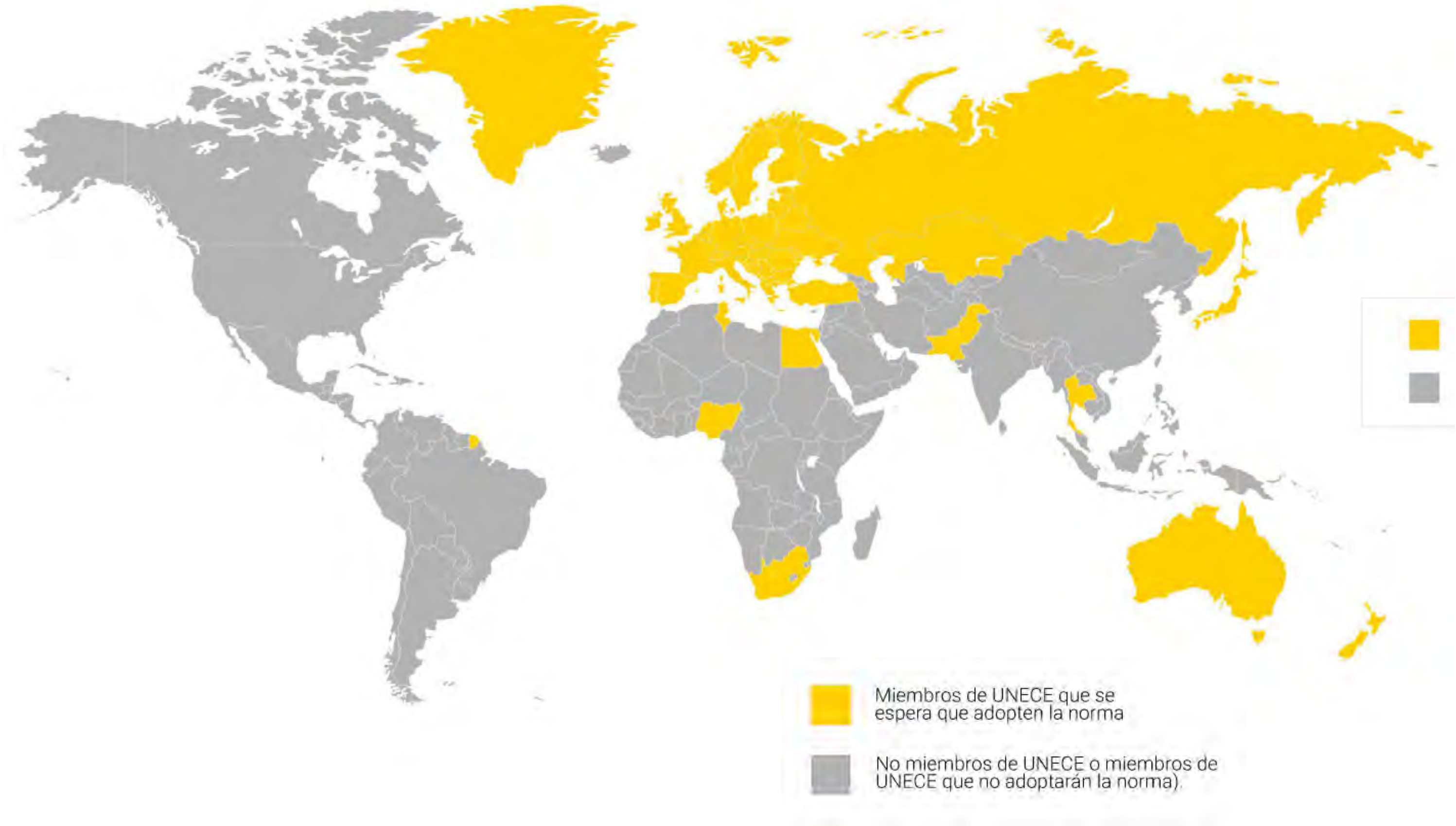
SERÁ OBLIGATORIO. Además, el fabricante también deberá informar a la Entidad Autorizada de **cualquier cambio que afecte a la relevancia del certificado** de cumplimiento del CSMS, como la aparición de nuevos ciberataques. Tras consultar con el fabricante, la Entidad Autorizada decidirá si es necesario 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 mediante 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 se espera que adopten la norma
No miembros de UNECE o miembros de UNECE que no adoptarán la norma).

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
-Armenia
-Australia
-Austria
-Azerbayán
-Bielorrusia
-Bélgica
-Bosnia Herzegovina
-Bulgaria

-Croacia
-Rep. Checa
-Dinamarca
-Egipto
-Estonia
-Finlandia
-Francia
-Georgia
-Alemania
-Grecia

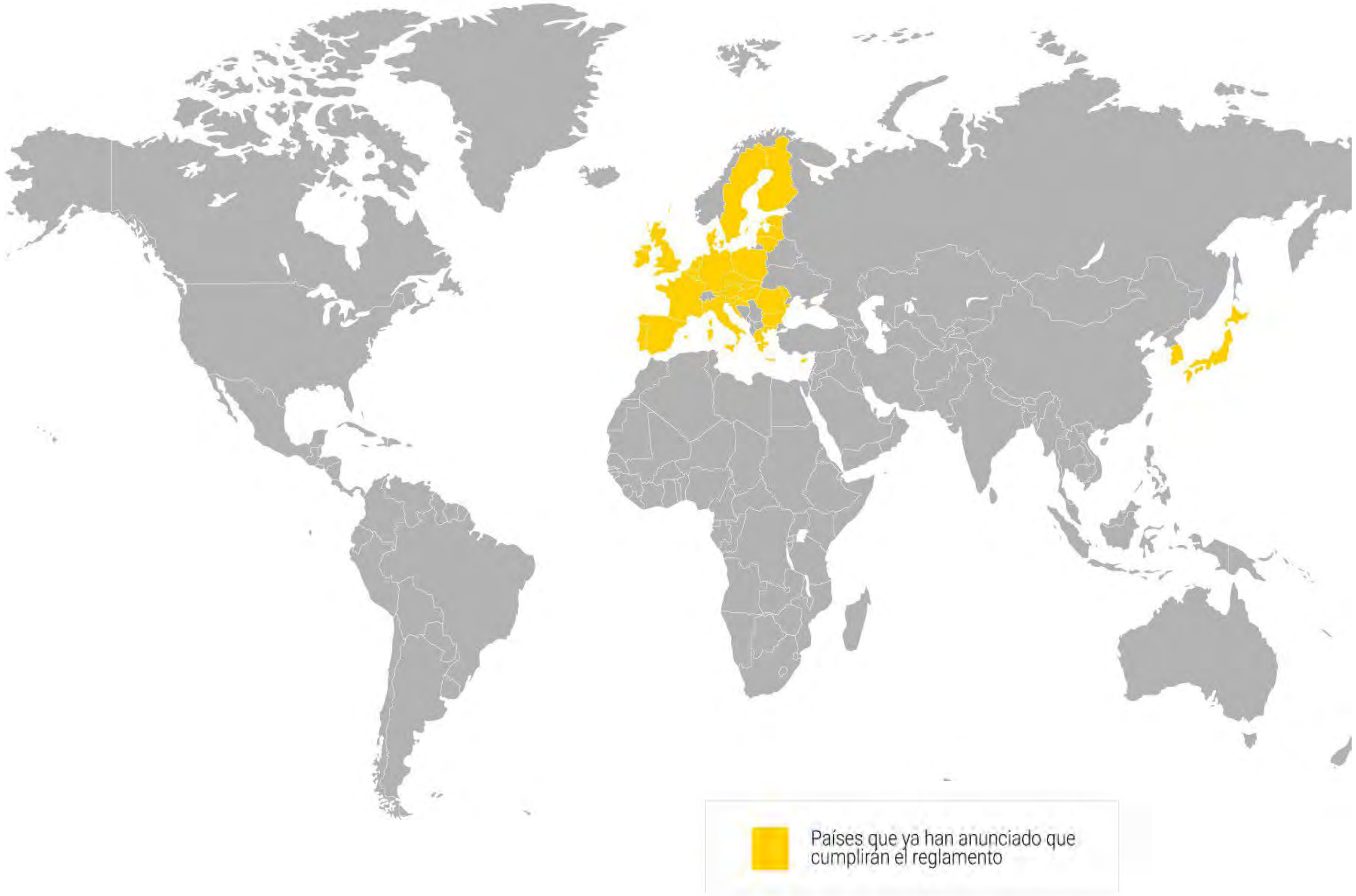
-Hungría
-Italia
-Japón
-Kazajistán
-Letonia
-Lituania
-Luxemburgo
-Malasia
-Montenegro
-Países Bajos

-Nueva Zelanda
-Nigeria
-Macedonia
-Noruega
-Pakistán
-Polonia
-Portugal
-Corea del Sur
-República de Moldova

-Rumanía
-Federación Rusa
-San Marino
-Serbia
-Eslovaquia,
-Eslovenia
-Sudáfrica
-España
-Suecia

-Suiza
-Tailandia
-Túnez
-Turquía
-Ucrania
-Reino Unido
-Irlanda del Norte

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
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
Suecia

Asia Pacífico

Japón
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 reglamen-to 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.

https://www.unece.org/trans/maps/un-transport-agreements-and-conventions-18.html

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 lanormativa UNECE/R155.

Categorías de vehículos afectados por la UNECE

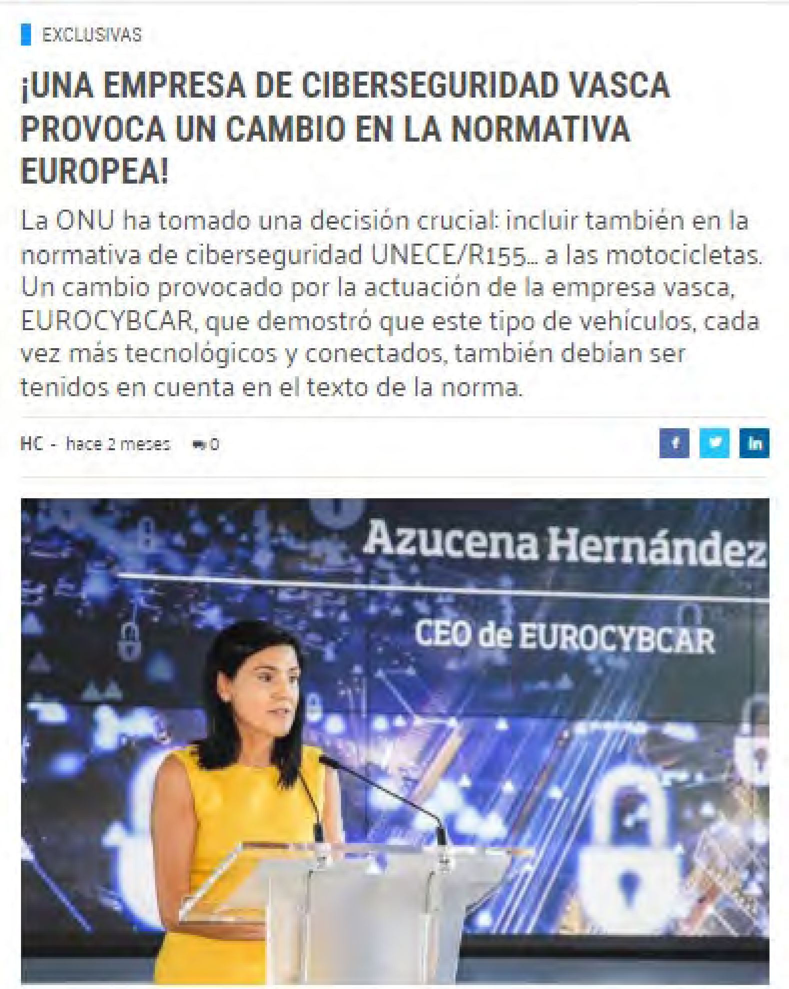
Categoría M:
Coches y autobuses.

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.

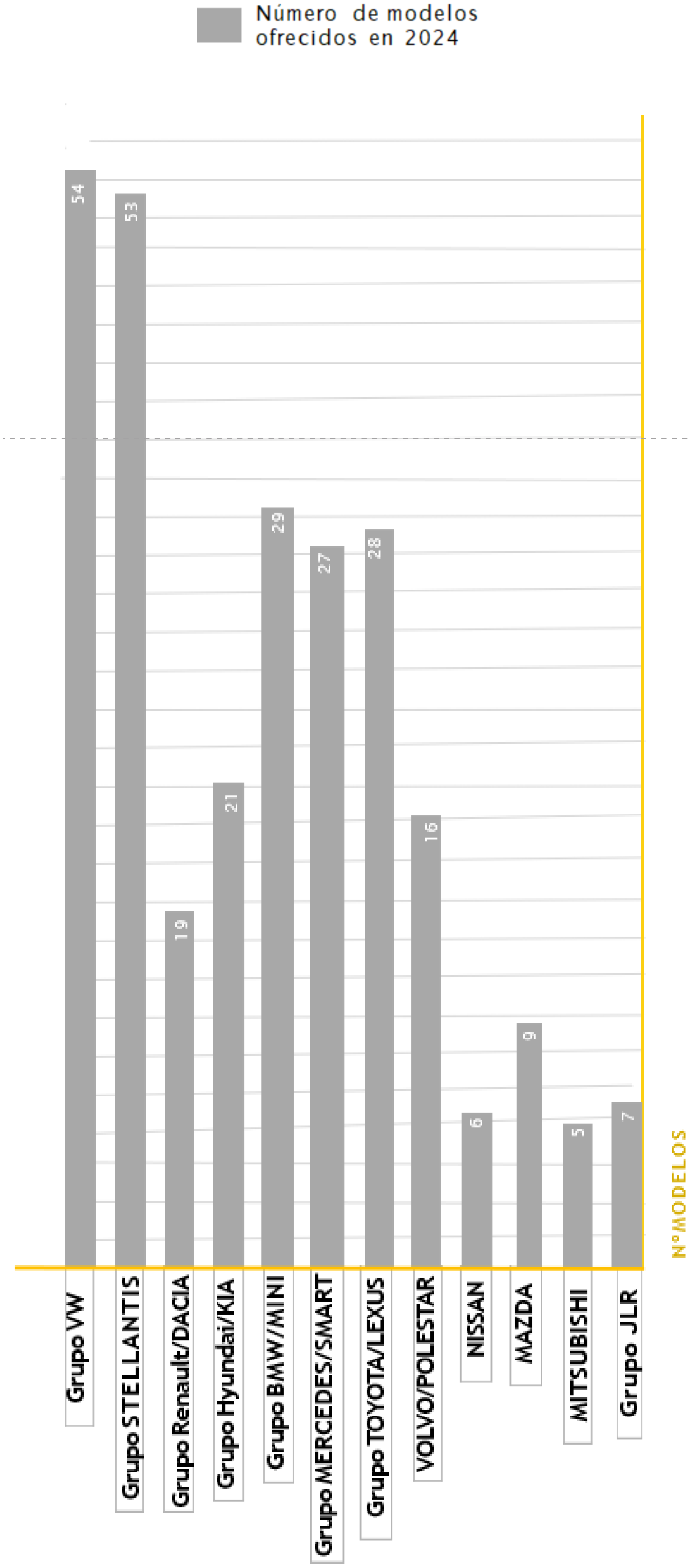
HC - hace 2 meses 0

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.



¿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 conlos requisitos de ciberseguridad que exige la nuevanormativa, sometiendo sus vehículos al Test EUROCYBCAR.

Modelos Fabricados en España 2023

	Fábricas Coches / Furgonetas
SEAT/CUPRA GRUPO PSA	Barcelona: 5 modelos
STELLANTIS	Vigo: 9 modelos Figueruelas, Zaragoza: 4 modelos Villaverde, Madrid: 2 modelos
GRUPO VW	Landaben, Pamplona: 3 modelos
RENAULT	Palencia: 2 modelos 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

Esa 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 vehículo -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.

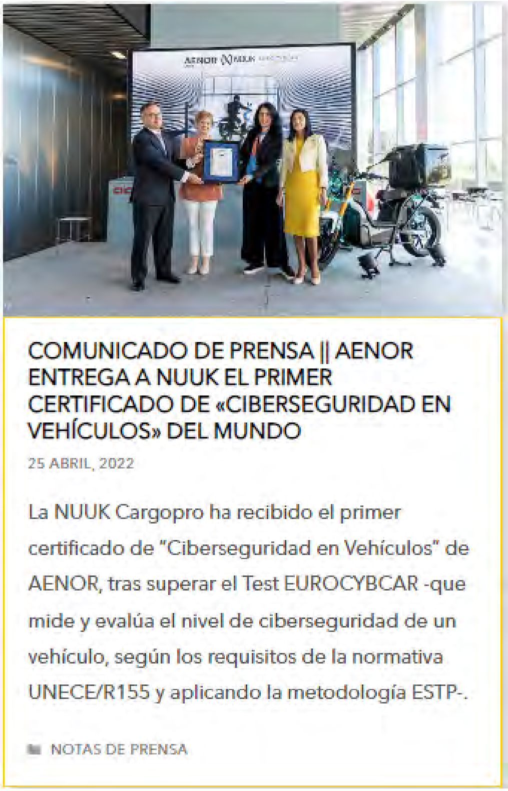
Una vez que el vehículo se ha sometido al protocolo de pruebas de EUROCYBCAR y lo ha superado -es APTO- se le concede un certificado de ciberseguridad, junto con AENOR, que avala el nivel de ciberseguridad que ha obtenido el vehículo.

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-.

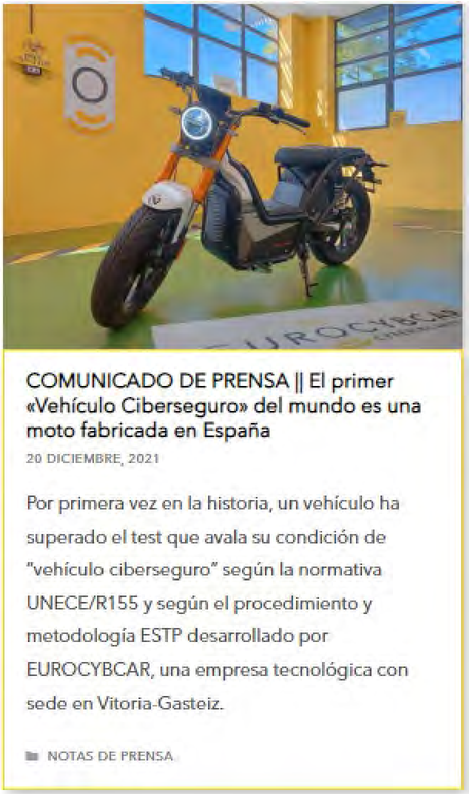


COMUNICADO DE PRENSA || AENOR ENTREGA A NUUK EL PRIMER CERTIFICADO DE «CIBERSEGURIDAD EN VEHÍCULOS» DEL MUNDO

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/

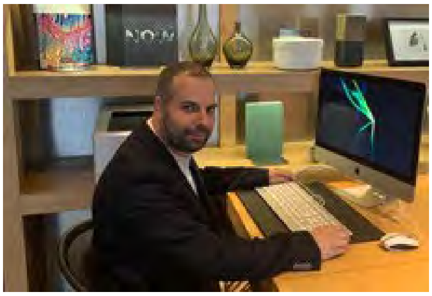
¿QUÉ OPINAN LOS EXPERTOS?

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 envigor 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 puedanser 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 YSEGURIDAD INDUSTRIAL (MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO). ADEMÁS, LIDERÓ EL GRUPO DE TRABAJO ESPAÑOL DE LA NORMATIVA UNECE/R155

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

¿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 procesode 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 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 metodolo gías 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 reconoci miento mutuo de las homologaciones concedidas entre las partesfirmantes, 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 ELMAYOR CAMBIO QUE HA DEBIDO REALIZAR UN FABRICANTE PARACUMPLIR 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.

EUROCYBCAR®
CYBERSECURITY TEST

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 portfolio 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 portfolio 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
PARQUE TECNOLÓGICO DE ÁLAVA EDIFICIO BIC
ALBERT EINSTEIN KALEA, 15 - 01510
VITORIA-GASTEIZ, ÁLAVA
+34 619 291 892
INFO@EUROCYBCAR.COM

CYBENTIA GRUPO

CONSULTORA
DE INVESTIGACIÓN,
CONCIENCIACIÓN
Y COMUNICACIÓN
ESTRATÉGICA

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

Annexes

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_6 and L_7 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;[1]

(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",[2] 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. [3]

[1] E.g. ISO 26262-2018, ISO/PAS 21448, ISO/SAE 21434

[2] https://www.unece.org/trans/main/wp29/datasharing.html

[3] 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[4] 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.[5] 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.[6]

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.

[4] The Working Party on Automated/Autonomous and Connected Vehicles (GRVA)

[5] This interpretation shall be reflected in the interpretation document referred to in the footnote to paragraph 5.3.3.

[6] 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: ....

....

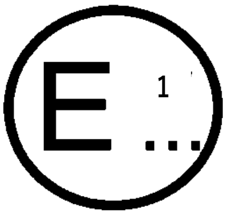
(*Stamp and signature of the manufacturer’s representative*)

Annex 2

Communication

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

issued by: Name of administration:
....
....
....



Concerning:[8] 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:

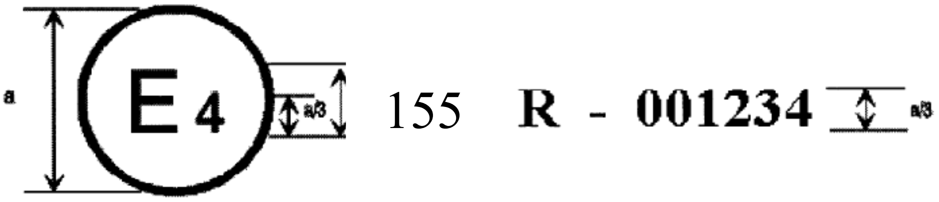
[7] Distinguishing number of the country which has granted/extended/refused/withdrawn approval (see approval provisions in the Regulation).

[8] Strike out what does not apply.

Annex 3

Arrangement of approval mark

Model A
(See paragraph 4.2 of this Regulation)



a = 8 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

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 (**insider attack**)
			1.2	**Unauthorized internet access** to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)
			1.3	**Unauthorized physical access** 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	**Attack on back-end server stops it functioning**, 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 (**insider attack)**
			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
			3.3	**Unauthorized internet access to the server** (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)
			3.4	**Unauthorized physical access to the server** (conducted for example by USB sticks or other media connecting to the server)
			3.5	**Information breach** 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	**Spoofing of messages** by impersonation (e.g. 802.11p V2X during platooning, GNSS messages, etc.)
			4.2	**Sybil attack** (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 **code injection**, for example tampered software binary might be injected into the communication stream
			5.2	Communications channels permit **manipulate** of vehicle held data/code
			5.3	Communications channels permit **overwrite** of vehicle held data/code
			5.4	Communications channels permit **erasure** 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 **unreliable or untrusted source**
			6.2	**Man in the middle** 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	**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	Information can be readily disclosed. For example, through eavesdropping on communications or through allowing unauthorized access to sensitive files or folders	7.1	**Interception of information** / interfering radiations / monitoring communications
			7.2	Gaining **unauthorized access** to files or data
	8	Denial of service attacks via communication channels to disrupt vehicle functions	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
			8.2	**Black hole attack**, 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 **gain privileged access**, for example root access
	10	Viruses embedded in communication media are able to infect vehicle systems	10.1	**Virus** 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 **internal** (e.g. CAN) **messages**
			11.2	Malicious **V2X messages,** e.g. infrastructure to vehicle or vehicle-vehicle messages (e.g. CAM, DENM)
			11.3	Malicious diagnostic messages
			11.4	Malicious **proprietary messages** (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 **over the air software update procedures**. This includes fabricating the system update program or firmware
			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**
	13	It is possible to deny legitimate updates	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
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 **tricked into taking an action** to unintentionally load malware or enable an attack
			15.2	**Defined security procedures** 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 **functions designed to remotely operate systems**, such as remote key, immobilizer, and charging pile
			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	Hosted 3rd party software, e.g. entertainment applications, used as a means to attack vehicle systems	17.1	**Corrupted applications**, 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	**External interfaces** such as USB or other ports used as a point of attack, for example through code injection
			18.2	Media infected with a **virus** connected to a vehicle system
			18.3	**Diagnostic access (e.g. dongles in OBD port)** 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 **piracy**)
			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.
			19.3	Extraction of cryptographic keys
	20	Manipulation of vehicle data/code	20.1	Illegal/unauthorized changes to **vehicle's electronic ID**
			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)
			20.4	Data manipulation to **falsify vehicle's driving data** (e.g. mileage, driving speed, driving directions, etc.)
			20.5	Unauthorized changes to **system diagnostic data**
	21	Erasure of data/code	21.1	Unauthorized deletion/manipulation of **system event logs**
	22	Introduction of malware	22.2	Introduce **malicious software** or malicious software activity
	23	Introduction of new software or overwrite existing software	23.1	**Fabrication of software** 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	**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
	25	Manipulation of vehicle parameters	25.1	Unauthorized access of **falsify the configuration parameters** of vehicle's key functions, such as brake data, airbag deployed threshold, etc.
			25.2	Unauthorized access of **falsify the charging parameters**, 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 **encryption keys** 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 **cryptographic algorithms**
	27	Parts or supplies could be compromised to permit vehicles to be attacked	27.1	**Hardware or software, engineered to enable an attack** or fails to meet design criteria to stop an attack
	28	Software or hardware development permits vulnerabilities	28.1	**Software bugs**. 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	**Using remainders** 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	**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
	31	Unintended transfer of data can occur	31.1	Information breach. Personal data may be leaked when the **car changes user** (e.g. is sold or is used as hire vehicle with new hirers)
	32	Physical manipulation of systems can enable an attack	32.1	**Manipulation of electronic hardware**, e.g. unauthorized electronic hardware added to a vehicle to enable "man-in-the-middle" attack **Replacement of authorized electronic hardware** (e.g., sensors) with unauthorized electronic hardware **Manipulation of the information** 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 M6	The vehicle shall verify the authenticity and integrity of messages it receives 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 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

Table A1 reference	*Threats to "Vehicle communication channels"*	*Ref*	*Mitigation*
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"

Table A1 reference	*Threats to "Update process"*	*Ref*	*Mitigation*
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"

Table A1 reference	*Threats relating to "Unintended human actions"*	*Ref*	*Mitigation*
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"

Table A1 reference	*Threats to "External connectivity and connections"*	*Ref*	*Mitigation*
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. 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"

Table A1 reference	*Threats to "Potential targets of, or motivations for, an attack"*	*Ref*	*Mitigation*
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. 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"

Table A1 reference	*Threats to "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened"*	*Ref*	*Mitigation*
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. 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. 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"

Table A1 reference	*Threats of "Data loss / data breach from vehicle"*	*Ref*	*Mitigation*
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"

Table A1 reference	*Threats to "Physical manipulation of systems to enable an attack"*	*Ref*	*Mitigation*
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"

Table A1 reference	*Threats to "Back-end servers"*	*Ref*	*Mitigation*
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"

Table A1 reference	*Threats relating to "Unintended human actions"*	*Ref*	*Mitigation*
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"

Table A1 reference	*Threats of "Physical loss of data"*	*Ref*	*Mitigation*
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)		

CYBENTIA GRUPO

CONSULTORA
DE INVESTIGACIÓN,
CONCIENCIACIÓN
Y COMUNICACIÓN
ESTRATÉGICA

UNECE R/155

APÉNDICES A LA NORMATIVA R155 DESDE 2021 A 2024

E/ECE/TRANS/505/Rev.3/Add.154/Amend.1

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."

E/ECE/TRANS/505/Rev.3/Add.154/Amend.2

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	**Spoofing of messages** by impersonation (e.g. V2X cooperative awareness or manoeuvre coordination messages, GNSS messages, etc.)
			4.2	**Sybil attack** (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:

Table A1 reference	*Threats to "Vehicle communication channels"*	*Ref*	*Mitigation*
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

CYBENTIA®
GRUPO

CONSULTORA
DE INVESTIGACIÓN,
CONCIENCIACIÓN
Y COMUNICACIÓN
ESTRATÉGICA

UNECE R/155

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

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 Adaptative 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) 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)

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)

Reproduction is permitted provided that the source is acknowledged.

Contact us (/unece-information-service)

CYBENTIA® GRUPO

CONSULTORA
DE INVESTIGACIÓN,
CONCIENCIACIÓN
Y COMUNICACIÓN
ESTRATÉGICA

UNECE R/156

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

E/ECE/TRANS/505/Rev.3/Add.155

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

Page

1. Scope

1.1. This Regulation applies to vehicles of Categories[1] 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:

[1] 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

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. [2]

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.

[2] 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.

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: ....

....

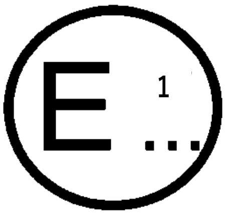
(Stamp and signature of the manufacturer's representative)

Annex 2

Communication

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

issued by: Name of administration:
....
....
....



Concerning:[2] 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.

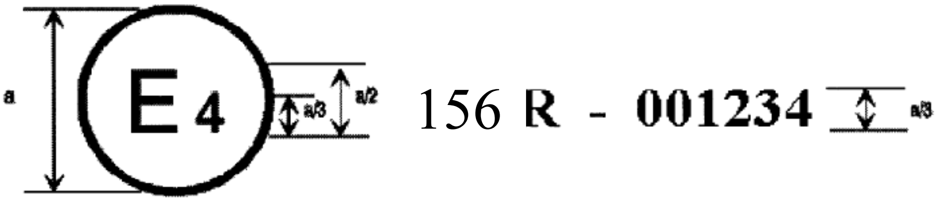
[1] Distinguishing number of the country which has granted/extended/refused/withdrawn approval (see marking provisions (footnote) in this Regulation).

[2] Strike out what does not apply.

Annex 3

Arrangement of approval mark

Model A
(See paragraph 4.2 of this Regulation)



a = 8 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*]

CYBENTIA GRUPO

CONSULTORA
DE INVESTIGACIÓN,
CONCIENCIACIÓN
Y COMUNICACIÓN
ESTRATÉGICA

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

WP.29 World Forum for Harmonization of Vehicle Regulations

- UN Regulation 155 on Cyber Security
- UN Regulation 156 on SW updates
- UN Recommendations on cyber security and software updates

European Union

- Cybersecurity Act
- General Data Protection Regulation
- NIS Directive (Network and Information Security)

ISO TC22/SC32/WG11 - Cybersecurity

- ISO/SAE 21434 Cybersecurity Engineering

ISO TC22/SC32/WG12 – Software update

- ISO 24089 Software Update Engineering

China

- Cybersecurity Law & Data Security Law
- Personal Information Protection Law
- Information Security: SAC/TC 260
- Automotive: SAC/TC 114/SC 34/WG Cyber

National Discussions

- UK BSI PAS 1885:2018
- …

USA

- NHTSA Cybersecurity Guidelines

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

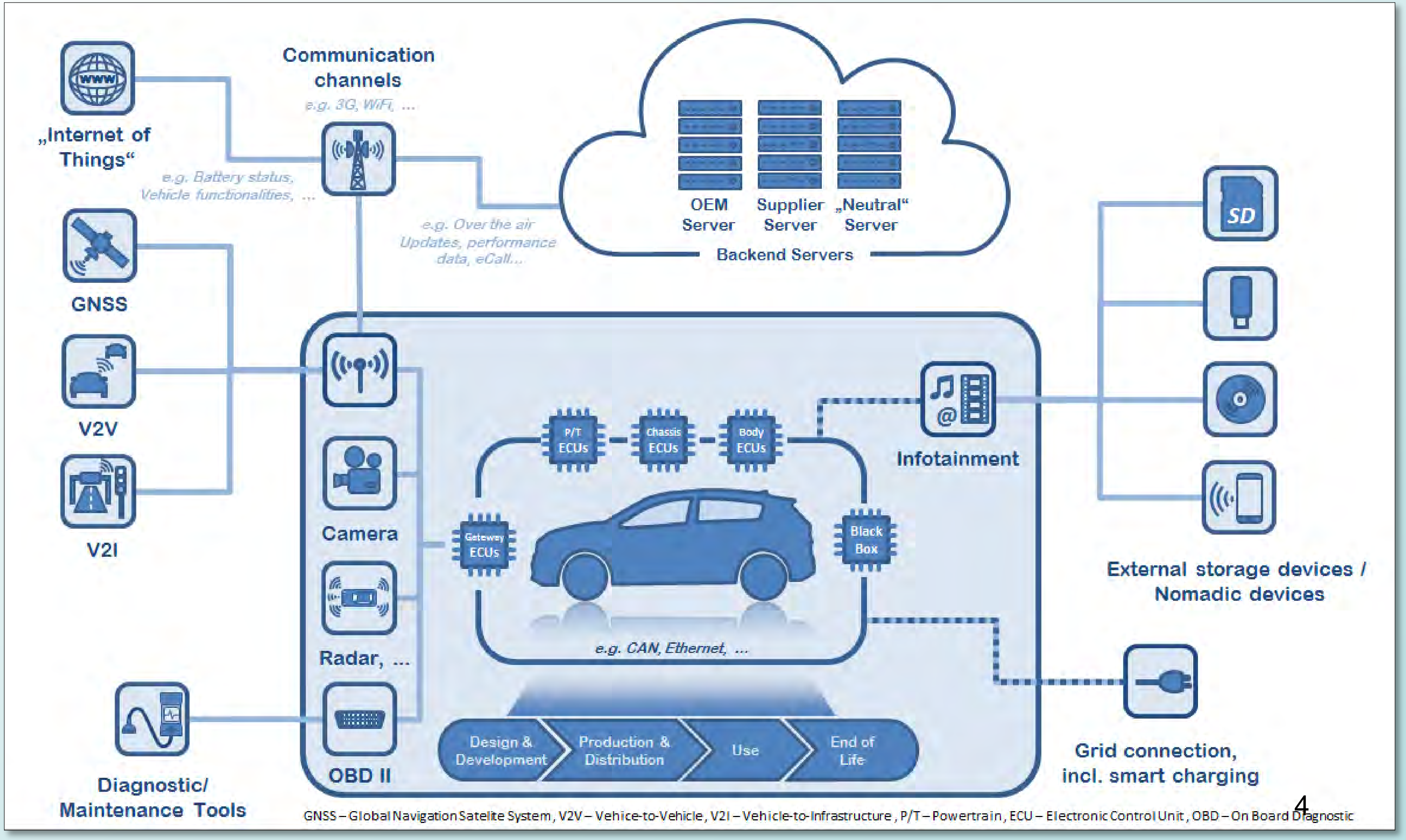
Developed under GRVA (chaired by Germany, Japan and China)
/ IWG Cybersecurity & OTA issues (chaired by UK, Japan and USA).
=> **Japan** and **European Union** are the first regions that make the regulations mandatory in their territory.

Why cybersecurity regulation?

- Risk of cyberattacks
  - **Safety/Security/Environmental impact**:
    - Hacker may
      - **be** the **vehicle user**
      - **manipulate** existing vehicle software
      - get access to **private/confidential data** (incl. location and charging history)
      - 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**



GNSS – Global Navigation Satelite System, V2V – Vehice-to-Vehicle, V2I – Vehicle-to-Infrastructure, P/T – Powertrain, ECU – Electronic Control Unit, OBD – On Board Diagnostic

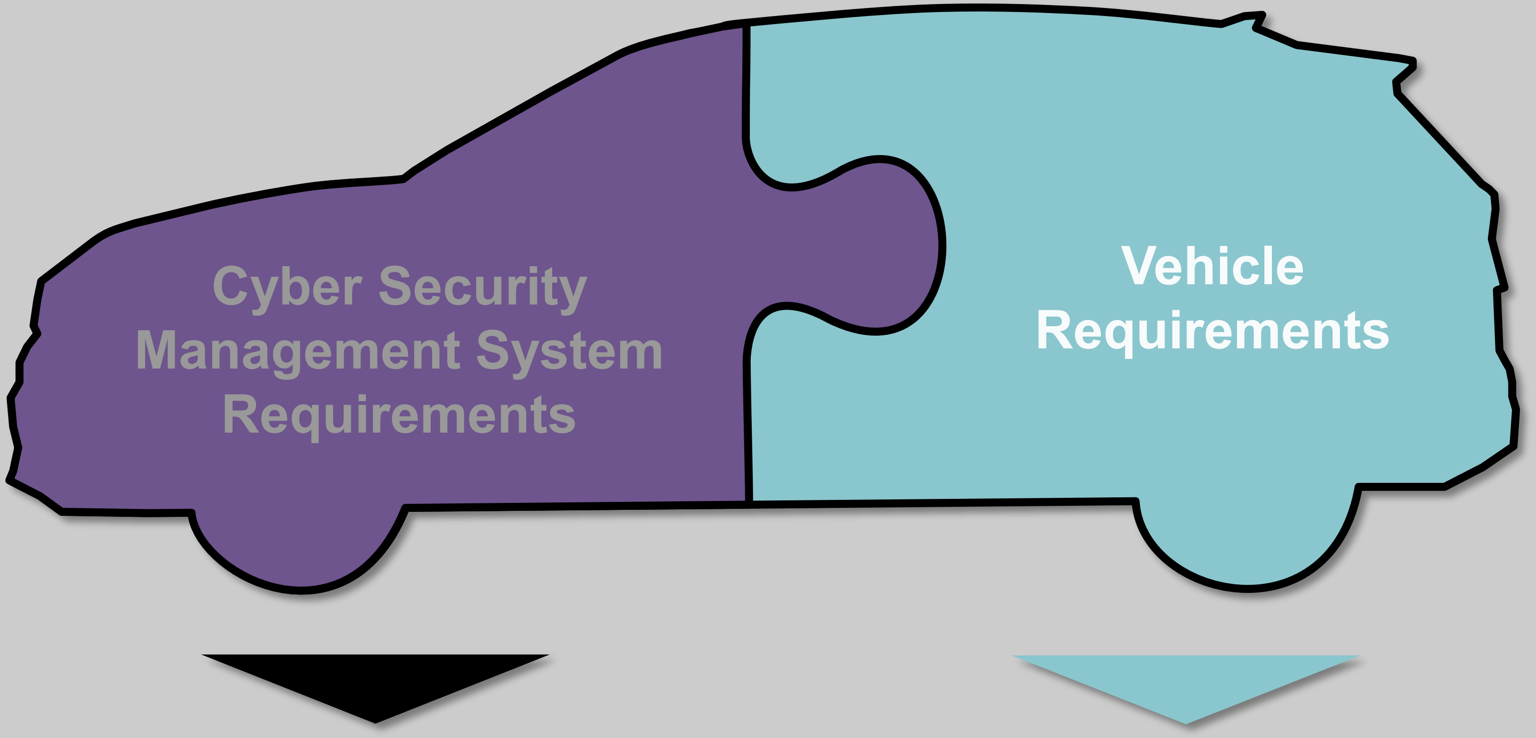
⇒ Cybersecurity cannot be covered by certification of only some specific components

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**



Cyber Security Management System Requirements

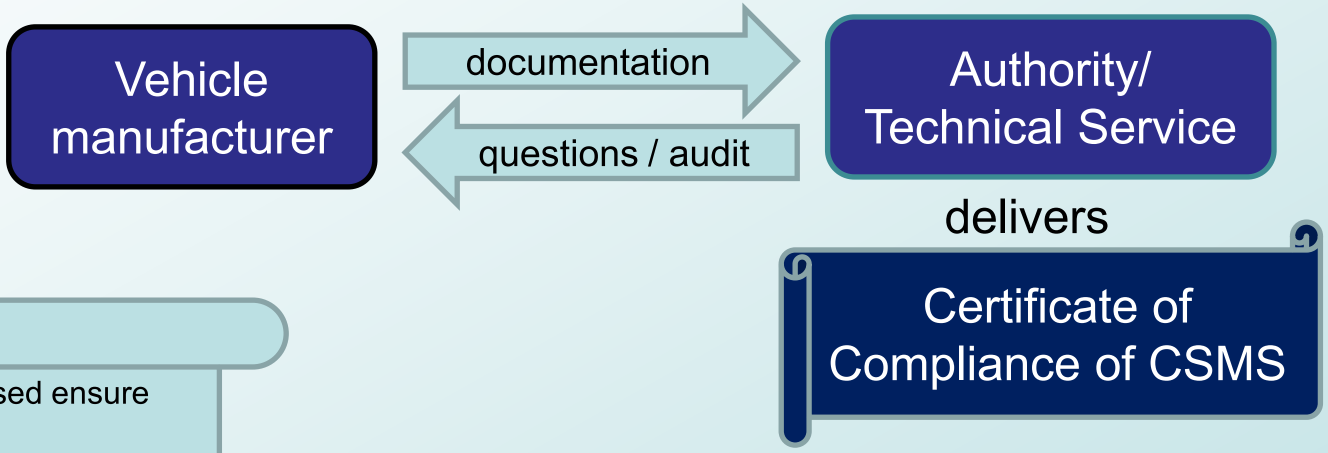
Vehicle Requirements

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:
a) manage cyber security
b) identification of risks to vehicle types (see Annex 5, part A)
c) assessment, categorization and treatment of the risks identified
d) verify that the risks identified are appropriately managed
e) testing the security of the system
f) ensuring that the risk assessment is kept current
g) monitor for, detect and respond to cyber-attacks on vehicle types and assess whether the cyber security measures implemented are still effective
h) 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

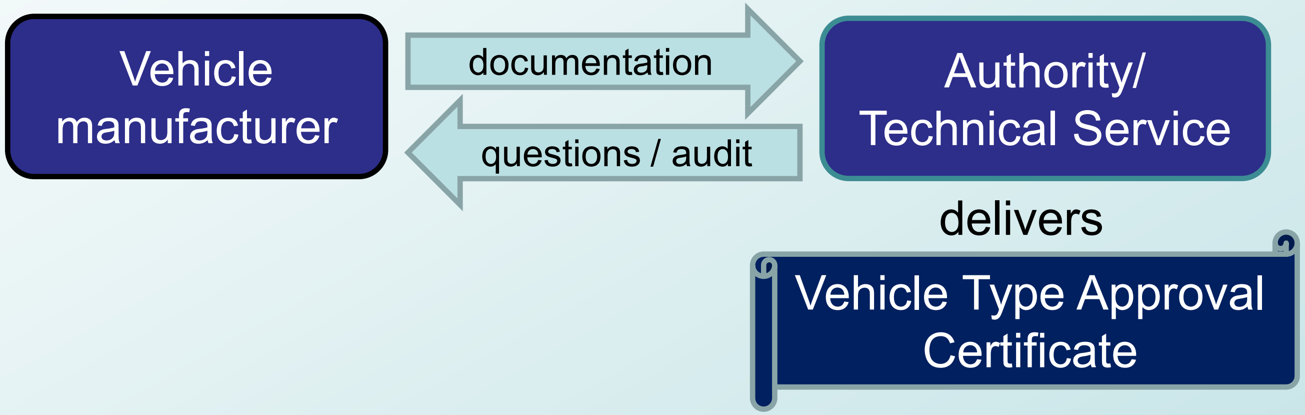
7.3.1. Vehicle manufacturer shall have valid Certificate of Compliance relevant to the vehicle type being approved.

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.


Vehicle manufacturer
documentation
questions / audit
Authority/ Technical Service
delivers
Vehicle Type Approval Certificate

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

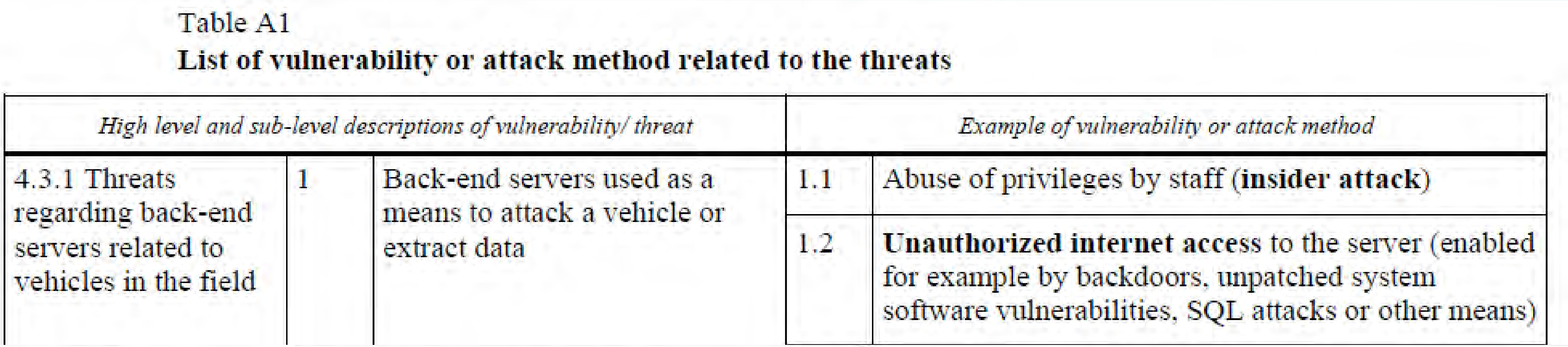
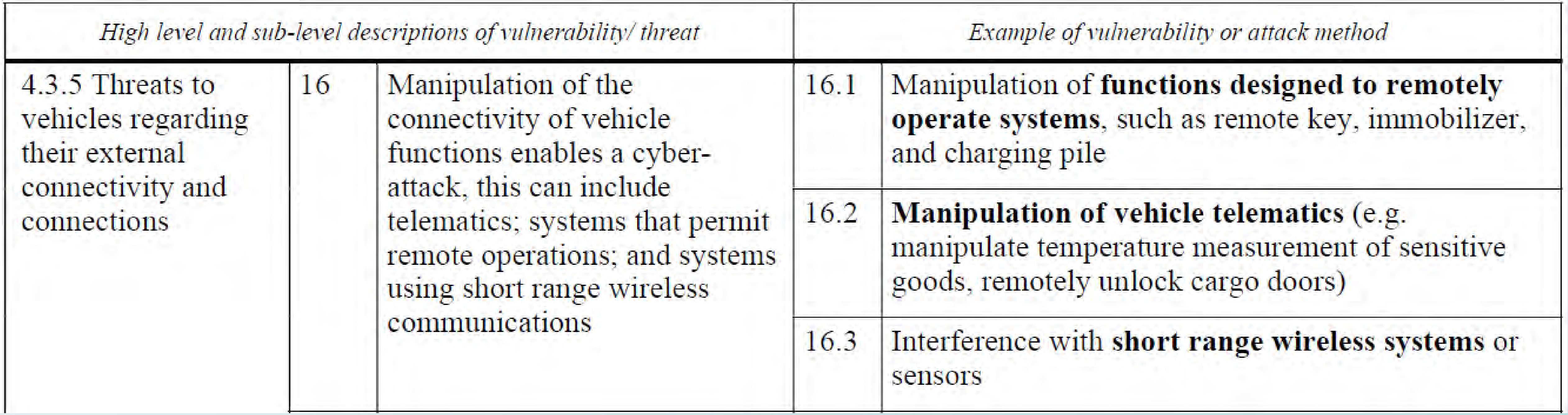


Table A1

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 (**insider attack**)
			1.2	**Unauthorized internet access** 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 **functions designed to remotely operate systems**, such as remote key, immobilizer, and charging pile
			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 B: Mitigations on vehicles

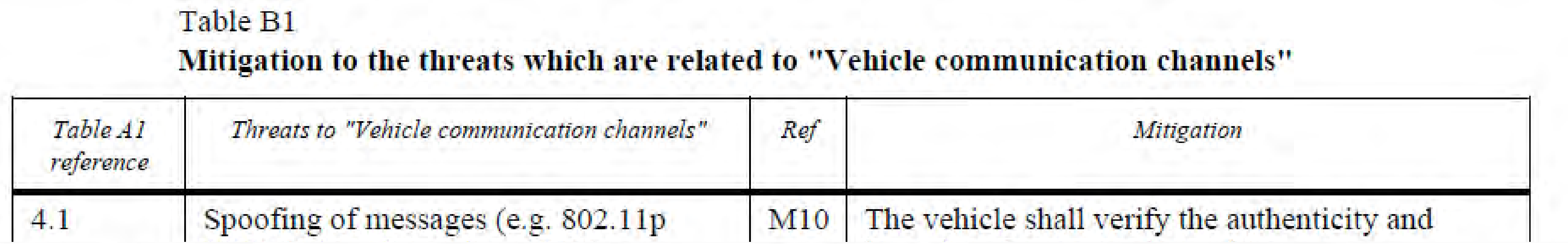


Table B1

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	M10	The vehicle shall verify the authenticity and

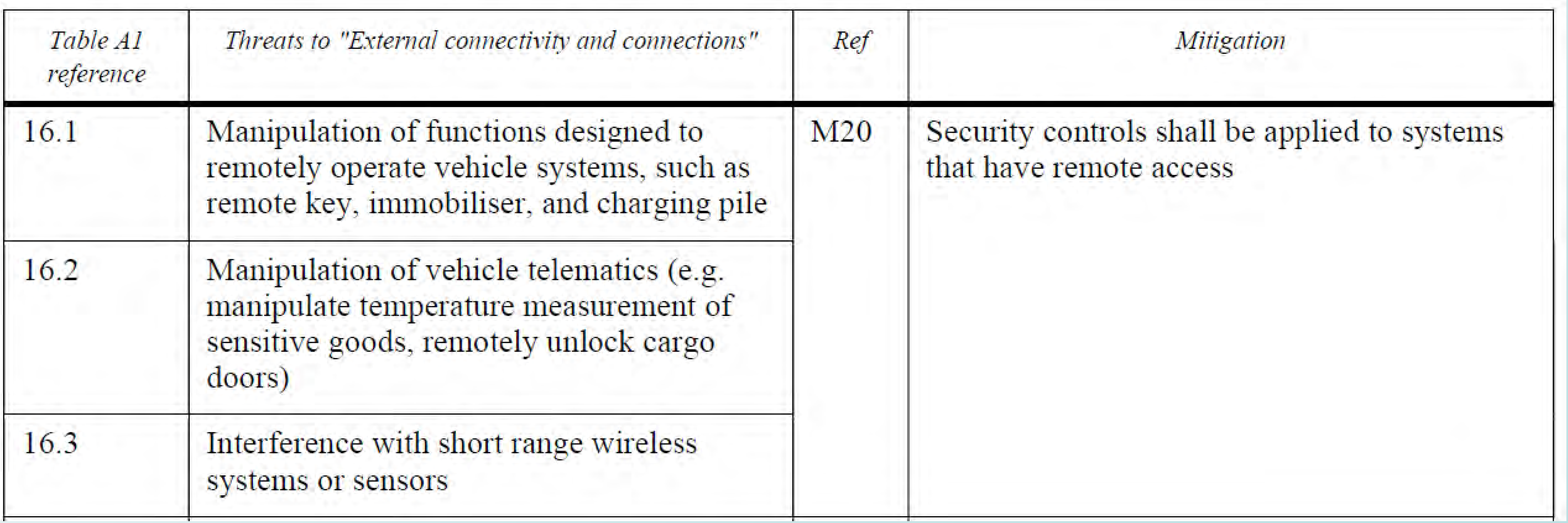


Table A1 reference	*Threats to "External connectivity and connections"*	*Ref*	*Mitigation*
16.1	Manipulation of functions designed to remotely operate vehicle systems, such as remote key, immobiliser, and charging pile	M20	Security controls shall be applied to systems that have remote access
16.2	Manipulation 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

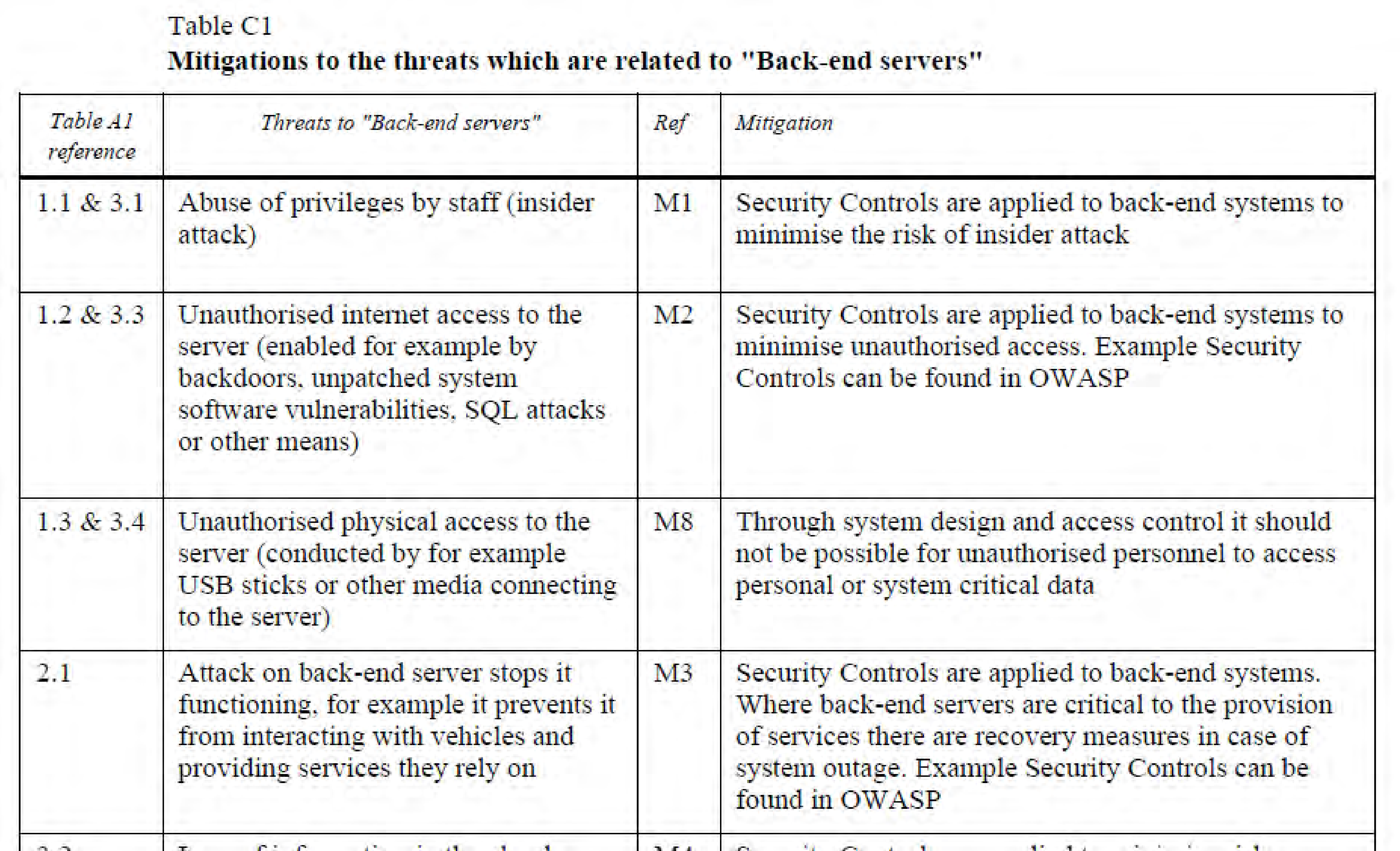


Table C1

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

Table A1 reference	*Threats to "Back-end servers"*	*Ref*	*Mitigation*
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

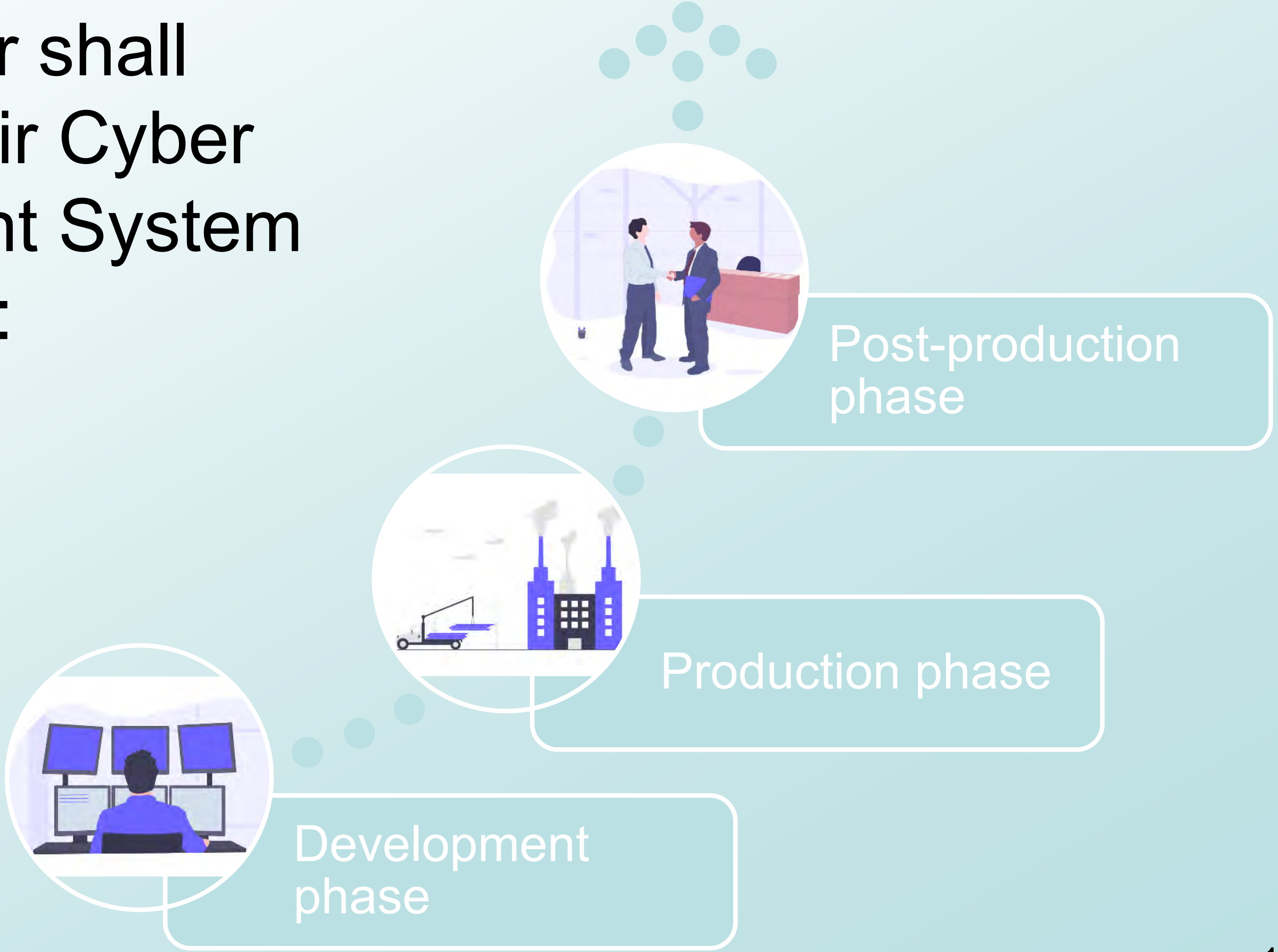
Requirements for the whole vehicle life cycle

- 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



Post-production phase

Production phase

Development 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!

CYBENTIA GRUPO

CONSULTORA
DE INVESTIGACIÓN,
CONCIENCIACIÓN
Y COMUNICACIÓN
ESTRATÉGICA

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/wp29fdocstts.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

ANEXOS

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_6 y L_7 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 [1];

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» [2], 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 [3].

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 [4] 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 [5]. 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 [6].

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: ………………………………………………………………………………………………

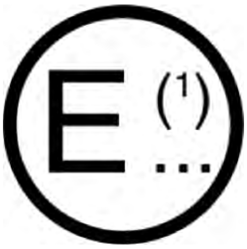
……

(*Sello y firma del representante del fabricante*)

ANEXO 2

Comunicación

[Formato máximo: A4 (210 × 297 mm)]



Expedida por: Nombre de la administración:
....
....
....

relativa a (2) 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.

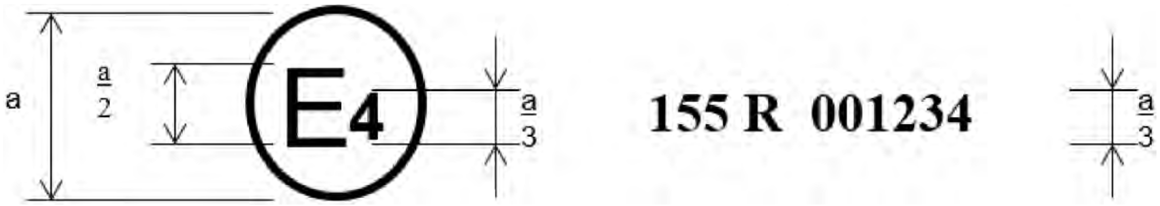
[2] Número distintivo del país que ha concedido/extendido/denegado/retirado la homologación (véanse las disposiciones del Reglamento relativas a la homologación).:

ANEXO 3

Disposición de la marca de homologación

MODELO A

(Véase el punto 4.2 del presente Reglamento)



a = 8 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) perdida 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 *back-end* en relación con vehículos sobre el terreno	1	Servidores *back-end* 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 *backdoors*, vulnerabilidades de un *software* 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 *back-end*, lo que afecta al funcionamiento de un vehículo	2.1	El ataque al servidor *back-end* 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 *back-end* 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 *backdoors*, vulnerabilidades de un *software* 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 *software* 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 sobreescribir 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 *software* de una unidad de control electrónico o el *firmware* 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 *root*
	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 *software*. Esto incluye la falsificación del programa de actualización del sistema o *firmware*
			12.2	Compromiso de los procedimientos locales/físicos de actualización de *software*. Esto incluye la falsificación del programa de actualización del sistema o *firmware*
			12.3	El *software* 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 *software* 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 *software* 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 *software* 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	*Software* 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 *software* 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 ODB) 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	Extracción de *software* propietario o protegido con derechos de autor de los sistemas del vehículo (piratería)
			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 *back-end* 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 *software* malicioso	22.2	Introducción de *software* malicioso o actividad de *software* malicioso
	23	Introducción de *software* nuevo o sobreescritura de *software* ya existente	23.1	Fabricación de *software* 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	*Hardware* o *software* diseñados para permitir un ataque o que no cumplen los criterios de diseño para detener un ataque
	28	El desarrollo de *software* o *hardware* permite vulnerabilidades	28.1	Errores de *software*. La presencia de errores de software puede ser la base de posibles vulnerabilidades aprovechables. Esto se aplica sobre todo si el *software* 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 *hardware* electrónico, p. ej., la instalación de *hardware* electrónico no autorizado en un vehículo para posibilitar un ataque de intermediario Sustitución de *hardware* electrónico autorizado (p. ej., sensores) por *hardware* electrónico no autorizado 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 *hardware*)
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 *software* en el flujo de comunicación	M10 M6	El vehículo verificará la autenticidad e integridad de los mensajes que recibe 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 sobreescribir los datos o el código almacenados por el vehículo		
5.4 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 *software* de una unidad de control electrónico o el *firmware* 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 *root*	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 *software* 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 *software*. Esto incluye la falsificación del programa de actualización del sistema o *firmware*	M16	Se emplearán procedimientos seguros de actualización del *software*
12.2	Compromiso de los procedimientos locales/físicos de actualización de *software*. Esto incluye la falsificación del programa de actualización del sistema o *firmware*		
12.3	El *software* 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 *software* 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 *software* crítico o el desbloqueo de características específicas del cliente	M3	Se aplicarán controles de seguridad a los sistemas de *back-end.* Cuando los servidores *back-end* 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 *software* 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 *software* utilizadas como método para atacar los sistemas del vehículo	M21	Se evaluará la seguridad del software, se autentificará y se protegerá su integridad. Se aplicarán controles de seguridad para minimizar el riesgo procedente del *software* 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 *software* 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 *back-end* 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 *software* malicioso o actividad de *software* 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 *software* 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 *software* y *hardware*

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	*Hardware* o *software* 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 *software* y *hardware*
28.1	La presencia de errores de *software* puede ser la base de posibles vulnerabilidades aprovechables. Esto se aplica sobre todo si el *software* 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 *software* y *hardware*. 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 *software* y *hardware*. 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 *hardware* del fabricante de equipo original, p. ej., la instalación de *hardware* 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 el cuadro C1

Cuadro C1

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

Referencia al cuadro A1	Amenazas para «servidores back-end»	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 *back-end* 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 *backdoors*, vulnerabilidades de un *software* del sistema sin parches, ataques SQL u otros medios)	M2	Se aplican controles de seguridad a los sistemas de *back-end* 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 *back-end* 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 *back-end*. Cuando los servidores *back-end* 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 *back-end* 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 *software* 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)		

CYBENTIA GRUPO

CONSULTORA
DE INVESTIGACIÓN,
CONCIENCIACIÓN
Y COMUNICACIÓN
ESTRATÉGICA

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

Submitted by GRVA

Informal document **WP.29-182-05**
182 WP.29, 10-13 November 2020
Agenda item 3.6.4.

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 alterative 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 sub-paragraphs 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". If 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

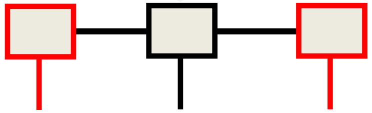
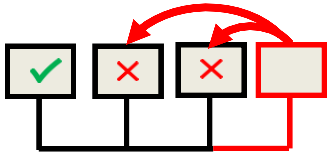
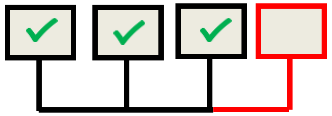
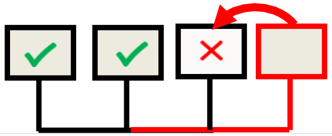
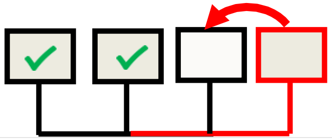
AI. Paragraph 8.

"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 **changes** in the E/E Architecture	Impact on type	Examples
New type	**Development of a new E/E Architecture**		Development of an E/E Architecture requires a **new type**.	Development of an E/E Architecture requires a **new type**.
	Change to the outcome of risk assessment by introducing new		Requires a **new type**, since security in existing subsystem is being influenced.	• Adding new external interfaces (NFC Near Field Communication) for new services such as personalization • Change of network topology by adding a new gateway
Extension of existing type	**Minor changes to the outcome of risk assessment by adding or replacing subsystems**	 	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 **thus requires a type extension**.	• Replacing a UMTS communication unit by a 5G communication unit -> additional communication possible • Replacing an ECU by a new one with a HSM (hardware security module)
No impact	**No change of outcome of risk assessment**		Replacing an existing subsystem, and this does not change the cybersecurity of the resulting E/E architecture, and thus does **not require a type extension**. **<u>This is the usual situation</u>**.	Replacing an ECU: 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 (in man-days)**
Pre-audit, if required *e.g. involvement of auditors in productive processes, planning of audit, adaptation of audit workflow*		
Document handover		
Preparation for audit activities *Including document review, e.g. sort, check for completeness, audit of contents*		
Conducting the on-site audit		
Assessment of rectification efforts *e.g. rectifications completed by auditee during the audit may address findings of the audit*		
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 *Examples*	**Staffing requirement** *Examples*	**Tasks/remarks** *Examples*
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	*Example:* *Lead auditor, CS process expert*	*Example: University degree in computer science, mathematics, physics, engineering or similar.*	*Example: Diploma or certificate.*
Work experience		*Example: Five years of job experience including two years in the field of information security.*	*Example: 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/context1

<Focus Area 2 *(e.g. risk management)*>

Requirement	Audit question	Intent/purpose of question	Minimum performance criteria	Best practice	Additional information/context1

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 *Examples*	**Staffing requirement**	**Tasks/remarks**
Lead assessor	*1*	*Manage assessment process; accountable and responsible*
CS process expert	*1*	*Responsible for transferring CSMS knowledge and understanding to the assessment of the vehicle type; ideally personal staffing overlap with CSMS audit team*
CS Product expert	*2*	
Penetration tester	*1-2*	
…		
Documentation Management		

[1] 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	*Example: lead assessor, product expert*	*Example: University degree in computer science, mathematics, physics, engineering or similar.*	*Example: Diploma or certificate.*
Work experience		*Example: Five years of job experience including two years in the field of information security.*	*Example: Job reference.*
Practical experience		*Example: Experience with automobile E/E architectures and experience with cybersecurity assessment and penetration testing*	*Example: Job or project reference.*
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 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	*Not applicable*
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.	
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]. 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	

<table>
<tr><td colspan="2">vulnerabilities which require a response from the vehicle manufacturer shall be mitigated within a reasonable timeframe.</td></tr>
<tr><td>Mitigation within reasonable timeframe</td><td>No timeframe defined by ISO/SAE DIS 21434 (E)</td></tr>
<tr><td colspan="2">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:
(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.</td></tr>
<tr><td>Monitoring after first registration</td><td>Clause 7.3 “Cybersecurity Monitoring”</td></tr>
<tr><td>Capability to analyse and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs</td><td>Not explicitly mentioned in ISO/SAE DIS 21434 (E), but could be seen as Cybersecurity Information.</td></tr>
<tr><td>Respecting privacy rights of car owners or drivers, particularly with respect to consent</td><td>Out of scope of ISO/SAE 21434, so not applicable</td></tr>
<tr><td colspan="2">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.</td></tr>
<tr><td>Dependencies that may exist with contracted suppliers</td><td>[RQ-06-09], [RQ-15-03], [RC-15-02]</td></tr>
<tr><td>Dependencies that may exist with contracted service providers</td><td>[RQ-06-09], [RQ-15-03], [RC-15-02]</td></tr>
<tr><td>Dependencies that may exist with manufacturer’s sub-organizations</td><td>[RQ-06-09], [RQ-15-03], [RC-15-02]</td></tr>
</table>

CYBENTIA GRUPO

CONSULTORA
DE INVESTIGACIÓN,
CONCIENCIACIÓN
Y COMUNICACIÓN
ESTRATÉGICA

Normalización en ciberseguridad para la movilidad conectada y automatizada de vehículos y su entorno

UNE

NormalizaciónEspañola

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 Tecnalia 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

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)[1], en particular de los Vehículos Conectados y Automatizados (CAVs)[2], Sistemas Inteligentes de Transporte (ITS)[3] y las tecnologías de comunicación y conectividad involucradas.

2 Antecedentes

El reto social de la movilidad inteligente[4] 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[5] 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 critica 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[6].

ENISA[7] 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[8], 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[9] en Europa, participan en varios proyectos piloto en el área de la movilidad inteligente. ERTICO también ha publicado recomendaciones[10] sobre tecnologías de comunicación para futuros escenarios de ITS cooperativos (C-ITS). El Foro Americano sobre el Futuro de la Privacidad[11] y la Asociación Nacional de Concesionarios de Automóviles (NADA) han publicado una guía para el consumidor[12] 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)[13] 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

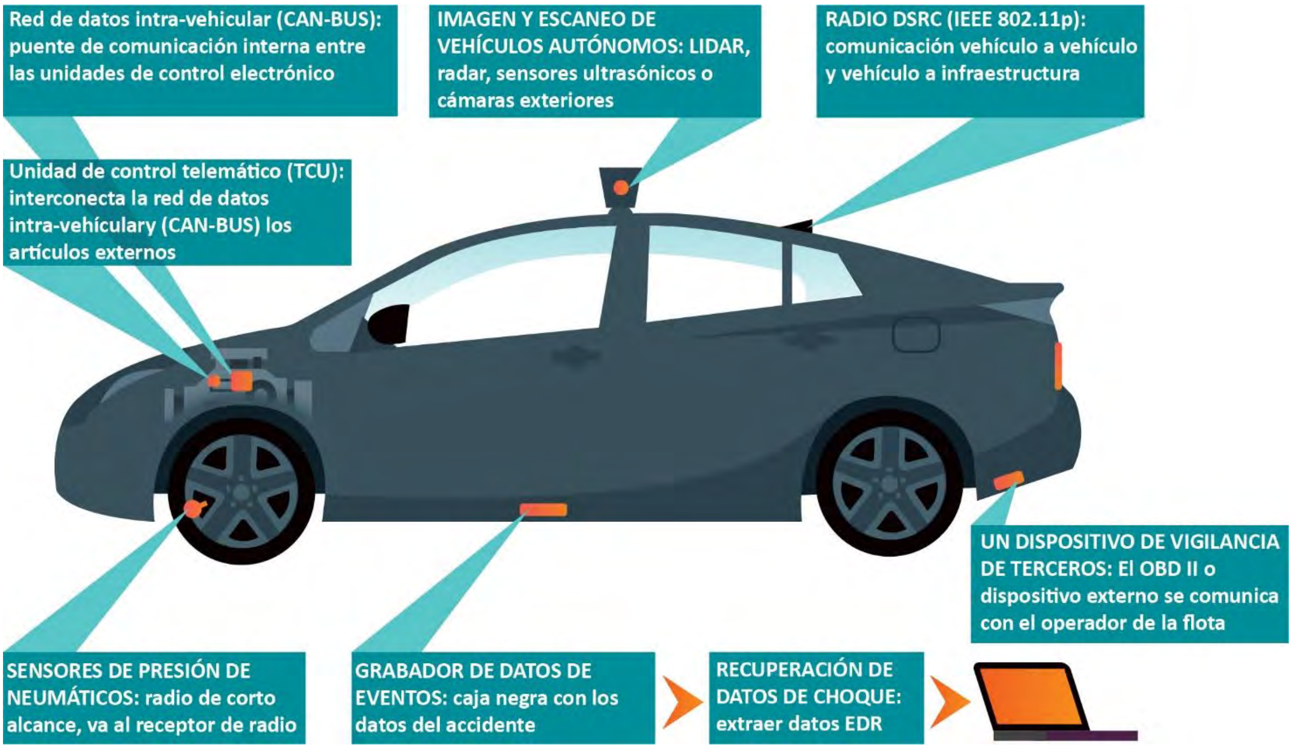

Red de datos intra-vehicular (CAN-BUS): puente de comunicación interna entre las unidades de control electrónico
IMAGEN Y ESCANEO DE VEHÍCULOS AUTÓNOMOS: LIDAR, radar, sensores ultrasónicos o cámaras exteriores
RADIO DSRC (IEEE 802.11p): comunicación vehículo a vehículo y vehículo a infraestructura
Unidad de control telemático (TCU): interconecta la red de datos intra-vehículary (CAN-BUS) los artículos externos
UN DISPOSITIVO DE VIGILANCIA DE TERCEROS: El OBD II o dispositivo externo se comunica con el operador de la flota
SENSORES DE PRESIÓN DE NEUMÁTICOS: radio de corto alcance, va al receptor de radio
GRABADOR DE DATOS DE EVENTOS: caja negra con los datos del accidente
RECUPERACIÓN DE DATOS DE CHOQUE: extraer datos EDR

Figura 1: Vehículo conectado con diferentes funciones

(Fuente: Foro sobre el Futuro de la Privacidad, modificado)

[13] https://www.its.dot.gov/resources/scms.htm

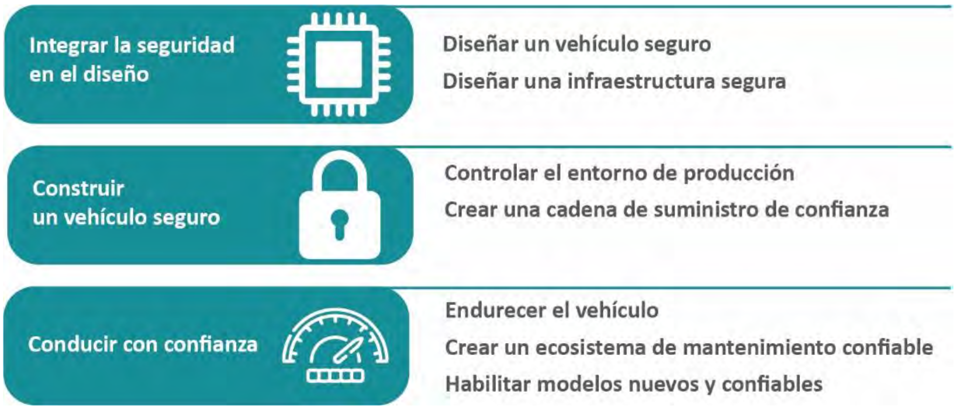

Integrar la seguridad en el diseño
Diseñar un vehículo seguro
Diseñar una infraestructura segura
Construir un vehículo seguro
Controlar el entorno de producción
Crear una cadena de suministro de confianza
Conducir con confianza
Endurecer el vehículo
Crear un ecosistema de mantenimiento confiable
Habilitar modelos nuevos y confiables

Figura 2: Enfoque de Diseño, Construcción y Conducción de IBM[14]
(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)

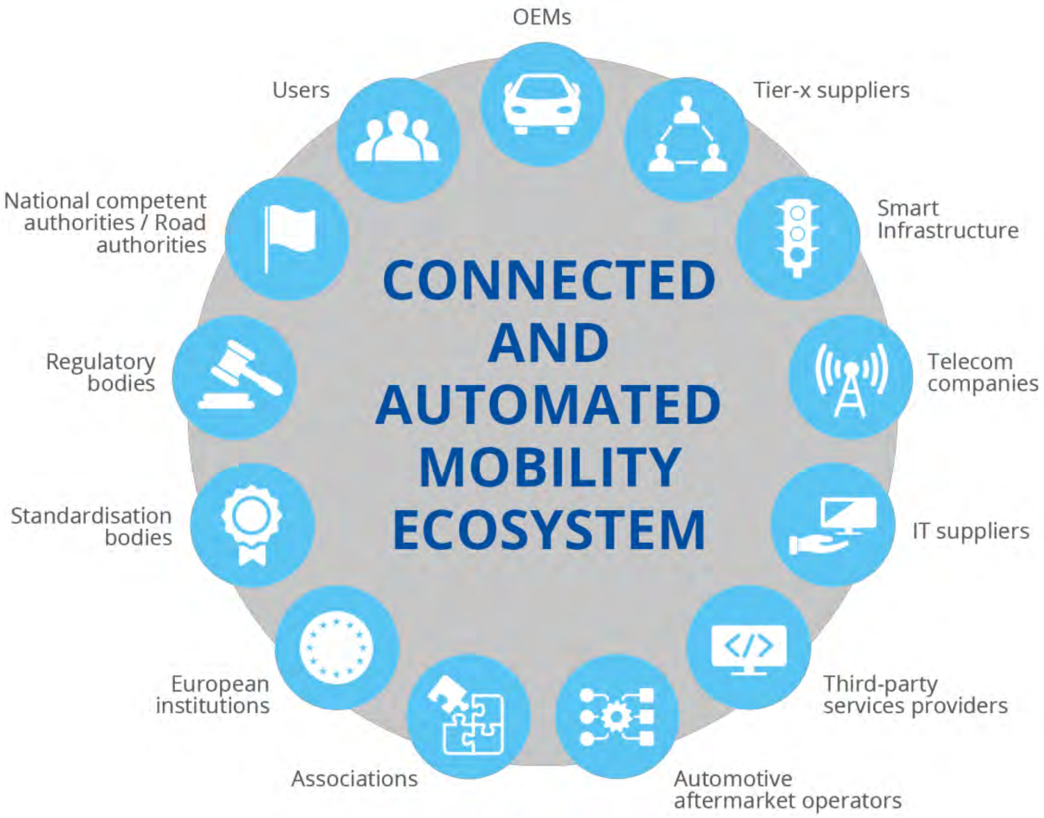
La industria de la Movilidad Conectada y Automatizada (CAM) se basa en un amplio ecosistema de actores que cubren las diferentes áreas de la cadena de valor desde I + D y fabricación, venta minorista y prestación de servicios, operaciones, mantenimiento y gestión de infraestructuras y flotas, así como 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[15], 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.


OEMs
Tier-x suppliers
Smart Infrastructure
Telecom companies
IT suppliers
Third-party services providers
Automotive aftermarket operators
Associations
European institutions
Standardisation bodies
Regulatory bodies
National competent authorities / Road authorities
Users
CONNECTED AND AUTOMATED MOBILITY ECOSYSTEM

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[16] 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/digitalsingle-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[17].

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)[18].

[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

El Centro Común de Investigación[19] de la Comisión Europea ha definido la Infraestructura de clave pública[20] de seguridad en toda la UE como la característica más relevante de C-ITS y V2X y ha establecido estos sistemas como una infraestructura critica 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).

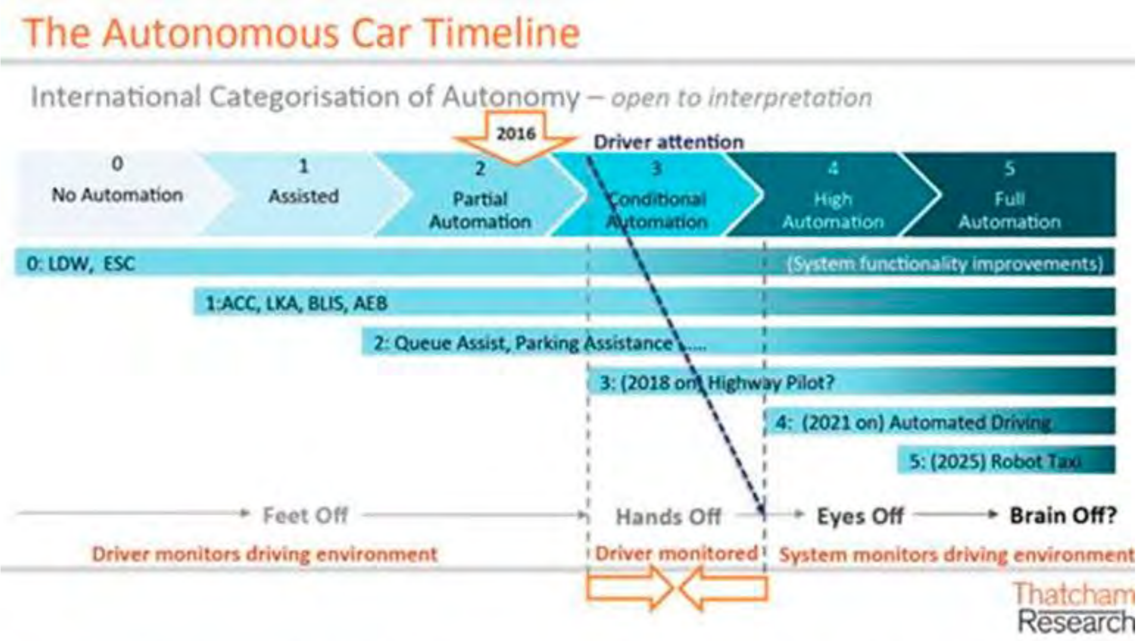

The Autonomous Car Timeline
International Categorisation of Autonomy – open to interpretation
2016
Driver attention
0
No Automation
1
Assisted
2
Partial Automation
3
Conditional Automation
4
High Automation
5
Full Automation
0: LDW, ESC
(System functionality improvements)
1:ACC, LKA, BLIS, AEB
2: Queue Assist, Parking Assistance.....
3: (2018 on) Highway Pilot?
4: (2021 on) Automated Driving
5: (2025) Robot Taxi
Feet Off
Hands Off
Eyes Off
Brain Off?
Driver monitors driving environment
Driver monitored
System monitors driving environment
Thatcham Research

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 procesado 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 estandardización 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 estandardización 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 estandardización, en IEC e ISO, para conectores, cables y conformidad para esta nueva ola de comunicaciones dentro del vehículo por encima del Gibabit 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 conexionado 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[21] 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.

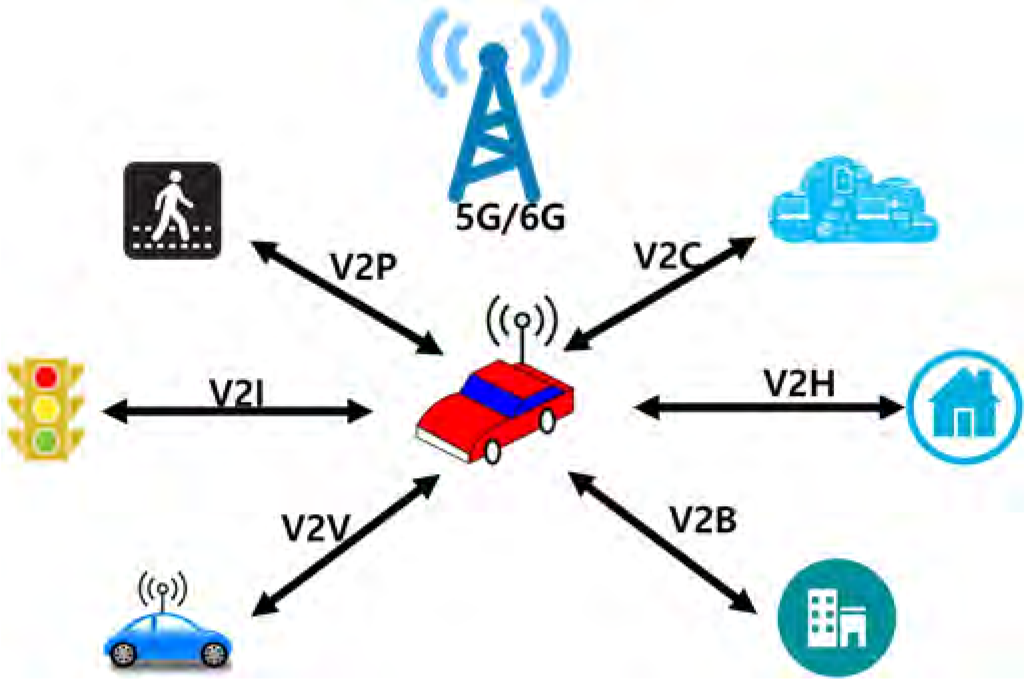
En cuanto a redes intra-vehiculares, el estado de la implementación tecnológica y de la estandardización se encuentra más avanzada.

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 estandardización 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 autentificación 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. Estandardizado en la familia de estándares ISO 17458. La definición de casos de uso se estandardizó 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. Estandardizado 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. Estandardizado 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. Estandardizado en la familia de estándares ISO 21111 e ISO/IEC/IEEE 8802-3. Hay desarrollos en estandardización 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 diagnosis 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 trasmisión.

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 trasmisión, lo cual podría ser fatal en muchas circunstancias y tener un impacto real en la seguridad (s*afety*) 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, estandardizado 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 valida. 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 "entreteinment" 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 tráficos 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 incluyo 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[22] 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[23] (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.[24]".

Esta norma establece las guías de auditoria 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 ingles) 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[25] 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

- El perfil de protección desarrollado por el BSI Alemán (organismo de certificación del esquema CC en Alemania) para equipos de señalización en la carretera[26].

- El perfil de protección desarrollado por la Federación Internacional del Automóvil para una unidad genérica de comunicaciones del vehículo[27] (PP pendiente de certificación en CC).

- Los perfiles de protección que se están desarrollado en el Consorcio industrial *"Car2Car Communication Consortium"* para los elementos más críticos en las comunicaciones del vehículo: el V2X HSM[28] o modulo 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[29] 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[30] 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[31] 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

[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

[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

[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[32], 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[33] 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)[34] 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 Publica (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:

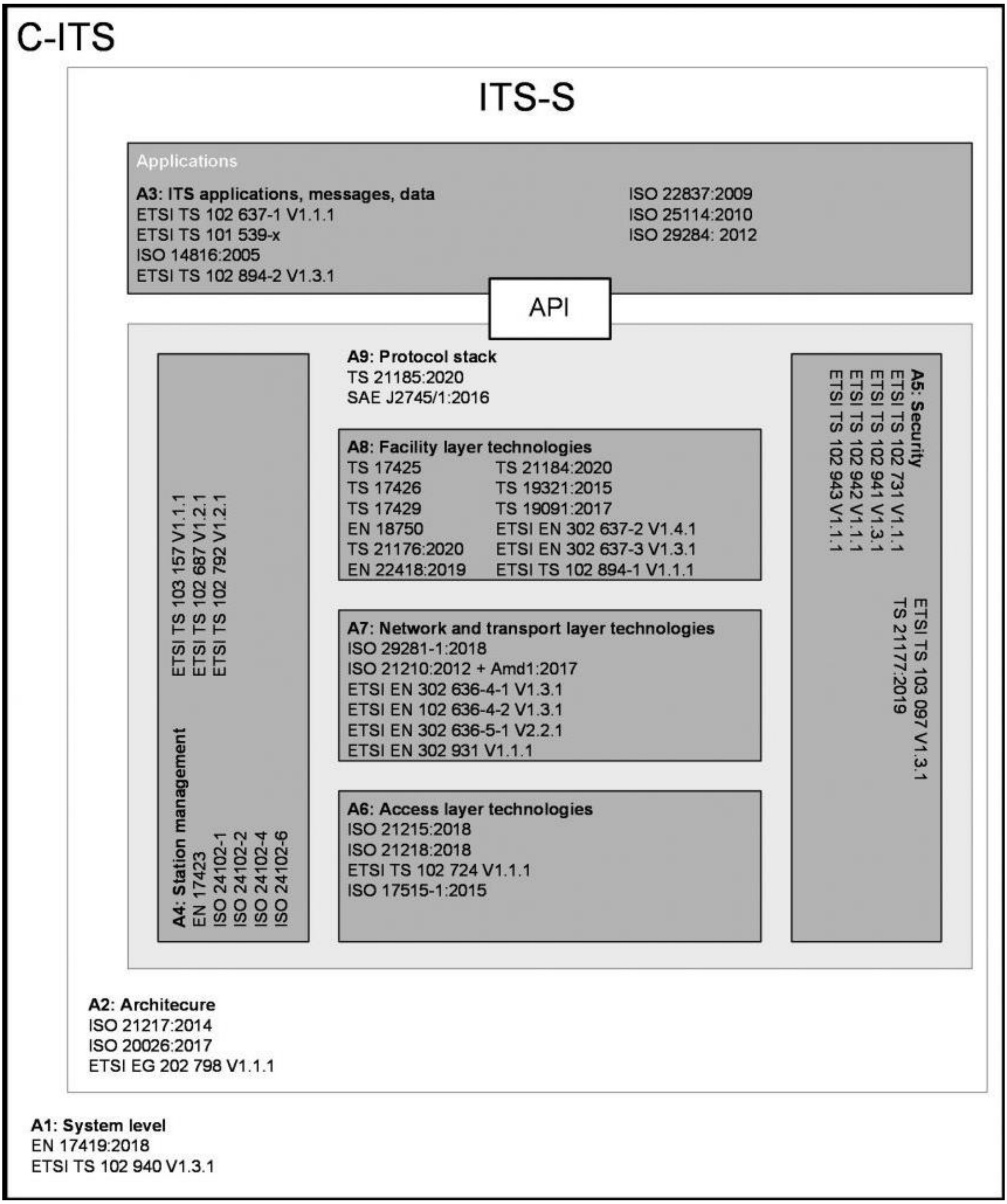
ETSI EN 302 636-4-1 V1.4.1	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking
ETSI TS 103 097 v1.3.	ITS Security; Security header and certificate formats
ETSI TS 102 941 v1.3.11	ITS Security; Trust and Privacy Management
ETSI TS 102 940 v1.3.1	ITS Security; ITS communications 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.[35].

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[36]
GSMA FS.14	Network Equipment Security Assurance Scheme. Security Test Laboratory Accreditation Requirements and Process[37]
GSMA FS.15	Network Equipment Security Assurance Scheme. Vendor Development and Product Lifecycle Requirements and Accreditation Process[38]
GSMA FS.16	Network Equipment Security Assurance Scheme. Dispute Resolution Process[39]

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.

[36] http://www.gsma.com/NESAS_Overview

[37] http://www.gsma.com/NESAS_Test_Lab_Accreditation

[38] http://www.gsma.com/NESAS_Product_Lifecycle_Accreditation

[39] 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 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[40] FIPS-140-3[41], 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*[42] .

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 llego 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”[43]
Press release: "Commission presents a Strategy towards cooperative, connected and automated mobility"[44]
Memo: "An EU strategy on cooperative, connected and automated mobility"[45]
Opinion of the European Economic and Social Committee[46]
Opinion of the European Parliament[47]

[42] 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

[45] 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)[48]
Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) (Release 1.1, June 2018)[49]
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[50]
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[51]

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 ingles *"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

[49] 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

[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)[52]

Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment[53]

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

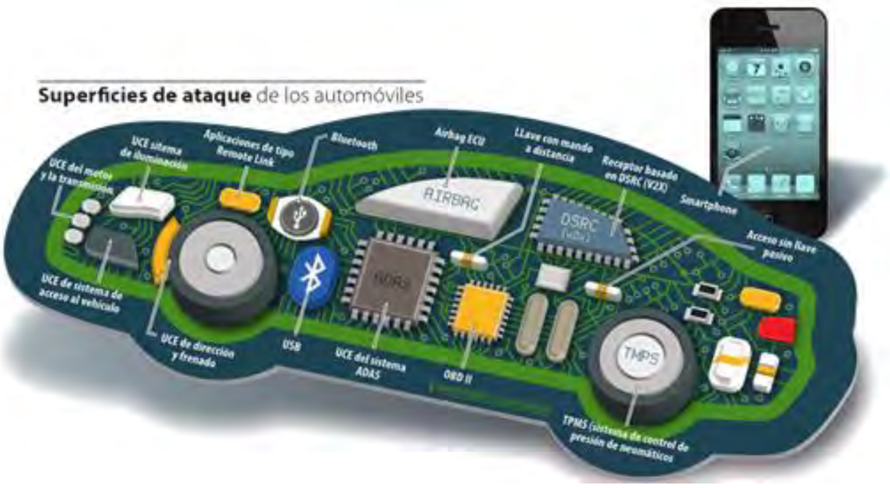
[53] https://ec.europa.eu/docsroom/documents/40763

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:


Superficies de ataque de los automóviles
UCE del motor y la transmisión
UCE sitema de iluminación
Aplicaciones de tipo Remote Link
Bluetooth
Airbag ECU
LLave con mando a distancia
Receptor basado en DSRC (V2X)
Smartphone
Acceso sin llave pasivo
UCE de sistema de acceso al vehículo
UCE de dirección y frenado
USB
UCE del sistema ADAS
OBD II
TPMS (sistema de control de presión de neumáticos
AIRBAG
DSRC
TMPS

- 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 crucero activo.
- Vulnerabilidad de las ECUs.
- Vulnerabilidad *keyless 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 TMPS.
- 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.

Asociación Española
de Normalización

(+34) 915 294 900 — **une@une.org**

www.une.org

Manual de buenas prácticas en seguridad para los vehículos inteligentes

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA GOOD PRACTICES FOR SECURITY OF SMART CARS

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. ENISA works with the EU, its member states, the private sector and Europe's citizens to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Since 2019, it has been drawing up cybersecurity certification schemes. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT

For contacting the authors please use iot-security@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

ENISA

ACKNOWLEDGEMENTS

Charalambos Tsitlakidis, European Commission – DG Communications Networks, Content and Technology

Christophe Jouvray, Valeo

Markus Tschersich, Continental

Gianmarco Baldini, European Commission – DG Joint Research Center

Jasja Tijink, Kapsch Trafficcom AG

Erwan Broquaire, Cerema

Jocely Delatre, ACEA

Ba Sadio, the National Cybersecurity Agency of France (ANSSI)

Dimitri Havel, Aston Martin Lagonda

Andy Davis, NCC Group

Carsten Maple, University Of Warwick, UK

Timo Van Roermund, NXP Semiconductors

Alessandro Farsaci, CNH Industrial - Iveco Commercial Vehicle

Ian Smith, GSMA

Reda Yaich, IRT SystemX

Johan Lindqvist, Volvo Cars

Christian Wieschebrink, the Federal Office for Information Security (BSI), Germany

Jan Muenther, Here Technologies

Christian Urban-Seelmann, Wabco

Horst Klene, Volkswagen AG

Mouhannad Alattar, Alliance Renault-Nissan-Mitsubishi

Lorenzo Perrozzi, Garrett Advancing Motion

Achim Fahrner, ZF Friedrichshafen AG

Michael Feiri, ZF Friedrichshafen AG

Jan de Meer, Association for Computing Machinery

Eetu Pilli-Sihvola, the Finnish Transport and Communications Agency Traficom

Jacques Kunegel, ACTIA Group

Joachim Lueken, Nokia Bell Labs

Julien Burlet, National Gendarmerie, Ministry of the Interior, France

Thomas Born, Vodafone

LEGAL NOTICE

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 2019/881.
This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

ISBN 978-92-9204-317-9, DOI 10.2824/17802

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report defines good practices for security of smart cars, namely connected and (semi-) autonomous vehicles, providing added-value features in order to enhance car users' experience and improve car safety. Taking stock of all existing standardization, legislative and policy initiatives, this report aims to serve as a reference point to promote cybersecurity for smart cars (connected and automated cars) across Europe and raise awareness on relevant threats and risks with a focus on "cybersecurity for safety".

The automotive industry is undergoing a paradigm change towards connected and autonomous vehicles[1]. Smart cars already available today provide connected, added-value features in order to enhance car users' experience or improve car safety. With this increased connectivity (that the emergence of 5G is expected to further promote) novel cybersecurity risks and threats arise and need to be managed.

It is undeniable that there is a rapid pace when it comes to technological advancements in the area of connected and autonomous cars. With the emergence of semi-autonomous and autonomous cars, which make use of advanced machine learning and artificial intelligence techniques, the potential risks and cybersecurity challenges increase. Moreover, Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) interfaces needed for the deployment of intelligent transport systems and autonomous cars, further exacerbate security risks since they largely expand the potential attack surface and attack vectors.

With the increasing smart cars connectivity and the emergence of (semi)-autonomous cars, novel cybersecurity challenges, risks and threats are arising. Attacks targeting smart cars may lead to vehicle immobilization, road accidents, financial losses, disclosure of sensitive and/or personal data, and even endanger road users' safety. Thus, appropriate security measures need to be implemented to mitigate the potential risks, especially as these attacks threaten the security, safety and even the privacy of vehicle passengers and all other road users, including pedestrians.

It is therefore important to analyse the relevant threats and cybersecurity risks pertaining to smart cars and put forward security measures to address these risks taking into account the particularities of this highly complex, heterogeneous and volatile environment.

Accordingly, this ENISA study provides the following information:

- High level reference model of connected and autonomous vehicles.
- Detailed asset and threat taxonomy for the connected and autonomous vehicles ecosystem.
- Concrete and actionable good practices to improve the cybersecurity posture of connected and autonomous vehicles.
- Mapping to existing legislative, standardization and policy initiatives to foster harmonization.

[1] See JRC 2019 Report 111477, Alonso Raposo M., Grosso, M., Després, J., Fernández Macías, E., Galassi, C., Krasenbrink, A., Krause, J., Levati, L., Mourtzouchou, A., Saveyn, B., Thiel, C. and Ciuffo, B. An analysis of possible socio-economic effects of a Cooperative, Connected and Automated Mobility (CCAM) in Europe. Effects of automated driving on the economy, employment and skills: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC111477/kjna29226enn.pdf

1. INTRODUCTION

Over the last few years, the automotive industry has undergone a paradigm change towards increasingly connected and autonomous cars. Smart cars available today are vehicles equipped with systems providing connected and added-value features in order to enhance car users experience and/or improve car safety. Within the next few years, smart cars' connectivity is expected to expand and smart cars will become connected to other vehicles, pedestrians and their surrounding infrastructure through information exchanges via Vehicle-to-Everything (V2X) communications[2]. Semi-autonomous and autonomous cars (i.e. levels 4 and 5 of autonomy as defined in SAE J3016[3]), which make use of advanced Machine Learning (ML) and Artificial Intelligence (AI) techniques, are also emerging. Indeed, several smart cars stakeholders (including car manufacturers, system suppliers, road operators and other providers) are already carrying out trials of supervised autonomous vehicles, with a driver on board ready to take control of the car if necessary.

In recent years, there has been a growing interest in autonomous cars both from end users and manufacturers and deployment of smart cars has a growing rate in the automotive market[4][5]. According to a survey of 5,500 global city dwellers from all around the world[6], 58% of global respondents are willing to take a ride in a driverless vehicle. Acceptance rates are higher in emerging markets such as China (75%) and India (85%) than in European countries such as United Kingdom (49%) and Germany (44%). However, the European economy is expected to benefit from autonomous vehicles[7], as EU gathers 23% of global motor vehicle production. Moreover, almost 72% of inland freight is transported by road in Europe, and trust in Original Equipment Manufacturers (OEMs) is strong. While optimistic predictions mention that fully automated vehicles could be widely deployed by 2030[8], scientific experts are more cautious and underline that further research is still required to build a fully autonomous vehicle, mostly in the fields of AI and cybersecurity[9].

Cybersecurity is a crucial aspect that will affect the evolution of smart cars. There have already been several research publications on attacks targeting smart cars. One of the most known attacks is the spectacular proof-of-concept remote attack[10] where the researchers took control of a vehicle and sent it off-the-road, thus leading to the recall of over a million cars. Lately, some researchers also demonstrated that it was possible to locally or remotely take control of smart

[2] See EC Communication "On the road to automated mobility: An EU strategy for mobility of the future": https://ec.europa.eu/transport/sites/transport/files/3rd-mobility-pack/com20180283_en.pdf, May 2018

[3] See SAE J3016 "Taxonomy and Definitions for Terms Related to Driving Automations Systems for On-Road Motor Vehicles": http://sae.org/standards/content/J3016_201806/

[4] See JRC 2019 Report 111477, Alonso Raposo M., Grosso, M., Després, J., Fernández Macías, E., Galassi, C., Krasenbrink, A., Krause, J., Levati, L., Mourtzouchou, A., Saveyn, B., Thiel, C. and Ciuffo, B. An analysis of possible socio-economic effects of a Cooperative, Connected and Automated Mobility (CCAM) in Europe. Effects of automated driving on the economy, employment and skills: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC111477/kjna29226enn.pdf

[5] See Autonomous cars: a big opportunity for European industry: https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Autonomous%20cars%20v1.pdf, January 2017

[6] See "Self-Driving Vehicles in an Urban Context": http://www3.weforum.org/docs/WEF_Press%20release.pdf

[7] See European Commission "On the road to automated mobility: An EU strategy for mobility of the future": https://ec.europa.eu/transport/sites/transport/files/3rd-mobility-pack/com20180283_en.pdf

[8] See "Rethinking Transportation 2020-2030 – The disruption of Transportation and the Collapse of the Internal-Combustion Vehicle and Oil Industries": https://static1.squarespace.com/static/585c3439be65942f022bbf9b/t/591a2e4be6f2e1c13df930c5/1494888038959/RethinkX+Report_051517.pdf

[9] See "Self-driving Ubers could still be many years away, says research head": https://nationalpost.com/pmn/news-pmn/canada-news-pmn/self-driving-ubers-could-still-be-many-years-away-says-research-head

[10] See "Hackers remotely kill a Jeep on the highway – with me in it": https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

cars infotainment system[11] by exploiting diagnostic services to manipulate smart cars functions. Moreover, security specialists succeeded to hijack cars using their smart alarm, thereby illegitimately performing actions such as enabling/disabling the immobilizer or cutting the engine[12]. Towards the objective to provide a generic development and evaluation environment for vehicle cybersecurity technologies, an open-source testing platform called PASTA[13] (Portable Automotive Security Testbed with Adaptability) was recently released; it simulates the remote operations of vehicle wheels, brakes, windows, and other features to learn more about the electronic communications features and find vulnerabilities as well as test exploits. However, such a platform may also be used by an attacker, thus facilitating their tasks.

With the increasing smart cars connectivity and the emergence of (semi)-autonomous cars, novel cybersecurity challenges, risks and threats are arising. For instance, there have been some experimental remote attacks[14,15] on autonomous cars' cameras and Light Detection and Ranging (LiDAR) systems showing effective camera blinding, making real objects appear further than their actual locations or even creating fake objects. In addition to malicious sensor manipulations, other attack vectors have been practically demonstrated such as Global Navigation Satellite Systems (GNSS) spoofing[16] and fooling AI-based functions[17] with the famous example of trapping a self-driving car by just drawing a chalk circle around the vehicle. Attacks targeting smart cars may lead to vehicle immobilization, road accidents, financial losses, disclosure of sensitive and/or personal data, and even endanger road users' safety. Thus, appropriate security measures need to be implemented to mitigate the potential risks, especially as these attacks threaten the security, safety and even the privacy of vehicle passengers and all other road users, including pedestrians.

1.1 OBJECTIVES

This ENISA study aims at addressing the security and privacy challenges related to the evolution of smart cars. The main objectives were to collect good practices to ensure the security of smart cars, while mapping the relevant security and privacy challenges, threats, risks and attack scenarios.

More specifically, the aim of this study is to identify the good practices in order to ensure smart cars security against cyber threats, while focusing on V2X communications and (semi-) autonomous cars[18]. Towards this end, the following objectives have been set:

- Analyse smart cars architecture and define a high-level reference model
- Identify smart cars sensitive assets
- Identify potential and main cyber threats, risks and attack scenarios targeting smart cars
- Map identified threats to assets
- Identify relevant security measures based on the threats and assets, and map the identified security measures to the relevant threat(s).

[11] See "Experimental security assessment of BMW cars: A summary report": https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Assessment_of_BMW_Cars_by_KeenLab.pdf

[12] See "Hacking smart car alarm systems": https://www.kaspersky.com/blog/hacking-smart-car-alarm-systems/26014/

[13] See "PASTA: Portable Automotive Security Testbed with Adaptability": https://i.blackhat.com/eu-18/Wed-Dec-5/eu-18-Toyama-PASTA-Portable-Automotive-Security-Testbed-with-Adaptability-wp.pdf

[14] See "Remote attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR": https://pdfs.semanticscholar.org/e06f/ef73f5bad0489bb033f490d41a046f61878a.pdf

[15] See "Self-driving and connected cars: fooling sensors and tracking drivers": https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers.pdf

[16] See "All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems": https://www.usenix.org/node/217477

[17] See "Meet the Artist Using Ritual Magic to Trap Self-Driving Cars": https://www.vice.com/en_us/article/ywwba5/meet-the-artist-using-ritual-magic-to-trap-self-driving-cars

[18] See SAE J3016 "Taxonomy and Definitions for Terms Related to Driving Automations Systems for On-Road Motor Vehicles": http://sae.org/standards/content/J3016_201806/

This ENISA study aims to serve as a reference point to promote collaborative automotive cybersecurity across the European Union and raise awareness of the relevant threats and risks with a focus on “security for safety”.

1.2 SCOPE

This ENISA study outlines good practices for the security of smart cars. It is building on the previous ENISA study on smart cars entitled “*Cyber Security and Resilience of Smart Cars*”[19] and mainly focuses on V2X communications and (semi-)autonomous cars[20] as these technologies were not previously considered.

During this study, ENISA identified available documentation and standards on smart cars cyber security, with a focus on connected and autonomous cars. ENISA also collected inputs from a number of automotive security experts through a structured questionnaire and a series of interviews. Following a thorough analysis of the identified material and the review of security experts feedbacks, ENISA identified the main assets and threats targeting smart cars. Based on these threats, a set of security measures and good practices were defined to ensure smart cars security.

The study highlights three groups of security measures to address security challenges in terms of technologies, policies and processes. A risk-based and holistic approach to security was undertaken. ENISA considered the cybersecurity of smart cars throughout their lifecycle (from conception to end-of-life) and addressed all the essential elements of automotive cybersecurity. Particular attention was paid to the overall supply chain while considering the different stakeholders involved in the smart cars manufacturing (i.e. OEM, software and hardware components providers, etc.).

1.3 EU AND INTERNATIONAL POLICY CONTEXT

The various attacks on smart cars[10,16,17,21,22,23,24] that were publicly reported over the last few years led to a relatively quick awareness of the automotive industry of the security needs and the development of several cybersecurity regulations and initiatives aiming to ensure properly secure vehicles, as presented below.

- **EU Policy**:
  - Early 2014, the Commission's Directorate-General for Mobility and Transport (DG MOVE) set up a C-ITS deployment platform. This latter was conceived as a cooperative framework including national authorities, Cooperative Intelligent Transport Systems (C-ITS) stakeholders and the European Commission with the objective to identify and agree on how to ensure interoperability of C-ITS across borders and along the whole value chain, as well as to identify the most likely and suitable deployment scenario(s).
  - In 2017, the Directorate-General for Internal Market, Industry, Entrepreneurship and Small and Medium-sized Enterprises (SMEs) (DG GROW) launched an initiative on safety regulations with the aim to contribute to a further decrease of the number of road fatalities and injuries considering amendments to the General Safety Regulation and the Pedestrian Safety Regulation.

[19] See ENISA (2016) “Cyber Security and Resilience of smart cars – Good practices and recommendations”: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

[20] See SAE J3016 “Taxonomy and Definitions for Terms Related to Driving Automations Systems for On-Road Motor Vehicles”: http://sae.org/standards/content/J3016_201806/

[21] See “Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR”: https://pdfs.semanticscholar.org/e06f/ef73f5bad0489bb033f490d41a046f61878a.pdf

[22] See “Illusion and Dazzle: Adversarial Optical Channel Exploits against Lidars for Automotive Applications”: https://eprint.iacr.org/2017/613.pdf

[23] See “Fast and Vulnerable: A Story of Telematic Failures”: https://www.usenix.org/system/files/conference/woot15/woot15-paper-foster.pdf

[24] See “Robust Physical-World Attacks on Deep Learning Visual Classification”: https://arxiv.org/pdf/1707.08945.pdf

  - In 2018, the Directorate-General for Communications Networks, Content and Technology (DG CONNECT) launched an initiative on Cooperative, Connected and Automated Mobility (CCAM) with the aim to:
    - provide further guidance on a governance framework for access and sharing of data generated by connected vehicles
    - clarify cybersecurity requirements for the connected car environment
    - provide guidance on the use of pioneer spectrum for 5G connectivity for large scale testing and experimentation for connected vehicles
  - In 2019, the European Commission has set up an informal group of a hundred experts named “the Single Platform for open road testing and pre-deployment of cooperative, connected, automated and autonomous mobility” in order to provide advice and support regarding testing and pre-deployment activities for CCAM[25].
  - The protection of road users’ privacy and personal information is also addressed by the recent EU General Data Protection Regulation (GDPR)[26] which officially went into effect in May 2018.
  - The Network and Information Security directive (NIS)[27] also addresses autonomous vehicles’ cybersecurity issues as it intends to provide generic security measures in order to enhance cybersecurity across EU.

- **International Context**:
  - The European OEMs published a set of cybersecurity principles, through the ACEA Principles of Automobile Cybersecurity[28], which are already implemented by OEM companies.
  - The National Highway Traffic Safety Administration (NHTSA) from the U.S. government issued in late 2016 a document introducing several cybersecurity best practices for smart cars[29].
  - The US Automotive Information Sharing and Analysis Center (Auto-ISAC) has been maintaining since 2016 a series of Automotive Cybersecurity Best Practices[30] which provide guidance on the implementation of automotive cybersecurity principles.
  - Several cybersecurity standards and recommendation documents are also under development. In particular, the United Nations Economic Commission for Europe (UNECE) is currently drafting a proposal for a recommendation on Cyber Security[31] with a focus on key cyber threats and vulnerabilities against vehicles as well as measures to be considered in order to mitigate the identified threats. UNECE is also introducing a United Nations regulation on cybersecurity which defines a set of requirements that shall be fulfilled by vehicle manufacturers, suppliers and service providers, covering the entire vehicle lifecycle (i.e. from the vehicle development to its decommissioning).

[25] See “European Commission Launches CCAM Single Platform”: https://connectedautomateddriving.eu/mediaroom/european-commission-launches-ccam-single-platform/

[26] See EU “General Data Protection Regulation”: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[27] See Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union”: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN

[28] See ACEA “https://www.acea.be/publications/article/acea-principles-of-automobile-cybersecurity”

[29] See NHTSA “Cybesecurity best practices for modern vehicles”: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwji2PqR0cDjAhXq2eAKHcnrAnUQFjAAegQIAxAC&url=https%3A%2F%2Fwww.nhtsa.gov%2Fstaticfiles%2Fnvs%2Fpdf%2F812333_CybersecurityForModernVehicles.pdf&usg=AOvVaw33nVAk2UWXpL3tzDmpRBjl

[30] See Auto-ISAC “Automotive Cybersecurity Best Practices – Executive summary”: https://www.automotiveisac.com/best-practices/

[31] See current draft of the UNECE “Proposal for Recommendation on Cyber Security”: https://www.unece.org/fileadmin/DAM/trans/doc/2019/wp29grva/ECE-TRANS-WP29-GRVA-2019-02e.pdf

- **Standards**:
  - The British Standards Institution (BSI) Group published in December 2018 two Publicly Available Specifications (PAS), namely PAS 1885[32] and PAS 11281[33]. The former, which is entitled "The fundamental principles of automotive cyber security", provides high-level guidance to provide and maintain cybersecurity. As regards to PAS 11281, entitled "Connected automotive ecosystems – Impact of security on safety – Code of practice", it provides recommendations for managing security risks in a connected automotive ecosystem.
  - The European Telecommunications Standards Institute (ETSI) has been developing a set of technical specifications, ETSI TS 102 940 to 102 943 [34], which define an Intelligent Transport System (ITS) security architecture along with services specification to ensure information confidentiality and prevent unauthorized access to ITS services. They also address the trust and privacy management for ITS communications.
  - The standard of Society of Automotive Engineers SAE J3061[35], officially published in January 2016, is considered as the first standard addressing automotive cybersecurity. It provides a set of high-level cybersecurity principles and guidance for cyber-physical vehicle systems.
  - The International Organization for Standardization (ISO) and SAE collaborated to supersede the SAE J3061 recommended practice and propose the ISO/SAE 21434[36]. This standard is also under development and focuses on automotive cybersecurity engineering by specifying requirements and providing recommendations for cybersecurity risk management for cars (including their components, software and interfaces) all along their entire lifecycle. Concurrently, the SAE is working on another document, SAE J3101, which aims to define common requirements for security to be implemented in hardware for ground vehicles.

In 2016, ENISA performed a study on smart cars security issues which resulted in a document entitled "Cyber Security and Resilience of smart cars"[37]. It has also established the Cars and Roads SECurity (CaRSEC) working group which addresses smart cars cybersecurity threats, challenges and solutions so as to protect road users' safety. CaRSEC group members are car manufacturers with focus on cybersecurity, suppliers and developers of embedded hardware/software for smart cars, road authorities and academia, as well as standardisation bodies and policy makers.

1.4 TARGET AUDIENCE

This study provides a set of good practices and security measures to improve smart cars security and mitigate the potential threats and risks. Therefore, similarly to the previous ENISA smart cars study, the target audience of this study is mainly:

- **Car manufacturers**: also referred to as OEMs, they design new cars and handle the assembly of the various car components. In particular, most of the various car components are not produced by the car manufacturer itself, but rather by their suppliers according to a set of functional, safety and security requirements defined by the car manufacturers.

[32] See "PAS 1885:2018 - The fundamental principles of automotive cyber security. Specification": https://shop.bsigroup.com/ProductDetail?pid=000000000030365446

[33] See "PAS 11281:2018 - Connected automotive ecosystems. Impact of security on safety. Code of practice": https://shop.bsigroup.com/ProductDetail?pid=000000000030365540

[34] See ETSI TS 102 940 v1.3.1, "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management"
ETSI TS 102 941 V1.2.1 "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management
ETSI TS 102 942 V1.1.1 "Intelligent Transport Systems (ITS); Security; Access Control"
ETSI TS 102 943 V1.1.1 "Intelligent Transport Systems (ITS); Security; Confidentiality services"

[35] See SAE J3061 "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems": https://www.sae.org/standards/content/j3061_201601/

[36] See ISO/SAE CD 21434 "Road Vehicles – Cybersecurity engineering": https://www.iso.org/standard/70918.html

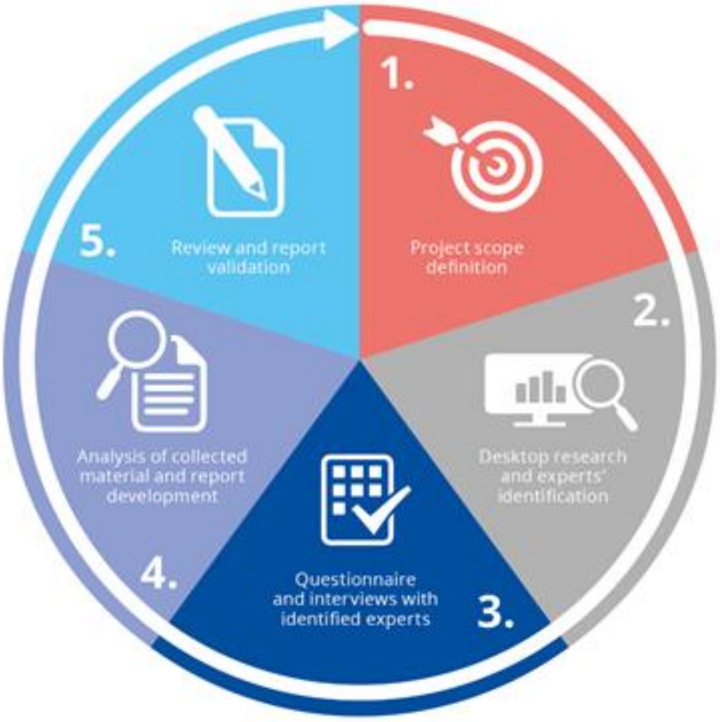
[37] Relation between this study and "Cyber Security and Resilience of Smart Cars" is described in Annex A.

- **Tier 1 and Tier 2 car components suppliers**: provide the different car components required to produce the car. Tier 1 refers to the entities having direct contractual relationships with the car manufacturers, whereas Tier 2 refers to the entities having contractual relationships with Tier 1 suppliers. For instance, car seats are manufactured by Tier 1 suppliers whilst electronic components or software are usually provided by Tier 2 suppliers.
- **Aftermarket suppliers**: provide added-value aftermarket products, such as smart dongles or third-party GNSS systems, which can be bought by customers and connected to the car to provide additional features.

1.5 METHODOLOGY

ENISA has developed this study following a five-step methodological approach as depicted in **Figure 1**.

Figure 1: Methodology


1.
Project scope definition
2.
Desktop research and experts' identification
3.
Questionnaire and interviews with identified experts
4.
Analysis of collected material and report development
5.
Review and report validation

1. **Project scope definition:** the first step consisted in establishing the scope of the project and identifying the main topics to be considered during the study.
2. **Desktop research and experts' identification:** extensive research of relevant documents to gather as much information as possible about (semi-)autonomous cars and V2X communication technologies. The identified documents and standards were used as references for the development of this report. During this step, subject matter experts were also invited to validate scope and provide feedback. Experts from car manufacturers, tier-1 and tier-2 suppliers as well as other organisations, such as Government Authorities and ITS system suppliers were invited. Additionally, experts from ENISA's CaRSEC[38] informal expert group were also invited to contribute.
3. **Questionnaire and interviews with identified experts:** ENISA got in touch with the identified experts in order to get their point of view. To this end, a structured

[38] See https://resilience.enisa.europa.eu/carsec-expert-group for more information on the terms of reference and scope of the ENISA CarSEC Informal Expert Group.

questionnaire covering various security aspects, such as critical assets, key threats targeting smart cars and awareness with respect to smart cars standards and guidelines, was developed. The questionnaire was completed by some of the identified experts, and interviews were conducted to collect additional valuable inputs to prepare the report.

4. **Analysis of collected material and report development:** all the collected information, either through desktop research or directly from the identified experts, was thoroughly analysed. This led to the development of the first draft of this report.
5. **Review and report validation:** ENISA shared the draft of the report with its relevant stakeholder communities and reference groups for review. Taking into account the stakeholders feedbacks, the proposed final version of the report was issued and a validation face-to-face workshop was organized to present the results of the study.

1.6 STRUCTURE OF THE DOCUMENT

The study is structured as follows:

- **Chapter 1 – Introduction:** provides introductory information on the objectives, scope, relevant EU and international policies, target audience, followed methodology and the structure of this study.
- **Chapter 2 – Smart cars: Connected and (semi-)autonomous cars:** first defines V2X communications, semi-autonomous and autonomous cars. Then, it provides a high-level reference architecture of smart cars and lists the sensitive assets to be protected.
- **Chapter 3 – Threats and risk analysis:** identifies the main threats against smart cars and indicates the affected assets. Some examples of significant smart cars attack scenarios are also detailed.
- **Chapter 4 – Security measures and good practices:** describes the security measures and good practices to mitigate the aforementioned attacks.

Further details are provided in the appendix:

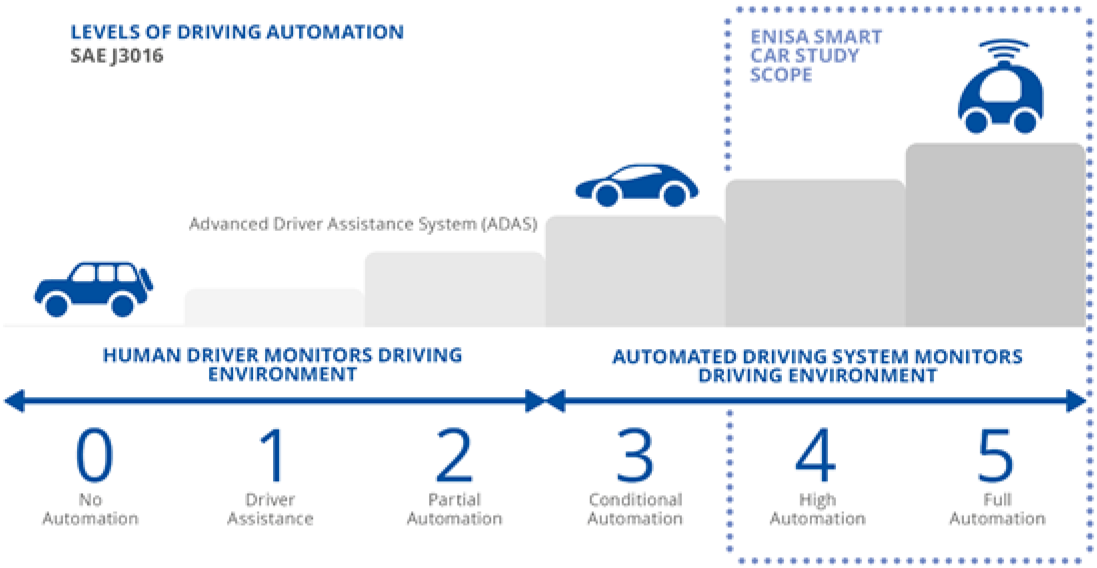
- **Annex A – Asset Taxonomy:** presents the different assets and provides a brief description of them
- **Annex B – Threat Taxonomy:** provides a brief description of the different threats and maps each threat to the asset(s) that may potentially be affected
- **Annex C – Mapping of security measures to threats, standard and good practices:** details the security measures mentioned in chapter 4 and maps them to the corresponding threats.

2. SMART CARS: CONNECTED AND (SEMI-) AUTONOMOUS CARS

2.1 DEFINITIONS

The SAE J3016[39] standard defines six levels of driving automation for on-road vehicles, ranging from level 0 with no driving automation at all to level 5 with full driving automation and no need for a driver, as shown in Figure 2.

Figure 2: SAE vehicles automation levels as defined in SAE J3016


LEVELS OF DRIVING AUTOMATION
SAE J3016
ENISA SMART CAR STUDY SCOPE
Advanced Driver Assistance System (ADAS)
HUMAN DRIVER MONITORS DRIVING ENVIRONMENT
AUTOMATED DRIVING SYSTEM MONITORS DRIVING ENVIRONMENT
0
No Automation
1
Driver Assistance
2
Partial Automation
3
Conditional Automation
4
High Automation
5
Full Automation

Even though the provided recommendations and good practices can apply to all vehicles (i.e. no matter their automation level), this study focuses on **semi-autonomous** and **autonomous cars**, which are also referred to as Automated Driving System-Dedicated Vehicle (ADS-DS) in SAE J3016 standard, as well as on **V2X communications**, defined as follows:

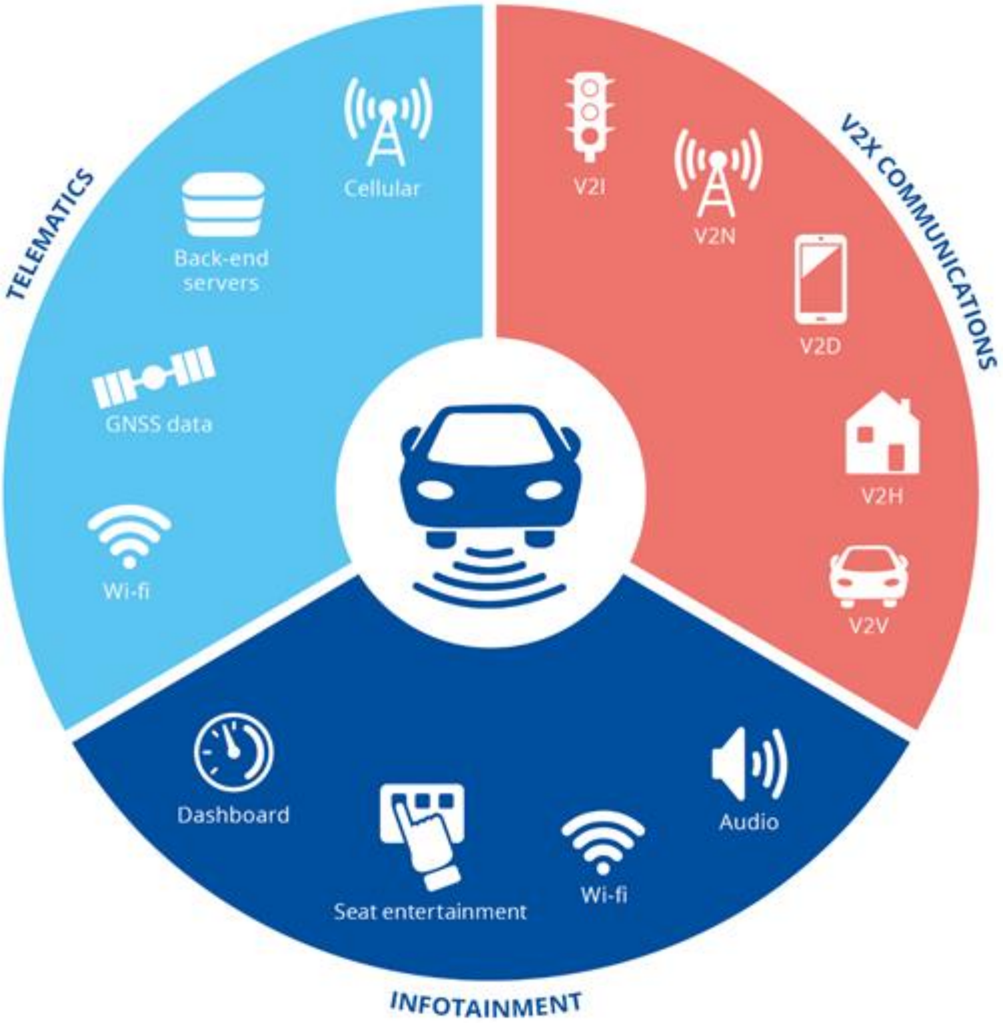
- **Semi-autonomous cars (level 4 of automation):** refers to highly automated cars that are equipped with a multitude of sensors in order to be able to autonomously (i.e. without any human driver intervention) perform **all** driving functions **under certain conditions** (e.g. on a given type of roads).
- **Autonomous cars (level 5 of automation):** refers to fully automated cars that are equipped with a multitude of sensors in order to be able to autonomously perform **all** driving functions **under all conditions** (i.e. at any time and on any road). Those cars may not even include a steering wheel or accelerator/brake pedals.
- **V2X communications:** refers to data exchanges between a vehicle and any other entity (e.g. a road infrastructure, another vehicle, a pedestrian, etc.). It covers the notions of V2V (Vehicle-to-Vehicle) communications and V2I (Vehicle-to-Infrastructure) communications. In this study, the term V2I refers to all communications between the vehicle and its

[39] See SAE J3016 “Taxonomy and Definitions for Terms Related to Driving Automations Systems for On-Road Motor Vehicles”: http://sae.org/standards/content/J3016_201806/

surrounding, aside from V2V communications. Thus, V2I includes V2P (Vehicle-to-Pedestrian) and V2N (Vehicle-to-Network) communications. To enable V2X communications, vehicles are equipped with different wireless communication systems such as Dedicated Short Range Communications (DSRC[40]), Visible Light Communication (VLC), Image Sensor Communication (ISC), Wi-Fi or mobile communication technologies, such as 3G, 4G and 5G. This study is meant to be agnostic about the communication technologies actually used.

Figure 3 gives an overview of the smart car ecosystem depicting systems and application both *in-vehicle [41] and outside the car.*

Figure 3: Smart cars ecosystem



In this study, we focus on smart cars that, as connected systems, have the necessary capabilities to autonomously perform all driving functions under certain (or all) conditions, and are able to communicate with their surroundings including other vehicles, pedestrians and Road-Side Units (RSU).

Good practices discussed in this report do not only concern passenger cars but also commercial vehicles (e.g. buses, coaches, etc.), including self-driving ride-sharing vehicles which can be

[40] In this document, DSRC refers to the standards from the European Committee for Standardization EN 12253:2004 and EN 12795:2002

[41] In-vehicle refers to assets inside the vehicle

shared with other users. This study does not focus on specific use cases such as connected infotainment and specific intra-vehicular communications.

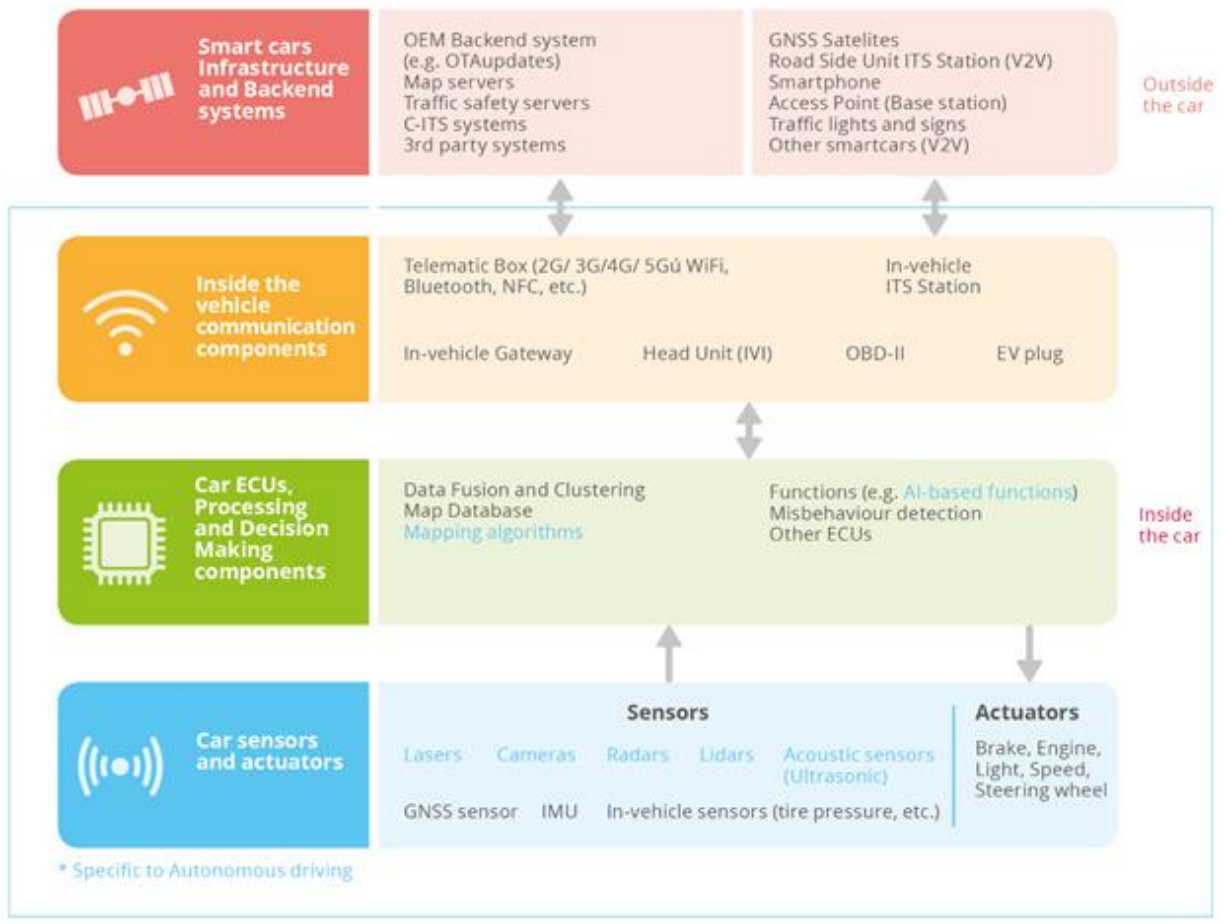
To achieve enhanced autonomous driving capabilities, smart cars rely on various technologies including:

- **Sensors and Actuators:** devices that have various capabilities, such as sensing and detecting objects, actuating, etc.
- **Artificial Intelligence:** algorithms that enable ECUs and computers to perform tasks typically associated with intelligent human beings.
- **Machine Learning:** algorithms that enable computers to act and enhance their ability to predict events or situations.
- **Cloud Computing:** solutions enabling access to shared sets of resources such as servers and applications with minimal requirements concerning managerial effort and service provider interaction.
- **Communications and/or Networks:** radio technologies and communication protocols that allow data exchange between different entities.

2.2 HIGH-LEVEL REFERENCE MODEL

Smart cars and especially (semi-)autonomous cars, which include several ECUs and components, may seem unduly complicated at first glance. Although smart cars functions (e.g. braking, steering, door locking, etc.) are the same throughout vehicles, nevertheless each OEM has its own in-vehicle architecture and there is no common and unique architecture that can be used as a reference model. **Figure 4** presents the high-level functional model that ENISA

Figure 4: High-Level Smart Cars Reference Model


Smart cars infrastructure and Backend systems
OEM Backend system
(e.g. OTAupdates)
Map servers
Traffic safety servers
C-ITS systems
3rd party systems
GNSS Satelites
Road Side Unit ITS Station (V2V)
Smartphone
Access Point (Base station)
Traffic lights and signs
Other smartcars (V2V)
Outside the car
Inside the vehicle communication components
Telematic Box (2G/ 3G/4G/ 5Gú WiFi, Bluetooth, NFC, etc.)
In-vehicle ITS Station
In-vehicle Gateway
Head Unit (IVI)
OBD-II
EV plug
Car ECUs, Processing and Decision Making components
Data Fusion and Clustering
Map Database
Mapping algorithms
Functions (e.g. AI-based functions)
Misbehaviour detection
Other ECUs
Inside the car
Car sensors and actuators
Sensors
Lasers
Cameras
Radars
Lidars
Acoustic sensors (Ultrasonic)
GNSS sensor
IMU
In-vehicle sensors (tire pressure, etc.)
Actuators
Brake, Engine, Light, Speed, Steering wheel
* Specific to Autonomous driving

defined for the study based on an extensive review of relevant efforts and having validated it with the experts. The model's aim is to provide a generic overview of the smart cars technologies and their interplay. It needs to be noted that the model is only indicative and does not reflect the complexity of the various automotive architectures; it aims at encapsulating the main elements of the latter in a high-level view. This model provides a general overview of the different functionalities, used technologies and most important components providing smart cars major features.

The high-level reference model consists of four layers arranged in order, with the three lowest layers being part of the smart car, whereas the upper layer represents components that are outside the actual containment of the car, but which are part of its environment such as RSUs and map servers for instance. In addition to the components and technologies depicted in **Figure 4**, smart cars also include critical functions (e.g. acceleration, braking, object detection, navigation, etc.) that ought to be protected against cyberattacks. Indeed, altering the operations of those functions may lead to unexpected situations (e.g. vehicle collision or crash) that could endanger road users' safety.

Hereinafter, we provide a brief description of the different layers:

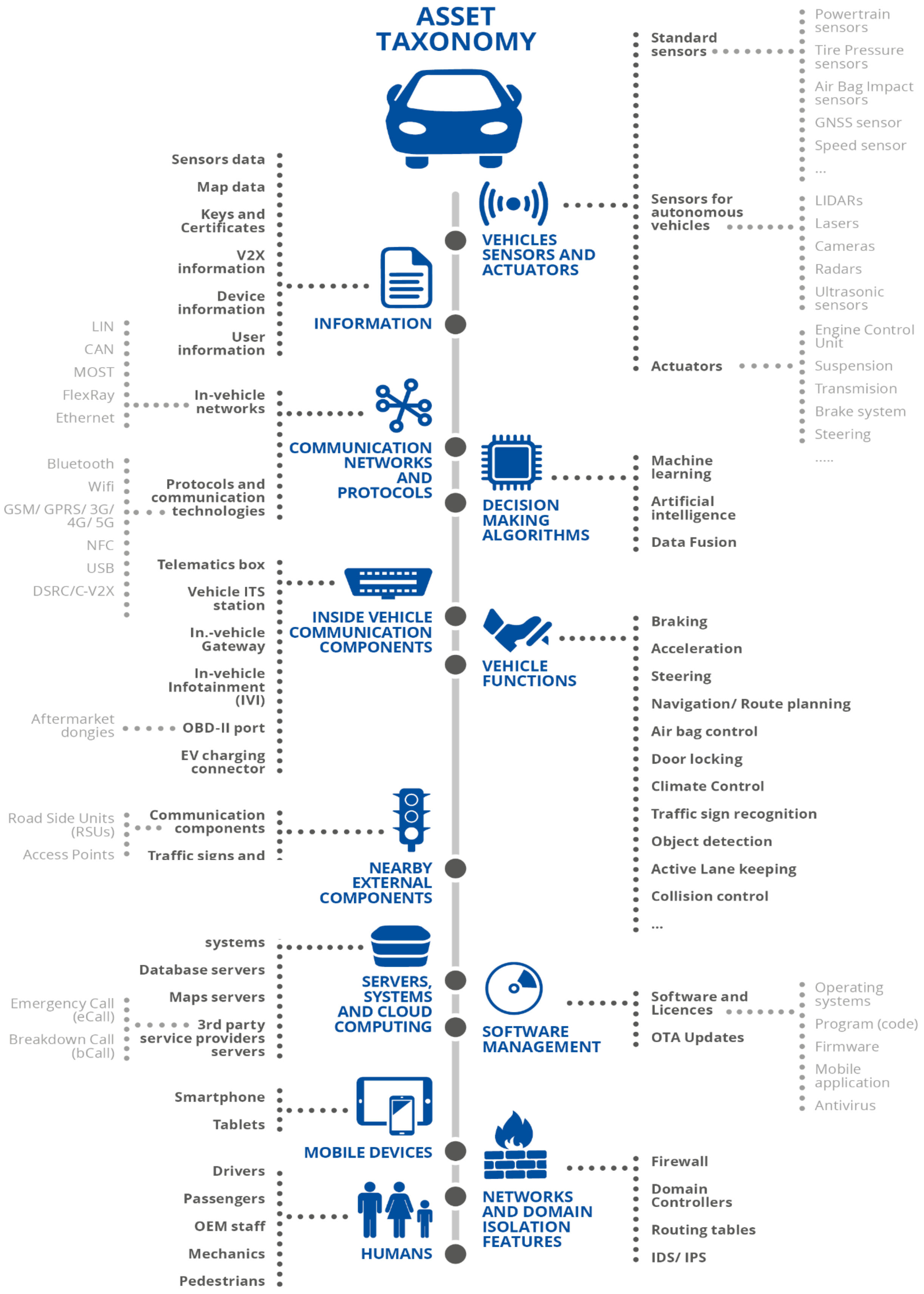
- **Car sensors and actuators:** the lowest layer of the architecture comprises the various smart cars sensors used to monitor the driving environment by collecting data on the vehicle surroundings, such as road conditions, distance to other objects and vehicles, Global Navigation Satellite Systems (GNSS) positions, as well as the different actuators that execute the necessary actions.
- **Car ECUs, processing and decision making components:** this layer comprises all the hardware and software components, including AI, that are used for the processing of the data received from layer Car sensors and actuators (i.e. data collected by the smart cars sensors) and In-vehicle communication components (e.g. data received from other C-ITS stations), as well taking the appropriate decision and transmitting it to the relevant actuator**.**
- **In-vehicle communication components:** this layer includes the different in-vehicle communication components used for both in-vehicle communications (e.g. Head-Unit which is also referred to as In-Vehicle Infotainment (IVI), or in-vehicle gateway) as well as communications with external components such as other vehicles or RSUs.

2.3 SMART CARS INFRASTRUCTURE AND BACKEND SYSTEMS:

This layer comprises the different external communication components (e.g. RSU, traffic signs) or systems (e.g. other vehicles, access points, pedestrian smartphone) that communicate directly with the smart cars, as well as servers and systems that remotely provide services to smart cars. It includes, amongst others, OEM back-end systems used for over-the-air (OTA) updates, map data servers and third party service provider's systems.assets taxonomy.

To address smart cars cybersecurity issues, it is essential to identify assets of such a complex ecosystem. A taxonomy of the key assets that should be protected in order to ensure highly secure vehicles is depicted in **Figure 5**, and a brief description of the different assets is provided in Annex A. Especially, smart cars functions (e.g. obstacle detection) are of utmost importance as they directly influence smart cars behaviours and may endanger passengers' safety. These functions are at the crossroads between different technologies from sensors to AI-based algorithms by way of infrastructure components, listed in the asset taxonomy. This highlights that securing smart cars requires a multidisciplinary approach, as assets domains are quite diversified.

Figure 5: Asset taxonomy



3. THREATS AND ATTACK SCENARIOS

3.1 THREATS TAXONOMY

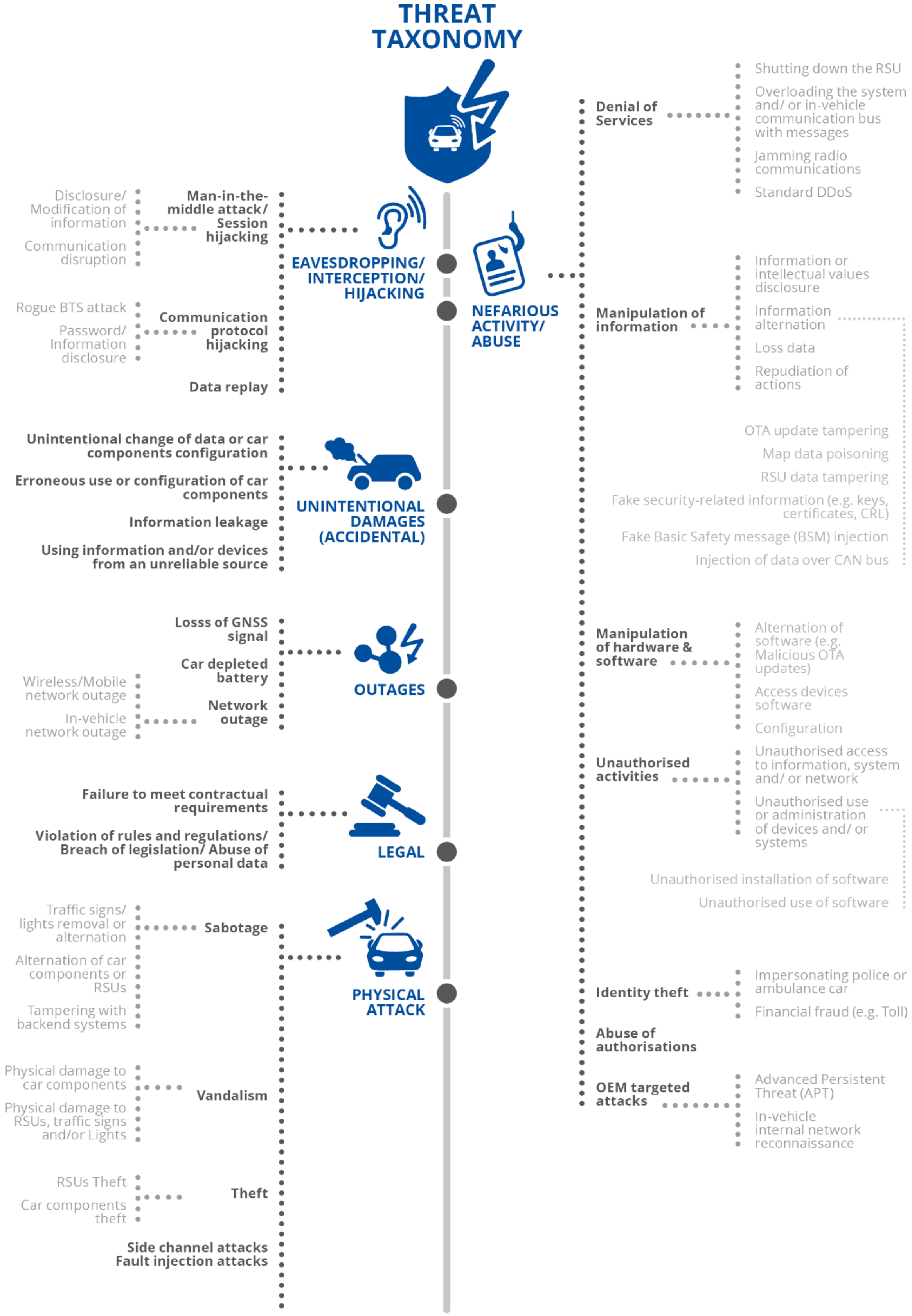
Smart cars increased connectivity and automation expose them to several crucial cyber threats. Those threats may directly target smart cars or their surroundings such as RSUs, traffic signs/lights or even remote servers of the OEM or third-party service providers.

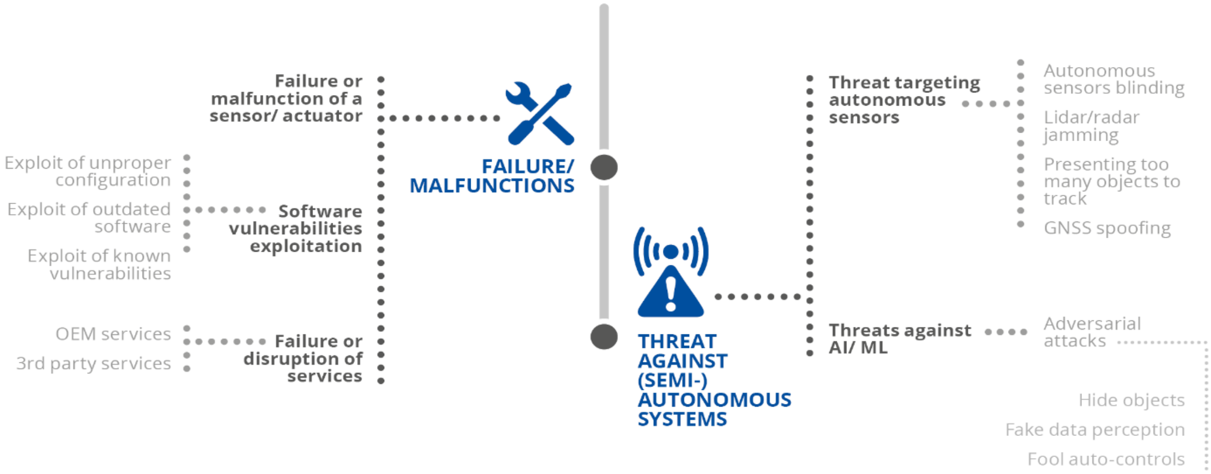
In accordance with the ENISA Threat Taxonomy[42], we have developed a threat taxonomy[43] focused on smart cars as depicted in **Figure 6**. Annex C provides a description of the different threats and identifies the assets that may be affected by each threat.

[42] See "ENISA Threat Taxonomy" (2016): https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view

[43] It is a snapshot of today's threats and may not be up-to-date in the future.

Figure 6: Threat taxonomy


THREAT TAXONOMY
EAVESDROPPING/ INTERCEPTION/ HIJACKING
Man-in-the-middle attack/ Session hijacking
Disclosure/ Modification of information
Communication disruption
Communication protocol hijacking
Rogue BTS attack
Password/ Information disclosure
Data replay
NEFARIOUS ACTIVITY/ ABUSE
Denial of Services
Shutting down the RSU
Overloading the system and/ or in-vehicle communication bus with messages
Jamming radio communications
Standard DDoS
Manipulation of information
Information or intellectual values disclosure
Information alternation
Loss data
Repudiation of actions
OTA update tampering
Map data poisoning
RSU data tampering
Fake security-related information (e.g. keys, certificates, CRL)
Fake Basic Safety message (BSM) injection
Injection of data over CAN bus
Manipulation of hardware & software
Alternation of software (e.g. Malicious OTA updates)
Access devices software
Configuration
Unauthorised activities
Unauthorised access to information, system and/ or network
Unauthorised use or administration of devices and/ or systems
Unauthorised installation of software
Unauthorised use of software
Identity theft
Impersonating police or ambulance car
Financial fraud (e.g. Toll)
Abuse of authorisations
OEM targeted attacks
Advanced Persistent Threat (APT)
In-vehicle internal network reconnaissance
UNINTENTIONAL DAMAGES (ACCIDENTAL)
Unintentional change of data or car components configuration
Erroneous use or configuration of car components
Information leakage
Using information and/or devices from an unreliable source
OUTAGES
Losss of GNSS signal
Car depleted battery
Network outage
Wireless/Mobile network outage
In-vehicle network outage
LEGAL
Failure to meet contractual requirements
Violation of rules and regulations/ Breach of legislation/ Abuse of personal data
PHYSICAL ATTACK
Sabotage
Traffic signs/ lights removal or alternation
Alternation of car components or RSUs
Tampering with backend systems
Vandalism
Physical damage to car components
Physical damage to RSUs, traffic signs and/or Lights
Theft
RSUs Theft
Car components theft
Side channel attacks
Fault injection attacks


Failure or malfunction of a sensor/ actuator
Exploit of unproper configuration
Exploit of outdated software
Exploit of known vulnerabilities
Software vulnerabilities exploitation
OEM services
3rd party services
Failure or disruption of services
FAILURE/ MALFUNCTIONS
THREAT AGAINST (SEMI-) AUTONOMOUS SYSTEMS
Threat targeting autonomous sensors
Autonomous sensors blinding
Lidar/radar jamming
Presenting too many objects to track
GNSS spoofing
Threats against AI/ ML
Adversarial attacks
Hide objects
Fake data perception
Fool auto-controls

3.2 EXAMPLES OF SMART CARS CYBER SECURITY ATTACK SCENARIOS

During the interviews, automotive experts assessed the criticality of several attack scenarios based on their potential impacts and the aforementioned threats, so as to enable the identification of critical attack scenarios. For each attack scenario, experts were asked to indicate whether they consider its potential impact (i.e. severity level) as high, medium or low. Table 1 depicts the different attack scenarios along with the interviewees' perceived severity level.

Table 1: Smart cars attack scenarios

ATTACK SCENARIOS	SEVERITY[44]
1. **Vulnerability exploit in a communication stack**: exploitation of a vulnerability in a communication stack of an in-vehicle network (e.g. no protection mechanism against replay attacks, lack of authentication, etc.) can lead to severe issues such as critical ECU reprogramming and taking control the vehicle over the Controller Area Network (CAN bus).	**High**
2. **Mobile car application[45] being hacked/attacked allowing access to the car**: by hacking the mobile application, an attacker could order a car to drive him somewhere although he is not allowed to do so.	**High**
3. **Attack on remote servers to influence car behaviours**: several attack scenarios exist regarding remote servers. For instance, an attacker could compromise map data with the aim to affect plausibility checks, or even alter data on traffic conditions to change the current car itinerary resulting in an inefficient service.	**High**
4. **Fake communication unit to compromise telematics unit and deploy rogue firmware:** use of malicious communication unit, such as Base Transceiver Station (BTS), Wi-Fi router, RSU, with the objective to spread a malware or just disrupting the infrastructure communications.	**High**
5. **Large scale deployment of rogue firmware after hacking OEM back-end servers:** penetration of OEM back-end servers with the aim to initiate malicious firmware updates could lead to devastating results as this kind of attacks is highly-scalable.	**High**
6. **Hacking an RSU with the aim to spread wrong traffic and safety messages:** as RSUs constitute an important part of the autonomous vehicles' ecosystem, they could be the target of hackers in order to create traffic jams or other kind of disruptions.	**High** – **Medium**
7. **Rogue vehicle sending wrong information through V2V interfaces:** vehicles unknown from the infrastructure (e.g. counterfeit cars) that are deployed to decrease the safety level by sending wrong information about traffic conditions and other functionalities (i.e. fake information with the aim to update map data).	**Medium**

[44] This severity is a global perception of the risk based on interviews. In practice, it varies strongly depending on the actual architecture of each smart car.

[45] Mobile application that provides value added services with respect to the car (e.g. mobile application that enables to unlock the car, start the engine, etc.)

8. **Sensor fooling by adversarial perturbation:** attack scenarios to disrupt the sensors' proper functioning by different means depending on the targeted sensor (e.g. flash the camera, relay the light waves from the LiDAR).	Medium – Low
9. **Communication jamming:** producing radio interferences to disrupt wireless networks so the vehicles cannot emit or receive V2X messages.	Low
10. **GNSS spoofing:** by replacing GNSS signals, an attacker can fool a third-party service into thinking that the vehicle is elsewhere in either time or location. This can lead to accident or vehicle theft.	Medium
11. **Blocking critical messages at automation level 4:** an attacker can block critical messages, such as Denial of a Service (DoS) attack, and prevent the semi-autonomous vehicle (or driver) from reacting appropriately to the situation (e.g. apply the brakes, warn the driver that he needs to take control of the vehicle, etc.).	High

Hereinafter, we detail three types of attack scenarios encompassing various use-cases. The first attack scenario (**Large scale deployment of a rogue firmware after hacking OEM back-end servers**) is typical of the threats lying over connected cars. The second one (**Hacking/altering a V2X mobile application that allows access to the car**) is extracted from V2X use-cases. The third one (**Sensor fooling by adversarial perturbation**) is more related to (semi-)autonomous features. These three attack scenarios were selected so as to represent different families of attacks linked with connected cars and automation levels 4 & 5, which are the focus of this study. The impact is an overall estimation based on the outcome of the interviews.

Attack scenario 1: Large scale deployment of a rogue firmware after hacking OEM back-end servers

DESCRIPTION

This attack scenario refers to deployment of malicious firmware from back-end servers. This could be initiated by OEMs employees (e.g. developers) or by external attackers capable of penetrating back-end servers. Malicious OTA updates could then be executed so that autonomous vehicles think it is a legitimate one, as it is initiated from a trusted server.

IMPACT

High – **Crucial**: Remote servers might communicate with numerous vehicles at the same time. Thus, compromising such a centralised server could affect the entire ecosystem, including passengers' safety.

EASE OF DETECTION	CASCADE EFFECT RISK
Medium: Remote servers should have enough resources to implement advanced monitoring techniques. However, the deployment of many remote servers increases the attack surface to be protected.	High: Such attacks are highly-scalable as they can be executed remotely and affect a fleet of vehicles instantly.

ASSETS AFFECTED	STAKEHOLDERS INVOLVED
Back-end system Software and Licenses OTA Updates Vehicle functions Information (User, Device, Keys and Certificates)	OEMs

ATTACK STEPS

1. To perform this attack scenario, the attacker needs first to penetrate the targeted OEM back-end server. This may be carried out by leveraging a known vulnerability of used software, a misconfiguration on the server side or by spoofing the administrator account for instance.
2. Once the attacker gets access to the OEM back-end server, the attacker can request the execution of an OTA firmware update for a given fleet of vehicles. To this end, he follows the same steps required to perform a legitimate OTA firmware update.
3. Upon receiving the OTA update request, vehicles acknowledge and accept the request as it is initiated by a legitimate OEM server.
4. Next, the attacker uploads a rogue firmware on the OEM back-end server and launches the OTA update process to deploy this firmware.
5. Once the rogue firmware is installed on smart cars, the attacker can take remote control of a fleet of vehicles by exploiting a backdoor introduced in the rogue firmware.

RECOVERY TIME / EFFORT	GAPS AND CHALLENGES
Medium – **High**: Depending on the nature of the deployed firmware, cancelling the update by returning back to the retro version can be challenging if the attacker was able to change update related information (e.g. certificates, policies). Use of logging can help to identify the attack origin.	Lack of awareness and knowledge Lack of a secure boot process Lack of proper product lifecycle management

COUNTERMEASURES

1. Regularly assess the security controls and patch vulnerabilities.
2. Deploy Intrusion Detection Systems (IDS) at vehicle and back-end levels.
3. Introduce a new device or software change into the vehicle only according to an established, accepted and communicated change management process.
4. Consider establishing a CSIRT.
5. Apply security controls at back-end servers.
6. Establish an incident handling process.
7. Incident report to back-end servers.
8. Conduct periodic reviews, of authorization and access control privileges for instance.
9. Software authenticity and integrity checked before installation.
10. Use of secure OTA firmware updates.

11. Protect OTA update process.
12. Use of secure boot mechanisms.
13. Application of security controls to back-end servers.
14. Apply least privileges principle and use individual accounts to access devices and systems.
15. Maintain properly protected audit logs.
16. Allow and encourage the use of strong authentication mechanisms.

Attack scenario 2: Hacking/altering a V2X mobile application that allows access to the car

DESCRIPTION	
IMPACT	
High: Such attacks can result in illegitimate access to the smart car or even its theft through the compromise or hacking of a V2X mobile application.	
EASE OF DETECTION	**CASCADE EFFECT RISK**
Medium: Individual should pay attention to the different applications installed on their smartphone (e.g. avoid installing suspicious applications).	Medium: This attack scenario target individuals and allows compromising many vehicles at once using V2X application
ASSETS AFFECTED	**STAKEHOLDERS INVOLVED**
Mobile application User information Keys and certificates Mobile devices (smartphones and Tablets)	OEMs Third-party service providers
ATTACK STEPS (SAMPLE BASED ON A REAL-CASE ATTACK SCENARIO)	
1. The attacker manages to retrieve user's credentials associated to a V2X application (e.g. car, traffic or platooning application) by one of the following means: by making the honest user install a fake application instead of the real one, via a phishing attack, or by leveraging an existing or a new discovered vulnerability in the V2X application. 2. Once the attacker has retrieved the user's credentials, he installs the legitimate V2X application and uses stolen credentials to login successfully; thus impersonating the honest user. 3. Finally, the attacker can use the V2X application to get access to the smart car, and potentially steal the smart car if keyless driving is allowed and the hacked application enables to start the engine.	
RECOVERY TIME / EFFORT	**GAPS AND CHALLENGES**

Medium: As soon as the flaw in the application that allow such attacks is discovered, a security patch should be applied. Depending on the vulnerability, it might take days or weeks. If V2X application user has informed OEM about credential compromise, they should revoke the disclosed credentials for that particular user.	Response to zero-day vulnerabilities Lack of awareness and knowledge Insecure design or development
COUNTERMEASURES	
1. Perform vulnerability surveys. 2. Third party testing of V2X applications. 3. Regularly assess the security controls and patch vulnerabilities. 4. Information sharing between different actors. 5. Adopt a holistic approach to security training and awareness among the employees. 6. Raise users' awareness. 7. Allow and encourage the use of strong authentication (e.g. multi-factor authentication). 8. Consider establishing a Computer Security Incident Response Teams (CSIRT). 9. Mitigate vulnerabilities or limitations of software libraries. 10. Protect mobile applications against reverse engineering and tampering of their binary code. 11. Securely store sensitive data on mobile devices.	

Attack scenario 3: Sensor fooling by adversarial perturbation

DESCRIPTION	
IMPACT	
High: The impact depends on the introduced perturbation. However, abusive detection, or lack of detection of stop signs could entail major accidents endangering road users' safety and leading to driver, passenger, or pedestrian deaths.	
EASE OF DETECTION	**CASCADE EFFECT RISK**
Medium: Without appropriate countermeasure, the modifications brought to the signs could be undetected by human eyes before an accident occurs.	Low: The perturbation is local, and may affect only the cars passing by the modified or spoofed sign.
ASSETS AFFECTED	**STAKEHOLDERS INVOLVED**
Decision Making algorithms Sensors for autonomous vehicles Vehicle functions	OEMs Road infrastructure

ATTACK STEPS (SAMPLE BASED ON A REAL-CASE ATTACK SCENARIO)

1. The attacker first analyses the capabilities of the targeted versions of cameras and AI-based image classifier to ensure detection and classification as desired of the modified sign. This setup phase can require trying multiple perturbation patterns or display parameters. The attacker needs to perform some experimentation as well, to test the adversarial perturbation and ensure that his attack will succeed.
2. At a next step, the attacker attaches a set of black and white stickers[46] to a physical road sign to cause misclassification of the traffic sign.
3. Due to the added stickers, the cars passing by the altered traffic sign will erroneously classify it into the attacker's targeted class (e.g. interpret a stop sign as a speed limit sign) and react accordingly (e.g. reduce speed instead of stopping the vehicle).

RECOVERY TIME / EFFORT	GAPS AND CHALLENGES
Medium: Sensor fooling attacks can go unnoticed. Once detected, modified traffic signs can be repaired in hours.	Traffic sign authentication would be an appropriate countermeasure but is complicated to deploy Collaboration of vehicles

COUNTERMEASURES

1. Protect critical sensors in order to prevent attacks that may alter their perception of the environment.
2. Hardening against Adversarial Machine Learning.
3. Use of hardware redundancy mechanisms.
4. Use of data redundancy mechanisms, such as sensors information fusion.
5. Perform data validation, for instance by comparing sign information collected by sensor with information from digital maps stored in the vehicle.

[46] "Robust Physical-World Attacks on Deep Learning Models": https://arxiv.org/pdf/1707.08945.pdf

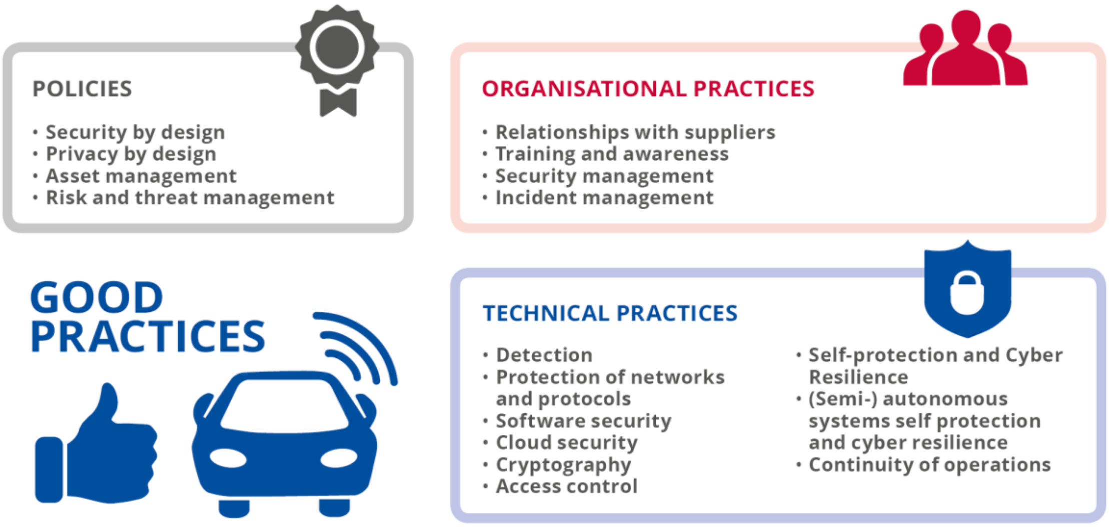
4. SECURITY MEASURES AND GOOD PRACTICES

4.1 SECURITY MEASURES CATEGORISATION

Security measures and good practices development is one of the major objectives of this study. Indeed, a considerable effort was expended to identify all relevant security measures in order to help mitigate the potential threats and risks, thus improving smart cars security.

The list of security measures has been established by analysing relevant documents and standards identified during desktop research[47]. This analysis allowed the identification of frequently mentioned topics regarding smart cars security and their classifications into different security domains. The resulting list consists of seventeen security domains grouped into three main categories, namely Policies, Organisational practices and Technical practices as shown in **Figure 7**. The latter provides a comprehensive view of smart cars security landscape, and points out the areas to be protected.

Figure 7: Cybersecurity Good Practices Overview



POLICIES

- Security by design
- Privacy by design
- Asset management
- Risk and threat management

ORGANISATIONAL PRACTICES

- Relationships with suppliers
- Training and awareness
- Security management
- Incident management

GOOD PRACTICES

TECHNICAL PRACTICES

- Detection
- Protection of networks and protocols
- Software security
- Cloud security
- Cryptography
- Access control
- Self-protection and Cyber Resilience
- (Semi-) autonomous systems self protection and cyber resilience
- Continuity of operations

[47] The data collection was performed between March and July 2019. Updates may have impacted the reference documents since the publication of this report. See Bibliography in chapter 6.

4.2 POLICIES

This first category of security measures encompasses the different policies and procedures to be established within organizations to ensure an appropriate cybersecurity level.

Policies-related security measures cover both security and privacy aspects, and have been classified into four main security domains, namely **Security by design**, **Privacy by design**, **Asset management** and **Risk and threat management**.

The security measures in this section are addressed at both OEMs and suppliers, due to the tight links between them.

4.2.1 Security by design

These security measures emphasize the need to consider security aspects from the very beginning of product development, throughout the supply chain and all over smart cars lifecycle.

- **PS-01**: Adopt a security by design approach where smart cars cybersecurity is considered from both the vehicles as well as the infrastructure perspective.
- **PS-02**: Address security in each relevant specification document to ensure that security aspects are considered from the very beginning of the concept phase, and not as an afterthought.
- **PS-03**: Promote the use of methodologies that consider security in every stage of the development phase and operations phases (e.g. DevSecOps[48], Secure Development Lifecycle (SDL)[49], etc.).
- **PS-04**: Consider including a security role within the product engineering team to lead security related tasks.

4.2.2 Privacy by design

This security domain includes a set of security measures related to the protection of private data that are collected, processed and/or stored by smart cars stakeholders.

- **PS-05**: Consider applying local and international privacy related regulations, such as the GDPR, to prevent privacy issues.
- **PS-06**: Conduct Privacy Impact Assessments (PIA), taken into account the context of use, in order to identify any privacy related risk, and define appropriate countermeasures to mitigate it.
- **PS-07**: Perform Privacy Audits during smart cars development and over back-end systems on a regular basis, e.g. at least once year, in order to ensure compliance with privacy related policies.

4.2.3 Asset Management

Hereinafter, security measures pertaining to assets discovery, monitoring, administration and maintenance are outlined.

- **PS-08**: Use tools supporting asset management that can automatically discover, identify and enumerate assets specific to the organization and smart cars ecosystem.
- **PS-09**: Ensure that the organization maintains a consistent and up-to-date asset inventory.

[48] DevSecOps is short for Development, Security and Operations. It aims to implement security decisions and actions at the same scale and speed as development and operations decisions and actions. See https://www.forcepoint.com/cyber-edu/devsecops

[49] See SAE J3061 "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems": https://www.sae.org/standards/content/j3061_201601/

- **PS-10**: Introduce a new device or software change into the vehicle only according to an established, accepted and communicated change management process.

4.2.4 Risk and Threat Management

This security domain gathers the security measures related to the process of risk and threat management.

- **PS-11**: Adopt an approach to risk management dedicated and suitable for automotive sector, considering emerging threats and attack scenarios targeting smart cars.
- **PS-12**: Perform a cybersecurity risk analysis from the very early stages of the design process, and which should be revised at least annually and upon any major change or in case of critical security vulnerability detection or critical security incident.
- **PS-13**: Monitor security vulnerabilities with a focus on vehicles that are on the market on a regular basis, e.g. every 6 months or more frequently based on risk assessment.
- **PS-14**: Conduct security evaluations, such as penetration testing, during the development phase and then, on a regular basis following an event driven approach, e.g. in the case of new threats or vulnerabilities and after major updates.
- **PS-15**: Consider establishing a threat intelligence process in order to be informed on emerging attack types and sources as well as new relevant vulnerabilities.
- **PS-16**: Regularly assess the security controls at least once a year overall smart cars lifecycle, and deploy patches (after testing them) to mitigate vulnerabilities.
- **PS-17**: Regularly check, at least every six months over smart cars lifecycle, that the security assumptions (e.g. operational environment assumptions) are still valid. In particular, consider defining procedure for communication and handling of end-of-life/out-of-warranty status for cybersecurity.

4.3 ORGANISATIONAL PRACTICES

Organisational and governance processes are of utmost importance to ensure smart cars security. In what follows, a set of organisational rules and best practices are detailed. They cover several aspects such as relationships with suppliers, employees training, incident management, etc.

4.3.1 Relationships with Suppliers

- **OP-01**: Foster security-related information sharing between the different stakeholders while protecting intellectual property.
- **OP-02**: Define cybersecurity relevant aspects of the partnerships along the supply chain, and develop security requirements and procurement guidelines for suppliers[50].

4.3.2 Training and Awareness

- **OP-03**: Share relevant information between all organisations, including subcontractors, suppliers and third parties to enhance smart cars security, by following the examples of existing Information Sharing and Analysis Centers (ISACs) for instance.
- **OP-04**: Adopt a holistic approach to security training and awareness among the employees, including employees on all levels of the organization, as well as consider expanding it to suppliers.
- **OP-05**: Ensure that security trainings are continuous, regular and frequently updated.

[50] The current draft of the ISO/SAE 21434 standard provide a Development Interface Agreement (DIA) template example where for each work product, one can clearly mark each organisation as either responsible, approver, support, inform or consult.

- **OP-06**: Raise vehicle owners', drivers' and passengers' awareness with respect to security issues and how to prevent them, on a regular basis.

4.3.3 Security Management

- **OP-07**: Consider establishing an OEM Security Operations Center (SOC) with clearly defined roles, responsibilities and cybersecurity competences to centralize knowledge on cybersecurity, monitor and anticipate potential threats.
- **OP-08**: Designate one or several[51] dedicated security team(s) with security specialists having diversified and broad range of competencies in security related topics (e.g. risk assessment, penetration testing, secure design, etc.).
- **OP-09**: Define a dedicated Information Security Management System (ISMS)[52] that covers smart cars entire lifecycle.
- **OP-10**: Consider defining an internal task force, which involves board-level management, to guide security-related strategic decisions and facilitate accountability.

4.3.4 Incident Management

- **OP-11**: OEMs and 3rd party suppliers should establish an incident handling process that should be tested and revised at least annually and as soon as possible in the case of a major change.
- **OP-12**: OEMs and 3rd party suppliers should consider establishing a Product Security Incident Response Team (PSIRT) and Computer Security Incident Response Team (CSIRT)[53]. Each team would be dedicated to handling security incidents respectively related to Products and Infrastructure and work along with the SOC if there is one.
- **OP-13**: Report incidents to back-end servers to ensure that systems are secure over their lifetime.
- **OP-14**: Define and classify relevant cybersecurity incidents to enable the identification of the most critical incidents and their prioritization, based on their potential impacts or broader effect for instance.
- **OP-15**: Consider establishing a secure and reliable process for detecting and handling misbehaving ITS stations, e.g. revoke credentials of misbehaving ITS stations.

4.4 TECHNICAL PRACTICES

Besides to the policies and organisational practices listed above, a set of technical security measures should be implemented to protect both smart cars and the associated back-end systems. Hereinafter, we provide an overview of these technical practices which covers several aspects such as software security, cloud security, detection, access control and so on.

4.4.1 Detection

- **TM-01**: Deploy Intrusion Detection Systems (IDSs) both at vehicle and back-end levels to enable the detection of malicious activities or policy violations.
- **TM-02**: Maintain properly protected audit logs to prevent their disclosure to unauthorised entities, while clearly defining their storage location and retaining period.

[51] For large organisations, it may be considered to build several security teams to split the scope, for instance, by separating corporate security policy, back-end systems and connectivity services, cars and embedded components security.

[52] "An ISMS consists of the policies, procedures, guidelines and associated resources and activities, collectively managed by an organisation, in the pursuit of protecting its information assets." See ISO 27000: https://www.iso.org/fr/standard/73906.html

[53] See for instance https://www.first.org/

- **TM-03**: Consider periodically reviewing network logs, access control privileges and assets configuration.
- **TM-04**: Perform data validation to check the correctness of incoming information.
- **TM-05**: Define appropriate forensics procedures to enable event reconstruction, facilitate crash investigation, prevent similar attacks and/or for accountability purposes.

4.4.2 Protection of Networks and Protocols

- **TM-06**: Protect remote monitoring and administration interfaces through mutual authentication and access control mechanisms to prevent illegitimate access to smart cars systems.
- **TM-07**: Protect the integrity and authenticity of all critical in-vehicle internal communications.
- **TM-08**: Protect the integrity and authenticity of all external communications between the smart cars and all the different entities it is interacting with.
- **TM-09**: Enforce session management policies for the different communication sessions (e.g. administration,) to avoid session hijacking.
- **TM-10**: Timestamp all exchanged messages using reliable time sources (e.g. provided by secure embedded component or coming from satellite system) to mitigate replay attacks.
- **TM-11**: Manage radio frequencies and the frequency of beaconing[54] and other repeated messages in order to prevent Distributed DoS (DDoS) attacks.
- **TM-12**: Implement frequency agility feature to prevent signals jamming, if applicable.
- **TM-13**: Perform packet filtering at the different layers (e.g. ECU and sensors, mobile network communications, etc.) to analyse incoming and outgoing packets and discard illegitimate traffic.
- **TM-14**: Provide end-to-end protection of sensitive data in terms of confidentiality and integrity using secure protocols.

4.4.3 Software Security

- **TM-15**: Secure the default configuration of devices and services and ensure that the most secure operation mode of device (or service) is used by default.
- **TM-16**: Ensure software authenticity and integrity before its installation, to ensure that only legitimate software is used.
- **TM-17**: Implement and document changes in configuration according to a change management policy developed by the organisation based on risk analysis.
- **TM-18**: Secure OTA firmware updates to avoid firmware manipulation, disclosure or rollback to vulnerable versions.[55]
- **TM-19**: Define a secure OTA update process.
- **TM-20**: Implement secure boot processes that ensure systems integrity and authenticity. A risk-based approach may be used to identify when secure boot is actually needed.
- **TM-21**: Ensure that vulnerabilities and limitations of software dependencies, especially open source libraries, are mitigated or addressed in a risk assessment.
- **TM-22**: Protect mobile applications against reverse engineering (e.g. through code obfuscation techniques) and against tampering of their binary code (e.g. by signing it).
- **TM-23**: Securely store sensitive data (e.g. passwords) on mobile devices, and protect local files created by the mobile application.

[54] Beacons are messages exchanged periodically over vehicular networks to carry information such as location, heading, and speed.

[55] An example of secure OTA firmware update guidelines can be found in the Uptane project documentation https://uptane.github.io/uptane-standard/uptane-standard.html

4.4.4 Cloud Security

- **TM-24**: Cover security and availability aspects in agreements with cloud security providers, if applicable.
- **TM-25**: In the context of cloud-based application and centralised systems, ensure that single points of failure are prevented.
- **TM-26**: Operate critical systems and applications within the private[56] or at least hybrid[57] deployment models.
- **TM-27**: Protect all data within the cloud and during transfer while ensuring that cloud services providers do not have access to the decryption keys, so as to mitigate any potential risk stemming from cloud attacks.

4.4.5 Cryptography

- **TM-28**: Encrypt all sensitive, personal and private data to prevent its disclosure to illegitimate entities. Moreover, authenticated encryption may be used to avoid the manipulation of personal data while ensuring their confidentiality.
- **TM-29**: Use well-known and standardized cryptographic schemes and protocols that are widely considered as secure, and avoid the use of proprietary schemes.
- **TM-30**: Use of storage encryption to protect both users' data as well as data needed to enforce smart cars security (e.g. used keys, security credentials, etc.).
- **TM-31**: Implement a secure key management process. The process should cover all the steps of key lifecycle: key length choice in relation with key lifetime, key generation using an appropriate level of entropy from a reliable source, secure key storage, key rotation and revocation, etc.
- **TM-32**: Consider the use of dedicated and tamper resistant hardware security modules for secure execution of cryptographic algorithms and secure key storage.

4.4.6 Access Control

- **TM-33**: Apply security controls at back-end servers; covering policies, physical and logical security aspects as well as the security of internal networks and data.
- **TM-34**: Apply least privileges principle and use individual accounts to access devices and/or systems.
- **TM-35**: Segregate remote access by developing a set of rules for the control and monitoring of remote communications.
- **TM-36**: Allow and encourage the use of strong authentication mechanisms, e.g. Multi-Factor Authentication (MFA), define an account lockout functionality, etc.

4.4.7 Self-Protection and Cyber Resilience

- **TM-37**: Implement differential monitoring on the GNSS system, to ensure accurate localisation data.
- **TM-38**: Apply a hardening approach on the different level (i.e. devices, network, back-end, etc.) to reduce the attack surface.

[56] A private cloud refers to a cloud environment that is operated exclusively for a single organization.
[57] A hybrid cloud combines both private and public cloud that are bound together for better cost-effectiveness and to provide more flexibility and control.

- **TM-39**: Reinforce interfaces robustness, e.g. to cope with buffer overflows or fuzzing.
- **TM-40**: Consider strengthening applications isolation at runtime, using trusted software technologies.
- **TM-41**: Apply system, sub-domain and network segregation using physical and logical isolation techniques where appropriate (based on risk assessment).

4.4.8 (Semi-) Autonomous Systems Self Protection and Cyber Resilience

- **TM-42**: Consider using inboard Inertial Navigation System (INS) or existing dead-reckoning methods to get localisation data, even in case of GNSS failure.
- **TM-43**: Protect critical autonomous sensors to prevent the different attacks aiming to alter smart cars environment perception.
- **TM-44**: Harden against Adversarial attacks, to prevent AI and ML components from being tricked.
- **TM-45**: Prevent data falsification or manipulation in regard to AI and ML.
- **TM-46**: Use of data redundancy mechanisms (e.g. sensor data fusion) that correlate data acquired from the different sensors in the vehicle and data obtained via V2X communications before making a decision.
- **TM-47**: Use of hardware redundancy mechanisms by adding extra hardware components able to carry out the required operations and perform self-driving tasks.

4.4.9 Continuity of Operations

- **TM-48**: Ensure that notifications are easy to understand, and help users find a remediation or workaround.
- **TM-49**: Create a Business Continuity Plan (BCP) and a Business Recovery Plan (BRP) that cover third-party aspects and are periodically tested, at least annually, to ensure the resilience of smart cars systems.
- **TM-50**: Define important parameters for the business continuity of the organisation, e.g. Recovery Time Objective (RTO), Maximum Tolerable Outage (MTO), etc.

5. ABBREVIATIONS

ACRONYM	DEFINITION
ADS-DV	Automated Driving System-Dedicated Vehicle
AI	Artificial Intelligence
AP	Access Point
Auto-ISAC	Automotive Information Sharing and Analysis Center
BSI	British Standards Institution
BSM	Basic Safety Message
BTS	Base Transceiver Station
CaRSEC	Cars and Roads SECurity working group
CCAM	Cooperative, Connected and Automated Mobility
CSIRT	Computer Security Incident Response Team
C-ITS	Cooperative Intelligent Transport Systems
DG CONNECT	Directorate-General for Communications Networks, Content and Technology
DG GROW	Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
DG MOVE	Directorate-General for Mobility and Transport
DSRC[58]	Dedicated Short-Range Communications
ECU	Electronic control Unit
E/E	Electrical and Electronic
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite System

[58] In this document, DSRC refers to the standards from the European Committee for Standardization EN 12253:2004 and EN 12795:2002

IDS	Intrusion Detection System
ICE	In Car Entertainment
IMU	Inertial Measurement Unit
IPS	Intrusion Prevention System
ISC	Image Sensor Communication
ISO	International Organization for Standardization
IT	Information Technology
ITS	Intelligent Transportation System
IVI	In-Vehicle Infotainment
LiDAR	Light Detection and Ranging
LIN	Local Interconnect Network
MFA	Multi-Factor Authentication
MITM	Man-In-The-Middle
ML	Machine Learning
MOST	Media Oriented Systems Transport
NFC	Near-Field Communication
NHTSA	National Highway Traffic Safety Administration
NIS	Network and Information Security directive
OBD	On-Board Diagnostic
OEM	Original Equipment Manufacturer
OS	Operation System
OTA	Over-The-Air
OT	Operational Technology
PAS	Publicly Available Specifications
PIA	Privacy Impact Assessment
RSE	Road Side Equipment

RSU	Road-Side Unit
SAE	Society of Automotive Engineers
SME	Small-Medium Enterprises
SOC	Security Operation Center
TCU	Telematic Control Unit
UNECE	United Nations Economic Commission for Europe
UTC	Universal Coordinated Time
V2I	Vehicle-to-Infrastructure
V2N	Vehicle-to-Network
V2P	Vehicle-to-Pedestrian
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything. Includes the notion of V2V, V2I, V2P and V2N communications
VLC	Visible Light Communication

6. BIBLIOGRAPHY/REFERENCES

SAE J3016 “Taxonomy and Definitions for Terms Related to Driving Automations Systems for On-Road Motor Vehicles”: http://sae.org/standards/content/J3016_201806/

ENISA (2016) “Cyber Security and Resilience of smart cars – Good practices and recommendations”: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

“Self-Driving Vehicles in an Urban Context”: http://www3.weforum.org/docs/WEF_Press%20release.pdf

European Commission “On the road to automated mobility: An EU strategy for mobility of the future”: https://ec.europa.eu/transport/sites/transport/files/3rd-mobility-pack/com20180283_en.pdf

“Rethinking Transportation 2020-2030 – The disruption of Transportation and the Collapse of the Internal-Combustion Vehicle and Oil Industries”: https://static1.squarespace.com/static/585c3439be65942f022bbf9b/t/591a2e4be6f2e1c13df930c5/1494888038959/RethinkX+Report_051517.pdf

“Self-driving Ubers could still be many years away, says research head”: https://nationalpost.com/pmn/news-pmn/canada-news-pmn/self-driving-ubers-could-still-be-many-years-away-says-research-head

“Hackers remotely kill a Jeep on the highway – with me in it”: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

“Experimental security assessment of BMW cars: A summary report”: https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Assessment_of_BMW_Cars_by_KeenLab.pdf

“Hacking smart car alarm systems”: https://www.kaspersky.com/blog/hacking-smart-car-alarm-systems/26014/

“PASTA: Portable Automotive Security Testbed with Adaptability”: https://i.blackhat.com/eu-18/Wed-Dec-5/eu-18-Toyama-PASTA-Portable-Automotive-Security-Testbed-with-Adaptability-wp.pdf

“PASTA 1.0 L and F Software Development Tools – Product details”: https://www.chip1stop.com/USA/en/view/dispDetail/DispDetail?partId=LANF-0000001

“Remote attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR”: https://pdfs.semanticscholar.org/e06f/ef73f5bad0489bb033f490d41a046f61878a.pdf

“Self-driving and connected cars: fooling sensors and tracking drivers”: https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers.pdf

“All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems”: https://www.usenix.org/node/217477

“Meet the Artist Using Ritual Magic to Trap Self-Driving Cars”: https://www.vice.com/en_us/article/ywwba5/meet-the-artist-using-ritual-magic-to-trap-self-driving-cars

“Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR”: https://pdfs.semanticscholar.org/e06f/ef73f5bad0489bb033f490d41a046f61878a.pdf

“Illusion and Dazzle: Adversarial Optical Channel Exploits against LiDARs for Automotive Applications”: https://eprint.iacr.org/2017/613.pdf

“Fast and Vulnerable: A Story of Telematic Failures”: https://www.usenix.org/system/files/conference/woot15/woot15-paper-foster.pdf

“Robust Physical-World Attacks on Deep Learning Visual Classification”: https://arxiv.org/pdf/1707.08945.pdf

“European Commission Launches CCAM Single Platform”: https://connectedautomateddriving.eu/mediaroom/european-commission-launches-ccam-single-platform/

EU “General Data Protection Regulation”: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union”: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN

Cybersecurity Best Practices for Modern Vehicles – NHTSA : https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf

Auto-ISAC “Automotive Cybersecurity Best Practices – Executive summary”: https://www.automotiveisac.com/best-practices/

UNECE “Proposal for Recommendation on Cyber Security”: https://www.unece.org/fileadmin/DAM/trans/doc/2019/wp29grva/ECE-TRANS-WP29-GRVA-2019-02e.pdf

“PAS 1885:2018 - The fundamental principles of automotive cyber security. Specification”: https://shop.bsigroup.com/ProductDetail?pid=000000000030365446

“PAS 11281:2018 - Connected automotive ecosystems. Impact of security on safety. Code of practice”: https://shop.bsigroup.com/ProductDetail?pid=000000000030365540

ETSI TS 102 940 v1.3.1, “Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management”: https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.03.01_60/ts_102940v010301p.pdf

ETSI TS 102 941 V1.2.1 “Intelligent Transport Systems (ITS); Security; Trust and Privacy Management https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.02.01_60/ts_102941v010201p.pdf

ETSI TS 102 942 V1.1.1 “Intelligent Transport Systems (ITS); Security; Access Control” https://www.etsi.org/deliver/etsi_ts/102900_102999/102942/01.01.01_60/ts_102942v010101p.pdf

ETSI TS 102 943 V1.1.1 “Intelligent Transport Systems (ITS); Security; Confidentiality services” https://www.etsi.org/deliver/etsi_ts/102900_102999/102943/01.01.01_60/ts_102943v010101p.pdf

ETSI TS 103 097 v1.3.1, “Intelligent Transport Systems (ITS); Security; Security header and certificate formats”: https://www.etsi.org/deliver/etsi_ts/103000_103099/103097/01.03.01_60/ts_103097v010301p.pdf

ETSI TR 102 893 “Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA) https://www.etsi.org/deliver/etsi_tr/102800_102899/102893/01.02.01_60/tr_102893v010201p.pdf

SAE J3061 “Cybersecurity Guidebook for Cyber-Physical Vehicle Systems”: https://www.sae.org/standards/content/j3061_201601/

ITF/OECD “Safer Roads with Automated Vehicles”, https://www.itf-oecd.org/sites/default/files/docs/safer-roads-automated-vehicles.pdf

ISO/SAE CD 21434 “Road Vehicles – Cybersecurity engineering”: https://www.iso.org/standard/70918.html

“ENISA Threat Taxonomy” (2016): https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view

“Tesla cars can be stolen by hacking the app”: https://promon.co/security-news/hacking-tesla-app-stolen-car/

“MobilBye: Attacking ADAS with Camera Spoofing”: https://arxiv.org/pdf/1906.09765.pdf

“Robust Physical-World Attacks on Deep Learning Models”: https://arxiv.org/pdf/1707.08945.pdf

“Self-driving Ubers could still be many years away, says research head”: https://nationalpost.com/pmn/news-pmn/canada-news-pmn/self-driving-ubers-could-still-be-many-years-away-says-research-head

“Domain Controlled Architecture – A new approach for large scale software integrated automotive systems”: https://pdfs.semanticscholar.org/65ff/f1cd276736bc5cf67d0cb30db269cd08b5f5.pdf

“VCIDS: Collaborative Intrusion Detection of Sensor and Actuator Attacks on Connected Vehicles”: http://php.scripts.psu.edu/muz16/pdf/PG-ea-Comm17.pdf

“Work-in-Progress: Road Context-aware Intrusion Detection System for Autonomous Cars”: https://sudiptac.bitbucket.io/papers/raids.pdf

“Intelligent Intrusion Detection in External Communication Systems for Autonomous Vehicles”: https://www.tandfonline.com/doi/full/10.1080/21642583.2018.1440260

"Hopping on the CAN Bus – Automotive Security and the CANard Toolkit": https://www.blackhat.com/docs/asia-15/materials/asia-15-Evenchick-Hopping-On-The-Can-Bus.pdf

"DEFCON – Connected Car Security": https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/defcon-connected-car-security/

"Spatially Clustered Autonomous Vehicle Malware: Producing New Urban Geographies of Inequity": https://journals.sagepub.com/doi/full/10.1177/0361198118794057

"Fast, Furious and Insecure: Passive Keyless Entry and Start in Modern Supercars": https://www.esat.kuleuven.be/cosic/fast-furious-and-insecure-passive-keyless-entry-and-start-in-modern-supercars/

"All your GPS Are Belong to Us: Towards Stealthy Manipulation of Road Navigation Systems": https://www.usenix.org/node/217477

"Analyzing and Enhancing the Security of Ultrasonic Sensors for Autonomous Vehicles": https://ieeexplore.ieee.org/document/8451864

"Jamming and Spoofing Attacks: Physical Layer Cybersecurity Threats to Autonomous Vehicle Systems": https://tlpc.colorado.edu/wp-content/uploads/2016/11/2016.11.21-Autonomous-Vehicle-Jamming-and-Spoofing-Comment-Final.pdf

UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security : https://www.unece.org/fileadmin/DAM/trans/doc/2019/wp29grva/ECE-TRANS-WP29-GRVA-2019-02e.pdf

Safety First for Automated Driving : https://www.aptiv.com/docs/default-source/white-papers/safety-first-for-automated-driving-aptiv-white-paper.pdf

SCOUT - Report on the state of the art of connected and automated driving in Europe : https://connectedautomateddriving.eu/publication/scout-deliverable-3-2-report-on-the-state-of-the-art-of-connected-and-automated-driving-in-europe-final/

PAS 1885:2018 The fundamental principles of automotive cyber security specification, bsi : https://shop.bsigroup.com/ProductDetail/?pid=000000000030365446&_ga=2.267667464.704902458.1545217114-2008390051.1545217114

GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document : https://www.gsma.com/iot/wp-content/uploads/2016/02/CLP.11-v1.1.pdf

Autonomous DevSecOps: Five Steps to a Self-Driving Cloud (ENT214-S) - AWS re:Invent 2018 : https://www.slideshare.net/AmazonWebServices/autonomous-devsecops-five-steps-to-a-selfdriving-cloud-ent214s-aws-reinvent-2018

Redhat DevSecOps : https://www.redhat.com/en/topics/devops/what-is-devsecops

What is DevSecOps? Developing more secure applications : https://www.csoonline.com/article/3245748/what-is-devsecops-developing-more-secure-applications.html

Security Champions Playbook :
https://www.owasp.org/index.php/Security_Champions_Playbook

Avoid Unnecessary Pain with a Security Champion :
https://www.csoonline.com/article/3299430/avoid-unnecessary-pain-with-a-security-champion.html

IoT Alliance Australia - Internet of Things Security Guidelines v1.2 :
https://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf

Privacy Impact Assessment : https://gdpr-info.eu/issues/privacy-impact-assessment/

Data Protection Impact Assessment (DPIA) : https://gdpr.eu/data-protection-impact-assessment-template/

GDPR: How to Perform a Data Audit : https://www.thesslstore.com/blog/gdpr-data-audit/

GDPR checklist for data controllers : https://gdpr.eu/checklist/

Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance : https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/identity-and-access-management-for-the-iot.pdf

Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things :
https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

IEC - IEC 62443-3-3:2013 System security requirements and security levels :
https://webstore.iec.ch/publication/7033

ISO - ISO/IEC 27001:2013 Information technology -- Security techniques – Information security management systems -- Requirements : https://www.iso.org/standard/54534.html

ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls : https://www.iso.org/standard/54533.html

NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations : https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile :
https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf

SANS Institute - Vulnerability Management: Tools, Challenges and Best Practices :
https://www.sans.org/reading-room/whitepapers/threats/paper/1267

Huawei - IoT Security White Paper 2017 :
https://www.huawei.com/minisite/iot/img/hw_iot_secutity_white_paper_2017_en_v2.pdf

NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks : https://csrc.nist.gov/publications/detail/nistir/8228/final

LNS - Putting Industrial Cyber Security at the top of the CEO agenda : https://www.honeywellprocess.com/en-US/online_campaigns/lns-cyber-report/Pages/Honeywell-LNS-Study_PuttingIndustrialCyberSecurityattheTopCEOAgenda.pdf

NIST - NIST SP 800 30r1 - Guide for Conducting Risk Assessments : https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security : https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Safety First for Automated Driving" (SaFAD) : https://www.daimler.com/innovation/case/autonomous/safety-first-for-automated-driving-2.html

European Commission -- Access to In-vehicle Data and Resources : https://ec.europa.eu/transport/sites/transport/files/2017-05-access-to-in-vehicle-data-and-resources.pdf

ENISA - Cyber Security and Resilience of Smart Cars : https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis : https://www.etsi.org/deliver/etsi_TR/102800_102899/102893/01.01.01_60/tr_102893v010101p.pdf

Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary : https://www.automotiveisac.com/best-practices/

IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use : https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_2018-04-09.pdf

International Telecommunications Union - Security capabilities supporting safety of the Internet of things : https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.4806-201711-I!!PDF-E&type=items

Five Star Automotive Cyber Safety Program : https://www.iamthecavalry.org/domains/automotive/5star/

Securing the Modern Vehicle : https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/securing-the-modern-vehicle.pdf

Security Development Lifecycle (SDL) : https://www.microsoft.com/en-us/securityengineering/sdl/practices

COLLABORATION AND ENGAGEMENT WITH APPROPRIATE THIRD PARTIES : https://www.automotiveisac.com/wp-content/uploads/2018/08/2018_01_18_Best_Practice_Guide_Third_Party_Collaboration_Engagemen.pdf

ENISA - Good practices for Security of Internet of Things in the context of Smart Manufacturing : https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program : https://webstore.iec.ch/preview/info_iec62443-2-1%7Bed1.0%7Den.pdf

Insecurity in the Internet of Thing : https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/insecurity-in-the-internet-of-things-15-en.pdf

IoT Security Awareness : https://resources.infosecinstitute.com/iot-security-awareness/#gref

Consumers don't care if their connected car can get hacked - here's why that's a problem : https://www.businessinsider.com/smart-car-hacking-major-problem-for-iot-internet-of-things-2016-3?IR=T

Shifting gears in cyber security for connected cars: https://www.mckinsey.com/~/media/mckinsey/industries/automotive%20and%20assembly/our%20insights/shifting%20gears%20in%20cybersecurity%20for%20connected%20cars/shifting-gears-in-cyber-security-for-connected-cars.ashx

CSIRTs in Europe:https://www.enisa.europa.eu/topics/csirts-in-europe?tab=articles

ACEA Principles of Automobile Cybersecurity: https://www.acea.be/publications/article/acea-principles-of-automobile-cybersecurity

Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practices: https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/securing-the-modern-vehicle.pdf

30% of Automotive Companies Lacking a Dedicated Cybersecurity Team : https://www.bleepingcomputer.com/news/security/30-percent-of-automotive-companies-lacking-a-dedicated-cybersecurity-team/

Security Champions Playbook : https://www.owasp.org/index.php/Security_Champions_Playbook

Avoid Unnecessary Pain with a Security Champion : https://www.csoonline.com/article/3299430/avoid-unnecessary-pain-with-a-security-champion.html

SAE J3061: https://www.researchgate.net/publication/307585960_Using_SAE_J3061_for_Automotive_Security_Requirement_Engineering

Security Operations Center : https://securityaffairs.co/wordpress/47631/breaking-news/soc-security-operations-center.html

MITRE :Cybersecurity Operations Center : https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf

Survey and Classification of Automotive Security Attacks - MDPI : https://www.mdpi.com/2078-2489/10/4/148/pdf-vor

PRESERVE - Security Requirements of Vehicle Security Architecture v1.1 : https://www.preserve-project.eu/sites/preserve-project.eu/files/PRESERVE-D1.1-Security%20Requirements%20of%20Vehicle%20Security%20Architecture.pdf

C-ITS Platform, WG5: Security & Certification - Final Report - Annex 2: Revocation of Trust in C-ITS : https://smartmobilitycommunity.eu/sites/default/files/Security_WG5An2_v1.0.pdf

ACEA Principles of Automobile Cybersecurity : https://www.acea.be/publications/article/acea-principles-of-automobile-cybersecurity

ENISA - Baseline Security Recommendations for IoT : https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices : https://www.iiconsortium.org/pdf/Endpoint_Security_Best_Practices_Final_Mar_2018.pdf

IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines : https://iotsecurityfoundation.org/wp-content/uploads/2016/12/Connected-Consumer-Products.pdf

OWASP (Open Web Application Security Project) - IoT Security Guidance : https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

SANS Institute - An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity : https://ics.sans.org/media/An-Abbreviated-History-of-Automation-and-ICS-Cybersecurity.pdf

A survey on open automotive forensics : https://forschung-sachsen-anhalt.de/publication/survey-open-automotive-forensics-1002323053

Log your car: the non-invasive vehicle forensics : https://ieeexplore.ieee.org/document/7847047

“My autonomous car is an elephant”: A Machine Learning based Detector for Implausible Dimension : https://ieeexplore.ieee.org/document/8556651

AUTOMOTIVE WORKING GROUP : https://www.w3.org/blog/auto/

OWASP: Session Management Cheat Sheet : https://www.owasp.org/index.php/Session_Management_Cheat_Sheet

OWASP: Session fixation : https://www.owasp.org/index.php/Session_fixation

CAR 2 CAR Communication Consortium - FAQ regarding Data Protection in C-ITS v1,0,0 : https://www.car-2-car.org/service/privacy/

Secure Device Configuration Guideline : https://security.berkeley.edu/secure-device-configuration-guideline

ISA-95.01 MODELS & TERMINOLOGY : https://isa-95.com/isa-95-01-models-terminology/

Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor : https://www.industry.usa.siemens.com/automation/us/en/formsdocs/Documents/2016%20MIA-

%2023%20Industrial%20Security%20Applying%20IoT%20Security%20Controls%20on%20the%20Industrial%20Plant%20Floor.pdf

Gowling WLG & UK Autodrive - Connected and Autonomous Vehicles: A Hacker's Delight? : https://gowlingwlg.com/GowlingWLG/media/UK/pdf/autodrive/170907-cyber-security-white-paper.pdf

Cybersecurity Solutions for Connected Vehicles : https://www.trendmicro.com/us/iot-security/content/main/document/IoT%20Security%20for%20Auto%20Whitepaper.pdf

Securing Self-Driving Cars : http://illmatics.com/securing_self_driving_cars.pdf?_sm_au_=iqs579QRrj9HP44Q

Using Open Source for security and privacy protection : https://security-and-privacy-reference-architecture.readthedocs.io/en/latest/10-using-oss.html

Federal Office for Information Security: Business Continuity Management : https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.pdf?__blob=publicationFile&v=1

GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems : https://www.gsma.com/iot/wp-content/uploads/2016/02/CLP.12-v1.0.pdf

Online Trust Alliance - IoT trust framework 2.5 : https://www.internetsociety.org/resources/doc/2018/iot-trust-framework-v2-5/

NIST - NIST SP 800-146 Cloud Computing Synopsis and Recommendations : https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf

SANS Institute - Building the New Network Security Architecture for the Future : https://www.sans.org/reading-room/whitepapers/internet/paper/38255

Cloud Security Alliance - Future Proofing the connected world : https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf

Federal Office for Information Security (BSI) - BSI-Standards 100-4 - Business Continuity Management : https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.pdf?__blob=publicationFile&v=1

FAQ: CAR 2 CAR Communication Consortium - FAQ regarding Data Protection in C-ITS v1,0,0 : https://www.car-2-car.org/fileadmin/documents/General_Documents/C2CCC_TR_2051_Data_Protection.pdf

European Commission - Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport System (C-ITS) : https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy_release_1.pdf

What is physical security? How to keep your facilities and devices safe from on-site attackers : https://www.csoonline.com/article/3324614/what-is-physical-security-how-to-keep-your-facilities-and-devices-safe-from-on-site-attackers.html

Principle of least privilege (POLP) : https://searchsecurity.techtarget.com/definition/principle-of-least-privilege-POLP

Improving security through least-privilege practices : http://techgenix.com/improving-security-through-least-privilege-practices/?_sm_au_=iqs579QRrj9HP44Q

GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems : https://www.gsma.com/iot/wp-content/uploads/2016/02/CLP.13-v1.0.pdf

Autonomous integrity monitoring of navigation maps on board intelligent vehicles : https://www.researchgate.net/publication/278826487_Autonomous_Integrity_Monitoring_of_Navigation_Maps_on_board_Intelligent_Vehicles

Symantec - Insecurity in the Internet of Things : https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/insecurity-in-the-internet-of-things-15-en.pdf

OWASP Internet of Things Project – OWASP : https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

OWASP Top Ten Project – OWASP : https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Secure hypervisor versus trusted execution environment : http://www.diva-portal.se/smash/get/diva2:1120483/FULLTEXT01.pdf?_sm_au_=iqs579QRrj9HP44Q

Isolated Execution in Many-core Architectures : https://eprint.iacr.org/2014/136.pdf

An Autonomous Vehicle Navigation System Based on Inertial and Visual Sensors : https://www.researchgate.net/publication/327470347_An_Autonomous_Vehicle_Navigation_System_Based_on_Inertial_and_Visual_Sensors

Security Innovation - Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR : https://pdfs.semanticscholar.org/e06f/ef73f5bad0489bb033f490d41a046f61878a.pdf

Towards deep learning models resistant to adversarial attacks : https://openreview.net/pdf?id=rJzIBfZAb

Explaining and harnessing adversarial examples : https://arxiv.org/pdf/1412.6572.pdf

Pixeldefend: Leveraging generative models to understand and defend against adversarial examples. In International Conference on Learning Representations (ICLR),2018 : https://openreview.net/forum?id=rJUYGxbCW

The robust manifold defense: Adversarial training using generative models : https://arxiv.org/abs/1712.09196

Thermometer encoding: One hot way to resist adversarial examples. In International Conference on Learning Representations (ICLR), 2018 : https://openreview.net/pdf?id=S18Su--CW

Securing the Future of AI and ML : https://docs.microsoft.com/en-us/security/securing-artificial-intelligence-machine-learning

Groupe PSA - Attacker model for Connected and Automated Vehicles Security Innovation - Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR : https://pdfs.semanticscholar.org/e06f/ef73f5bad0489bb033f490d41a046f61878a.pdf

Duo Security - The Internet of Fails ; Where IoT Has Gone Wrong : https://www.slideshare.net/markstanislav/the-internet-of-fails-where-iot-has-gone-wrong-and-how-were-making-it-right

A Hard Problem with No Easy Answers | Decipher - IoT Security : https://duo.com/decipher/iot-security-hard-problem-no-easy-answers

Center for Internet Security (CIS) - Critical Security Controls : https://www.cisecurity.org/controls/

oneM2M - Standards for M2M and the Internet of Things - TR 0008 Security V2.0.0 - Security. Technical Report : http://www.onem2m.org/images/files/deliverables/Release2A/TR-0008-Security-v_2_0_1.pdf?_sm_au_=iqs579QRrj9HP44Q

OWASP – Mobile Application Security Verification Standard: https://github.com/OWASP/owasp-masvs/releases/download/1.1.4/OWASP_Mobile_AppSec_Verification_Standard_1.1.4_Document.pdf

ENISA – Smartphone Secure Development Guidelines: https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016

ANNEX A: ASSET TAXONOMY

Annex A lists the different assets mentioned in **Figure 5**, and provides a brief description of each asset.

Asset Group	Assets	Description
Car sensors and actuators	Standard Sensors	These devices are common sensors (e.g. tire pressure, air bag impact, GNSS, speed, powertrain, seat belt, passenger occupancy, temperature, oil, water coolant, parking and climate control sensors) usually embedded in cars to measure some parameters and/or monitor or detect some events. The collected data is transmitted to ECU for processing purposes.
	Sensors for autonomous vehicles	These devices are relatively new sensors embedded in autonomous vehicles to provide self-driving capabilities (e.g. localization, enabling the detection and identification of objects and people). This category of sensors mainly includes the following sensors: • Light Detecting and Ranging (LiDAR) • Lasers • Cameras • Radars • Ultrasonic sonars
	Actuators	These devices are an important part of vehicles. They interact with the environment by converting an electrical signals received from the ECU into an action (e.g. apply the brake when a red light or a pedestrian crossing the road is detected, speed reduction on bad weather conditions, change of direction to get around an obstacle). The engine control unit, suspension, transmission, brake system and steering system are some examples of actuators.
Decision Making Algorithms **(Car ECUs, processing and decision making components** **Smart cars Infrastructure and Backend systems)**	ML and AI algorithms	These software components provide smart cars with the capability to perform tasks that are typical for intelligent beings, such as reacting to an unanticipated and new situation based on previously collected data. ML and AI algorithms are implemented inside smart cars to enable them to react in real time whenever required, but they may be implemented outside the vehicle in remote servers as well.

Asset Group	Assets	Description
	Data fusion algorithms	These software components combine data acquired from different sensors (e.g. LiDAR and camera) and V2X communications.
Vehicle Functions **Car sensors and actuators** **Car ECUs, processing and decision making components**	Vehicle functions	This term refers to the different vehicle functions (such as braking, acceleration, operating the steering wheel, route planning, etc.) which rely on one or several sensors data as well as processing and actuating nodes to operate correctly.
Software management **Car ECUs, processing and decision making components** **In-vehicle communication components** **Smart cars Infrastructure and Backend systems**	Software and Licenses	This term refers to the different software components of the vehicle. It includes on-board operating systems (which manage the resources of a given smart car hardware device and provides common services for other computer programs to run), programs and codes (which are written to perform a given task or technological objective, such as AI-based algorithms as well as real-time monitoring algorithms, or even protocol stacks/cryptographic algorithms' software implementations), mobile applications (which correspond to programs running on mobile devices such as smartphones and tablets that are used to communicate with the smart car, to unlock the doors for instance) and antivirus (which is a particular software that monitors a device or network to detect and identify malwares, and prevent them from infecting devices) as well as on-board firmware (which is a class of software that are stored on a device read-only memory and provides instructions on how the device should operate). A smart car can include several OSes embedded on different devices. As for programs, antivirus and firmware, they can be found at every level: from ECUs to back-end servers.
	Software updates	This term refers to software updates (including Over-The-Air (OTA) updates) that are used by the OEM to remotely or locally deploy new firmware or software on smart cars.
Inside vehicle Communication Components	Telematics box	This electronic module is the vehicle main communication unit. It provides the capability to connect to the cellular communication networks and enables other short and long range communications based on several technologies, such as Near Field Communications (NFC), Bluetooth, WiFi, etc.

Asset Group	Assets	Description
In-vehicle communication components	Vehicle ITS station	This device enables wireless V2V and V2I communications.
	In-Vehicle Gateway	This device plays a crucial role in smart cars. It interconnects the various in-vehicle networks to the telematics box and ITS station. It also provides physical isolation between the different functional domains.
	In-Vehicle Infotainment (IVI)	This asset, also known as Head Unit or In-car Entertainment (ICE), refers to a vehicle system combining information exchanges (between the vehicle and the drivers/passengers through a touch screen-based tablet like device) and entertainment (i.e. audio and video). Smartphones can also be paired with such unit, allowing remote connectivity. It provides a hardware interface for the entire vehicle.
	OBD-II port	The OBD-II port, also called diagnostics plug, is an external interface that allows plugging different maintenance and diagnostic devices to smart cars.
	EV charging connector	The interface used to plug an electric or hybrid smart car to a charging station.
Communication Networks and Protocols **(Car ECUs, processing and decision making components** **In-vehicle communication components** **Car sensors and actuators**	In-Vehicle networks	In-vehicle communications and domain subnetworks rely on several protocols such as Controller Area Network (CAN), Local Interconnect Network (LIN), Media Oriented Systems Transport (MOST), FlexRay and Ethernet.
	Protocols and communication technologies	Telematics box and ITS station provide different wireless communication technologies including 802.11p (DSRC), Cellular-V2X (C-V2X), cellular technologies (2G, 3G, 4G, 5G), NFC, Wi-Fi, Bluetooth.
Nearby External Components **Smart cars Infrastructure and Backend systems**	Communication Components	These devices refers to nearby communication components interacting with smart cars. They include: Access Points (AP) which is a cellular networking hardware device that supports cellular communications and which directly communicates with the smart car telematics box. Road Side Unit (RSU), also known as Road Side Equipment (RSE), which is a communication device located on the roadside to provide connectivity and enable communication between the road side infrastructure and smart cars.

Asset Group	Assets	Description
	Traffic signs and lights	Traffic signs and lights provide road users and smart cars with the necessary safety instructions and are mainly used to regulate the speed and traffic flow. In particular, traffic signs give the driving practices to follow and warn about dangerous conditions while traffic lights provide vehicles and drivers with the necessary instructions to follow at intersections and along roads. This asset includes lane marking as well.
Network and Domain Isolation Features **Car ECUs, processing and decision making components,** **In-vehicle communication components** **Smart cars Infrastructure and Backend systems**	Firewall	This network security device or software monitors and controls incoming and outgoing network traffic based on a predetermined set of security rules.
	Routing table	It corresponds to a set of rules enabling to direct data packets to its destination or drop the packet if no match is found.
	Domain controllers[59]	These devices interconnect the different in-vehicle functional domains. They need to be powerful in terms of processing capabilities and real-time performance in order to support autonomous vehicles' highly interconnected architecture.
	IDS/IPS	Intrusion Detection Systems (IDS) allow automatic monitoring of the happening events, and analyses them to detect any potential sign of intrusion. Intrusion Prevention Systems (IPS) can also perform given actions whenever some specific events happen in attempt to stop the incident. Such systems can be found deployed at the vehicle level[60,61] as well as the infrastructure level[62].
Servers, Systems and Cloud Computing **Smart cars Infrastructure and Backend systems**	Back-end Systems	This term refers to the back-end systems which enable Over-The-Air updates among other services.
	Database servers	This term refers to a database back-end system which consists of both hardware and software used to run a database. These servers may for instance store and process in-vehicle data and resources to enable service providers to propose services such as software updates.
	Maps servers	This term refers to remote servers that provide longitudinal and lateral data to the smart cars, thus

[59] See "Domain Controlled Architecture – A new approach for large scale software integrated automotive systems": https://pdfs.semanticscholar.org/65ff/f1cd276736bc5cf67d0cb30db269cd08b5f5.pdf

[60] See "VCIDS: Collaborative Intrusion Detection of Sensor and Actuator Attacks on Connected Vehicles": http://php.scripts.psu.edu/muz16/pdf/PG-ea-Comm17.pdf

[61] See "Work-in-Progress: Road Context-aware Intrusion Detection System for Autonomous Cars": https://sudiptac.bitbucket.io/papers/raids.pdf

[62] See "Intelligent Intrusion Detection in External Communication Systems for Autonomous Vehicles": https://www.tandfonline.com/doi/full/10.1080/21642583.2018.1440260

Asset Group	Assets	Description
		enabling it to navigate and to decide the next trajectory to reach its destination. These servers may also provide a map database that can be locally stored on the vehicle.
	Third- party service providers servers	This term refers to remote servers used by service provider in order to propose added value services such as eToll for toll payments and breakdown call (bCall).
Information **Throughout model**	Sensors data	This asset refers to data that is gathered by the different smart car sensors and which will be transmitted to the appropriate ECU for processing.
	Keys and certificates	This asset refers to the different keys and certificates used for security purposes (such as authentication, securing the exchanges, secure boot, etc.). Keys are stored in devices embedded in the vehicle (e.g. ECU) and/or in servers depending on their use.
	Map data	This asset refers to the information about the car environment. Map data allow to increase the passenger safety by correlation its information with the sensors perception. Contrary to GNSS which gives only information about the geolocalization, map data gives information about the surrounding environment.
	V2X information	This asset refers to the different information exchanged via V2X communications (e.g. emergency vehicle approaching, roadworks/collision warning and traffic information).
	Device information	This asset refers to the different information related to a device embedded in a smart car (e.g. ECU, TCU) or connected devices (e.g. smartphones, tablet). This includes information such as type, configuration, firmware version, status, etc.
	User information	This asset refers to smart cars user (e.g. driver, passenger, etc.) information such as name, role, privileges and permissions.
Humans **Throughout model**	Drivers	This asset refers to all individuals who are entitled to drive the smart car. This asset is optional when considering SAE automation level 5 as such smart car is fully automated.
	Passengers	This asset refers to all individuals that are onboard smart cars.

Asset Group	Assets	Description
	OEM staff	This asset refers to OEM individuals who have physical or remote privileged access to the smart car for several purposes (such as maintenance, adding features and performing updates).
	Mechanics	This asset refers to non-OEM individuals who have physical access to smart cars for maintenance purposes.
Mobile Devices **(Smart cars Infrastructure and Backend systems)**	Smartphones and Tablets	This term refers to portable devices that run mobile applications providing added value services to the vehicle user.

ANNEX B: THREAT TAXONOMY

Annex B provides a brief description of the different threats subcategories mentioned in **Figure 6**, and maps each threat to the asset(s) that may potentially be affected.

Threat Category	Threat	Description	Impacted Assets
Nefarious activity/Abuse	Denial of Service	Smart cars and their infrastructure, may be subject to Distributed Denial of Service (DDoS) attacks, or even used to launch such attacks. DoS attacks may target (or originate from) RSUs or the IT systems. An attacker may for instance shut down the RSU (via physical access or remotely), overload the system with messages to process or even jam radio communications, etc. In-vehicle components can also be the target of DoS attacks. For instance, overloading the CAN bus with malicious messages will alter the vehicle behaviour[63].	All assets
	Malware	These malicious software aim at performing unwanted and illegitimate actions such as disabling smart cars functions (e.g. prevent car unlocking or immobilize the engine). Malware can cause unexpected behaviours of the smart car and even endanger passengers' safety. Common examples or malwares are Ransomware[64], viruses, Trojan horses, Spyware[65] and exploit kits.	All assets
	Manipulation of hardware and software	This threat consists of unauthorized and illegitimate alteration of a component firmware, operations or configuration data by an attacker (e.g. malicious OTA updates). An attack might also access the binary file, compromising the intellectual property. The risk is emphasized when there are no security measures (e.g. secure boot) to protect the authenticity of critical hardware and software components. An attacker may also perform Man-in-the-middle attacks by	All assets

[63] See "Hopping on the CAN Bus – Automotive Security and the CANard Toolkit": https://www.blackhat.com/docs/asia-15/materials/asia-15-Evenchick-Hopping-On-The-Can-Bus.pdf

[64] See "DEFCON – Connected Car Security": https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/defcon-connected-car-security/

[65] See "Spatially Clustered Autonomous Vehicle Malware: Producing New Urban Geographies of Inequity": https://journals.sagepub.com/doi/full/10.1177/0361198118794057

Threat Category	Threat	Description	Impacted Assets
		manipulating the hardware. Potential consequences of this kind of threats may include inappropriate smart cars behaviours.	
	Manipulation of information	This threat consists of illegitimate and unwanted data alteration by an attacker. To this end, the attacker may use various technical means such injecting fake Basic Safety Message (BSM)[66], performing map data poisoning, faking security-related information (e.g. keys, certificates, Certificate Revocation List), tampering with RSU data or OTA update exchanges, injection of packet over CAN bus[67], repudiation of actions (e.g. deny eToll), loss of data (e.g. erase of vehicle history), etc. Information manipulation threats may result in inappropriate decisions that are based on the altered/falsified data, and may also lead to information or intellectual values disclosure.	- Vehicle sensors and actuators - Decision making algorithms - Vehicle Functions - Network and Domain Isolation Features - Information - In-vehicle Communication Networks - In-vehicle Communication Components - External Communication Components - Servers, Systems and Cloud Computing - Mobile Devices - Humans
	OEM Targeted attacks	Cyberattacks targeting smart cars manufactured by a specific OEM or its backend systems during which the attackers typically use several attack methods and entry points to achieve their goals. Such attacks are usually scalable and may lead to reputational damage and/or information or intellectual property disclosure (such as the knowledge of in-vehicle internal architecture).	All assets
	Unauthorised activities	A legitimate user may try to access unauthorized functions for various reasons: they might want to circumvent DRMs on applications or media, or get an unauthorized	All assets

[66] A specific message format aimed to convey critical vehicle state information in support of V2V safety applications, as defined in SAE J2735 https://www.sae.org/standards/content/j2735_201603/

[67] See “Hopping on the CAN Bus – Automotive Security and the CANard Toolkit”: https://www.blackhat.com/docs/asia-15/materials/asia-15-Evenchick-Hopping-On-The-Can-Bus.pdf

Threat Category	Threat	Description	Impacted Assets
		access to features (geo-fencing, digital tachograph…), or they might simply want to tune the vehicle for comfort or performance purposes. Outside vehicles, manufacturers may also be confronted with garages using unauthorized or unlicensed professional tools and software. Unauthorised software may also be installed by an attacker. This threat also includes the notion of cloning, for example when an attacker copies the firmware of an existing device, in order to commercialize it without authorization.	
	Identity theft	Impersonation attacks in which an adversary successfully assumes the identity of one of the legitimate parties in the system or in a communication protocol. A common example is to impersonate a key fob[68] to steal the associated car. This may, however, be completed for other purposes, such as fraud, for example if a user wants their car to display another identity when communicating with: - road infrastructures such as toll systems, thus leading to financial fraud; - manufacturer backend[46] (to get access to paid services without subscription). An attacker may also impersonate a police car or ambulance in order to make other vehicles slow down or pull over. Thus, the attacker can reach his destination more quickly.	All assets
	Abuse of authorizations	A disgruntled employee (backend services, garage) may use their authorizations to perform malicious actions (e.g. create illegitimate user accounts, or add malicious software into the system). A slightly different scenario would be for an infotainment application to abuse its authorizations (for example, to mine private data or perform surveillance activities).	All assets

[68] See "Fast, Furious and Insecure: Passive Keyless Entry and Start in Modern Supercars": https://www.esat.kuleuven.be/cosic/fast-furious-and-insecure-passive-keyless-entry-and-start-in-modern-supercars/

Threat Category	Threat	Description	Impacted Assets
Threats against (semi-) autonomous systems	Threats targeting autonomous sensors	Smart cars autonomous sensors (like cameras, LiDARs and Radar sensors) may be subject to DoS attacks using several means such as presenting too many objects to track, blinding camera[69] and LIDAR/radar jamming[70]. GNSS spoofing[71] attacks may also be performed in an attempt to deceive a GNSS receiver through the broadcast of incorrect GNSS signals.	- Sensors for autonomous vehicles - Vehicle Functions - Information
	Threats against AI and ML	Attacks may be carried out against AI and ML features. For instance, the attacker may perform adversarial perturbation[72] in an intent to hide objects, fool auto-controls (e.g. radar/LIDAR confusion) and/or perceive fake data (e.g. fake crash sound or ultrasonic reflection[73], magnetic attacks targeting odometric sensors). An attacker may also provide malicious inputs during the model training phase in order to alter the classification.	- Sensors for autonomous vehicles - Decision Making algorithms - Vehicle Functions - Information
Physical attack	Sabotage	Intentional tampering of a device by an attacker with the aim to alter the proper functioning of the vehicle, thus endangering the safety of smart cars passengers and roads users. The attacker may directly target smart cars components (e.g. by compromising decision making algorithms or brake system, replacing a car component with a malicious one), or alter/remove RSUs, traffic signs and/or lights. The attacker may even compromise backend systems (e.g. eCall platform, database servers) in an attempt to execute unauthorized operations.	All assets
	Vandalism	Intentional physical degradation of car components (e.g. damage cameras), RSUs, traffic signs or lights (e.g. alter or remove traffic signs on the road). Such threat would impact the operations of the vehicle and	- Vehicle sensors and actuators - Decision making algorithms - External

[69] See “Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR”: https://pdfs.semanticscholar.org/e06f/ef73f5bad0489bb033f490d41a046f61878a.pdf

[70] See “Illusion and Dazzle: Adversarial Optical Channel Exploits against LiDARs for Automotive Applications”: https://eprint.iacr.org/2017/613.pdf

[71] See “All your GPS Are Belong to Us: Towards Stealthy Manipulation of Road Navigation Systems”: https://www.usenix.org/node/217477

[72] See “Robust Physical-World Attacks on Deep Learning Visual Classification”: https://arxiv.org/pdf/1707.08945.pdf

[73] See “Analyzing and Enhancing the Security of Ultrasonic Sensors for Autonomous Vehicles”: https://ieeexplore.ieee.org/document/8451864

Threat Category	Threat	Description	Impacted Assets
		make cause accidents and dangerous situations.	communication components - Information - Humans
	Theft	Theft of devices (e.g. car components, RSUs) that may alter the vehicle proper functioning and endanger road users' safety.	- Vehicle sensors and actuators - Decision making algorithms - External communication components - Information - Humans
	Side-channel attacks	Side-channel attacks consist in exploiting physical characteristics of the computing platform (e.g. execution time, power consumption) to recover security credentials (i.e. cryptographic keys and passwords) in order to bypass security mechanisms. Such attacks generally require a physical access to the targeted device, but some of them (e.g. timing attacks) may be performed remotely. Side channel attacks could target critical ECUs or other devices that use security credentials (e.g. for V2X communications).	- Vehicle sensors and actuators - Functions - Software and licenses - Information - In-vehicle communication networks
	Fault injection	Fault injection threats consist in disrupting the computational operations of a security mechanism (e.g. skipping a password verification) to bypass security mechanisms. Such attacks generally require a physical access to the targeted device, but some of them (e.g. Rowhammer attacks) can be performed remotely. They would mainly target critical ECUs.	- Vehicle sensors and actuators - Functions - Software and licenses - Information - In-vehicle communication networks
Failures / Malfunctions (Car sensors and actuators **Car ECUs, processing**	Failure or malfunction of a sensor/actuator	This threat impacts the proper functioning of a sensor and/or actuator. It may accidentally happen (e.g. as a result of improper use or maintenance). It may also be intentional through software vulnerabilities (e.g. ability to spread a malware on ECUs).	- Vehicle sensors and actuators - Functions - Software and licenses

Threat Category	Threat	Description	Impacted Assets
and decision making components)			- Information - In-vehicle communication networks - In-vehicle communication components - Decision making algorithms - Humans
	Software vulnerabilities exploitation	Threats leveraging the use of outdated software versions, bugs, improper configurations, zero-day vulnerabilities or specific software components such as weak cryptographic algorithms or vulnerable open source libraries. Unsecure OTA updates might also be exploited in order to spread a malware or perform software downgrade to a version with known vulnerabilities.	All assets
	Failure or Disruption of service	This threat targets OEM services and/or third party services in order to limit the car features, or disrupt smart cars' operations. It could be done by different means (e.g. DDoS attack, malicious software updates).	- Decision making algorithms - Functions - Software and licenses - External communication components - Servers, systems and cloud computing - Information - Humans - Mobile devices
Eavesdropping **/Interception** **/Hijacking**	Communication protocol hijacking	Cyberattacks that exploit flaws in communication protocols so as to perform impersonation attacks (e.g. rogue BTS attack due to a lack of authentication), replay attacks (e.g. performing an ECU software downgrade), or more generally the injection of malicious packets, the interception of information or the disruption of communications. Such threats may lead to	All assets

Threat Category	Threat	Description	Impacted Assets
		the disclosure of sensitive and/or private information, including passwords.	
	Data replay	Cyberattack that exploits data replay techniques. Such attack can occur at the protocol level (e.g. lack of timestamp and/or authentication) but also at the sensor level (e.g. use a repeater to create a ghost vehicle).	-Decision making algorithms -Functions -External communication components -In-vehicle communication networks -In-vehicle communication components - Servers, systems and cloud computing -Information -Humans
	Man-in-the-middle attack / Session hijacking	Man-In-The-Middle (MITM) attacks exploit the lack of authentication to disrupt the communications between legitimate entities or to disclose/modify exchanged information (e.g. provide fake information to RSUs to affect traffic conditions). They apply to both in-vehicle and V2X communications.	All assets
Unintentional Damages (accidental) (In-vehicle communication components)	Unintentional change of data or car components configuration	Unintentional modification of configuration or data by a legitimate entity leading to potential vulnerabilities. It can arise from the misconfiguration of an equipment (e.g. by mechanics or OEM staff during maintenance) or simply because defined security procedures were not followed.	All assets
	Information leakage	This may typically concern administration errors in back-end services or errors when storing data intended for diagnostic in garages, for example.	- Information - Humans
	Using information and/or devices from an unreliable source	Unintentional damages may cascade from ill-defined trust relationships: for example, trusting a third-party cloud provider with poor data protection, or failing to notify a Tier developer that the data they will store is sensitive.	All assets

Threat Category	Threat	Description	Impacted Assets
	Erroneous use or configuration of car components	Unintentional damage to car components (e.g. cameras or autonomous sensors) due to an erroneous use or misconfiguration by a smart cars' users, insufficiently trained OEM staff members (e.g. incompatibilities between components), mechanics (e.g. when using diagnostic equipment), or lack of adaptation to the changing threat landscape (the use of vulnerable cryptography is an example of this).	-Vehicle sensors and actuators - Decision making algorithms - Functions - In-vehicle communication components - In-vehicle communication networks - Information - Humans - Mobile devices
Outages (Smart cars Infrastructure and Backend systems)	Loss of GNSS signal	GNSS jamming[74] that may be either performed by the smart car legitimate user (e.g. to fraud GNSS tolls, avoid tracking mechanisms) or by an external attacker aiming to disrupt the proper functioning of the vehicle.	- Decision making algorithms - External communication components - Servers, systems and cloud computing - Information - Humans - Mobile devices
	Car depleted battery	This threat aims to partially or completely drain the smart car battery (e.g. through the use of a malware). The attacker's goal is to decrease the overall performance of a car, or immobilize it.	- Functions - Humans - Mobile devices
	Network outage	This threat aims to bring down internal (e.g. CAN bus) and/or external (e.g. C-V2X) networks so that the vehicle cannot operate normally. Such attacks can arise from improper configurations (e.g. CAN bus overload due to multiple applications accessing data at the same time) or from targeted attacks (e.g. DDoS).	All assets

[74] See "Jamming and Spoofing Attacks: Physical Layer Cybersecurity Threats to Autonomous Vehicle Systems": https://tlpc.colorado.edu/wp-content/uploads/2016/11/2016.11.21-Autonomous-Vehicle-Jamming-and-Spoofing-Comment-Final.pdf

Threat Category	Threat	Description	Impacted Assets
Legal	Failure to meet contractual requirements	Breach of contractual requirements by Tier 1 and/or Tier 2 car components or software suppliers. Such threat may lead to financial, safety, privacy and/or operational impacts.	All assets
	Violation of rules and regulations/Breach of legislation/ Abuse of personal data	Lack of compliance with international or European regulations and laws (e.g. GDPR and UNECE regulations). Such threat may have an impact on users' privacy (e.g. disclosure of user's personal information) or road users' safety (e.g. no eCall feature). In particular, the abuse of personal data consists in compromising sensitive and private data (e.g. authentication credentials, name and address, daily commutes) stored in the smart cars or in OEM/service providers backend servers. The attacker's main goal is to retrieve individuals' private information in order to sell it, or even use it for another attack vector (e.g. social engineering, phishing).	All assets

ANNEX C: SECURITY MEASURES MAPPING

Security Domain	Security Measures/ Good Practices	Threat Groups	References
Security by design	**Adopt a Security by Design Approach.** Treat automotive cybersecurity as a cycle, and not as a one-off process. Take into consideration cybersecurity aspects in any activity of the development of the solution from the very beginning. Adopt security by design approach both from the vehicle as well as from the infrastructure perspective. In particular, the secure design should demonstrate how the vehicle security covers the threats identified in the risk assessment. Design should also take into account cybersecurity key principles such as defence in depth, principle of least privilege, disabling of test/debug features and ports, etc. Regarding critical services, more resilient/advanced solutions, such as hardware-supported Trusted Computing Base (TCB), may be used.	All	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles: Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -Safety First for Automated Driving -US Department of Transportation - Cybersecurity Best Practices for Modern Vehicles -SCOUT - Report on the state of the art of connected and automated driving in Europe -PAS 1885:2018 The fundamental principles of automotive cyber security specification, bsi

Security Domain	Security Measures/ Good Practices	Threat Groups	References
Security by design	**Address security in relevant specification documents.** In each design document, include a chapter that addresses the security of all information and control systems in the smart vehicle and the corresponding infrastructure. This ensures that security aspects are considered from the very begining of the concept phase, and not as an afterthought.	All	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles: Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -Safety First for Automated Driving -GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines - Overview Document -US Department of Transportation - Cybersecurity Best Practices for Modern Vehicles -SCOUT - Report on the state of the art of connected and automated driving in Europe
Security by design	**Promote the use of DevSecOps methodology.** The DevSecOps process aims at merging the security discipline within DevOps, thus considering security in every stage of the development process. By having security and development teams working together early in the development lifecycle, security naturally finds itself in the product by design.	All	-Autonomous DevSecOps: Five Steps to a Self-Driving Cloud (ENT214-S) - AWS re:Invent 2018 -Redhat DevSecOps -What is DevSecOps? Developing more secure applications -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Security by design	**Consider including a security role within the product engineering team.** Bring Information Technology (IT) / Operational Technology (OT) people, including people in charge of security topics, together in all phases. Making security an equal consideration alongside	All	-PAS 1885:2018 The fundamental principles of automotive cyber security - Specification -Autonomous DevSecOps: Five Steps to a Self-Driving Cloud (ENT214-S) - AWS re:Invent 2018 -Security Champions Playbook -Avoid Unnecessary Pain with a Security Champion

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	development and operations is a must for any stakeholder of the supply chain.		
Privacy by design	**Consider applying privacy regulations.** OEMs and all third parties should address privacy related issues based on applicable local and international regulations such as the GDPR. To meet privacy-related regulatory requirements, several privacy-preserving rules should be followed such as defining the purpose of private data processing, only collecting a minimal amount of personal data and avoid collecting private data if they are not necessary. Privacy protection accountability aspects should be taken into account, enabling OEMs, Tier 1 and Tier 2 to demonstrate the implemented measures and their effectiveness.	• Legal	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -Safety First for Automated Driving -SCOUT - Report on the state of the art of connected and automated driving in Europe -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Privacy by design	**Conduct PIA.** Autonomous vehicles may collect private information about the owner and/or passengers of the vehicle for a variety of purposes (e.g. authorization, comfort customization, entertainment settings), thus PIA need to be conducted in line with GDPR requirements to identify any potential privacy related risk and define appropriate countermeasures to mitigate it.	• Nefarious activity/abuse • Legal	-GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview -IoT Alliance Australia - Internet of Things Security Guidelines v1.2 -Privacy Impact Assessment -Data Protection Impact Assessment (DPIA)

Security Domain	Security Measures/ Good Practices	Threat Groups	References
Privacy by design	**Perform Privacy Audits.** Perform privacy audits during smart car development and over back-end systems that focus on how individuals' private data are handled, collected, stored and processed, to ensure compliance with privacy-related policies. Privacy audits should be performed on a regular basis, at least once a year or even more frequently depending on PIA.	• Nefarious activity/abuse • Legal	-GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview -IoT Alliance Australia - Internet of Things Security Guidelines v1.2 -GDPR: How to Perform a Data Audit -GDPR checklist for data controllers
Asset management	**Use tools supporting asset management.** Asset management systems should be robust. Used asset management tools should be able to dynamically discover, identify and enumerate assets specific to the organization and smart cars ecosystem.	• Nefarious activity/abuse • Hijacking • Failures/Malfunctions	-Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance Cloud Security Alliance - Security Guidance for Early Adopters of the - Internet of Things -IEC - IEC 62443-3-3:2013 System security requirements and security levels -ISO - ISO/IEC 27001:2013 Information technology -- Security techniques – Information security management systems -- Requirements -ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls -NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations -NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile -SANS Institute - Vulnerability Management: Tools, Challenges and Best Practices -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification

Security Domain	Security Measures/ Good Practices	Threat Groups	References
Asset management	**Ensure that there exists a consistent and up-to-date asset inventory.** This inventory should include, among others, current firmware/operation system (OS) version, used hardware, supported communication protocols, etc. Asset inventory should also include gathered known vulnerabilities related to particular assets. The responsibility for maintaining an up-to-date asset inventory should be clearly defined and assigned to the system owner.	• Nefarious activity/abuse • Hijacking • Failures/Malfunctions • Physical attacks	-Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things -Huawei - IoT Security White Paper 2017 -IEC - IEC 62443-3-3:2013 System security requirements and security levels -NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Asset management	**Introduce a new device or software change into the vehicle only according to an established, accepted and communicated change management process.** Do not allow any changes or introduction of a new device or software unless designated approvals are received. Approved changes should be documented and the relevant documentation updated. Emergency changes may be carried out based on a verbal approval from the Change Management Committee Head and the system owner. However, post emergency, the standard procedure for documenting the change and risk analysis is to be applied.	• Nefarious activity/abuse • Hijacking • Unintentional damages • Physical attacks	-IEC - IEC 62443-3-3:2013 System security requirements and security levels -ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls -LNS - Putting Industrial Cyber Security at the top of the CEO agenda -NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations -NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification

Security Domain	Security Measures/ Good Practices	Threat Groups	References
Risk and Threat management	**Adopt an approach to risk management dedicated to the automotive sector.** The approach to risk management should consider new parameters, threats and attack scenarios targeting smart cars ecosystem, and cover all interdependencies between cyber-physical scenarios, cyber-physical environmental and safety during the assessment phase.	All	-ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls -NIST - NIST SP 800 30r1 - Guide for Conducting Risk Assessments -NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations -NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security -NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile -PAS 1885:2018 The fundamental principles of automotive cyber security – Specification
Risk and Threat management	**Risk and threat analysis.** Perform risk and threat analysis involving cybersecurity experts from the very early stages of the design process of the vehicle to identify critical assets as well as security risks and associated mitigations. Cybersecurity risks targeting smart cars should be assessed and prioritized to establish efficient security measures. Risk and threat analysis should be revisited at least annually, and upon any major change or in case of critical security vulnerabilities detection or critical security incidents.	All	-PAS 1885:2018 The fundamental principles of automotive cyber security - Specification -Safety First for Automated Driving -European Commission -- Access to In-vehicle Data and Resources -US Department of Transportation - Cybersecurity Best Practices for Modern Vehicles - ETSI TR 102 893: Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)

Security Domain	Security Measures/ Good Practices	Threat Groups	References
Risk and Threat management	**Monitor security vulnerabilities.** Once a vehicle is on the market, the OEM should consider the monitoring of security vulnerabilities and fix security flaws accordingly. The vulnerabilities monitoring could include developer findings, on-line researches, CSIRTs advisories, as well as input from customers and security researchers. Vulnerabilities monitoring should be regularly performed, for instance every 6 months or even more frequently based on risk assessment.	All	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -Safety First for Automated Driving -SCOUT - Report on the state of the art of connected and automated driving in Europe -ENISA - Cyber Security and Resilience of Smart Cars -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Risk and Threat management	**Penetration testing.** Conduct security evaluations (e.g. penetrations tests) during the development phase and then on a regular basis following an event driven approach, e.g. after major updates or in the case of new threats or vulnerability. Such testing should cover all layers of the smart cars. To facilitate evaluations, frameworks for validation and verification from external laboratories should be provided.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis -Safety First for Automated Driving -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Risk and Threat management	**Consider defining a threat intelligence process.** Consider incorporating a threat intelligence process within the threat management approach of automotive organisations in order to be informed on emerging attack types and sources, as well as new relevant vulnerabilities.	All	-Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary -Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things -GSMA (Global System for Mobile Communications) - GSMA CLP.14 IoT Security Guidelines for Network Operators -Huawei - IoT Security White Paper 2017

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	Organizations should rely on various sources of information (e.g. other OEMs, specilized entities, CWE and CVE common sources, etc.) and share information with trusted industry partners, ISACs and CSIRTs. Determine the impact of threats detected through the threat intelligence process by performing a risk analysis.		-IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use -International Telecommunications Union - Security capabilities supporting safety of the Internet of things -NIST - NIST SP 800 30r1 - Guide for Conducting Risk Assessments -NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations
Risk and Threat management	**Regularly assess the security controls and patch vulnerabilities.** Smart cars actors should define appropriate assessment procedures to regularly check, at least once a year or more frequently based on risk assessment or patch deployment, the effectiveness of their security measures, and patch them whenever needed. Patches should be tested before deployment.	All	-ENISA - Cyber Security and Resilience of smart cars -UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -Five Star Automotive Cyber Safety Program -Securing the Modern Vehicle -Security Development Lifecycle (SDL) -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Risk and Threat management	**Regularly check the security assumptions over smart cars lifecycle.** Assumptions are made to ensure that the security requirements are sufficient based on risk and threat analysis. These assumptions include, but are not limited to, operational environment assumptions, limitations in the usage of the vehicle, assumed properties of cryptographic schemes, etc. Vendors and users should be encouraged to regularly check, for	All	-ENISA - Cyber Security and Resilience of smart cars -UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -Five Star Automotive Cyber Safety Program -Securing the Modern Vehicle

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	instance every 6 months or even more frequently based on risk assessment, that these assumptions are still valid over smart cars lifecycle. Security assumptions need to be updated according to significant systems changes/updates, support of new technologies and/or communication mechanisms/technologies, etc. In particular, a procedure for communication and handling of end of life/out of warranty status for cybersecurity may be defined.		
Relationships with suppliers	**Foster security-related information sharing between the different stakeholders while protecting intellectual property.** Suppliers and service providers should provide evidences about the implementation of their cybersecurity management system to a vehicle manufacturer, as stated in UNECE regulation. For transparency purposes, OEMs should consider providing similar evidences to their suppliers and service providers as well.	All	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -COLLABORATION AND ENGAGEMENT WITH APPROPRIATE THIRD PARTIES -Auto ISAC - Automotive Cybersecurity Best Practices -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Relationships with suppliers	**Define cybersecurity relevant aspects of the partnerships along the supply chain, and develop security requirements and procurement guidelines for suppliers.**	• Nefarious activity/abuse • Failures/Malfunction • Unintentional damages	-Auto ISAC - Automotive Cybersecurity Best Practices -UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -European Commission -- Access to In-vehicle Data and Resources

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	To prevent security risks and threats that may stem from outsourced services or components/systems provided by third party suppliers, organisations should define procurement guidelines as well as security requirements to be applied to their third parties suppliers. A security SLA may also be established between the organisation and its supplier to define the security level that the the supplier should meet.		-PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Training and awareness	**Information sharing between different actors.** All organisations, including sub-contractors, suppliers and third parties should work together to enhance the security of smart cars. Organisations should consider communicating with other companies on a sector level including the supply chain and participate in international security events and working groups formed to enable discussion, cooperation and intelligence sharing across organisations to improve security awareness.	All	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -European Commission -- Access to In-vehicle Data and Resources - Auto ISAC - Automotive Cybersecurity Best Practices -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Training and awareness	**Adopt a holistic approach to security training and awareness among the employees, including employees on all levels of the organization.** Security training should cover smart cars relevant threats and be tailored to the employees' roles and responsibilities and the different	• Nefarious activity / Abuse • Unintentional damages	-ENISA - Good practices for Security of Internet of Things in the context of Smart Manufacturing -IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program -ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls -NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	level of knowledge of the participants. For instance, all newly hired employees and employees that change responsibilities should be provided with an appropriate cybersecurity training when starting their new job.		Information Systems and Organizations -NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security -NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile -World Economic Forum - Industrial Internet of Things: Unleashing the Potential of Connected Products and Services -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Training and awareness	**Ensure that security trainings are continuous, regular and frequently updated.** Training programs should be updated after new important threats disclosure and adjusted according to the lessons learned from ongoing incident handling and recovery activities.	• Nefarious activity / Abuse • Unintentional damages	-ENISA - Good practices for Security of Internet of Things in the context of Smart Manufacturing -Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance -Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things -IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program -ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls -NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security -NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile
Training and awareness	**Raise vehicle users' awareness.** Vendors and public authorities should explain to vehicle owners, drivers and passengers which actions can contribute to mitigate potential threats, such as how to securely use interfaced systems such as smartphones and onboard tablets,	• Nefarious activity / Abuse • Unintentional damages	-ENISA - Cybersecurity and resilience of smart cars -Insecurity in the Internet of Thing -IoT Security Awareness -Consumers don't care if their connected car can get hacked - here's why that's a problem

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	basic security best practices, etc. This should be done on a regular basis, especially when significant changes/patches occur or when new threats emerge.		-Shifting gears in cyber security for connected cars
Security management	**Consider establishing a Security Operation Center (SOC).** Consider the creation of a SOC consisting of OT and IT cybersecurity specialists with clearly defined roles, responsibilities and cybersecurity competences to centralize knowledge on cybersecurity, monitor and anticipate potential threats by ensuring that potential security incidents are correctly identified, investigated and reported. Managing and acting upon the growing number of security alerts can become very complex, especially for large fleets. Therefore, a robust SOC is needed to ensure all alerts are analyzed and handled properly.	All	-ENISA - Good practices for Security of Internet of Things in the context of Smart Manufacturing -Security Operations Center -MITRE :Cybersecurity Operations Center
Security management	**Designate one or several dedicated security team(s).** As dealing with cybersecurity issues requires a very narrow set of skills, actors of the smart car industry should rely on specialists to perform several kinds of activities, notably risk management, secure design, training and awareness, penetration testing and corporate security. Whether this security team(s) should be in-house or a third-	All	-ENISA - Cybersecurity and resilience of smart cars -Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practices -30% of Automotive Companies Lacking a Dedicated Cybersecurity Team

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	party company is not indifferent in some cases; in particular, risk management and corporate security require a very good knowledge of the company to be easily outsourced.		
Security management	**Define a dedicated Information Security Management System (ISMS).** Vehicles in the wild cannot be completely protected if the company itself is not able to properly protect critical assets. For example, if vehicles or components have keys injected during production, the risk of leaking these keys may be more important on the company site than on the vehicles side. For this reason, an effective ISMS is of utmost importance. The SAE J3061 describes such an ISMS, and provides references to standards often used for this purpose (ISO 27001 and NIST 800-53).	All	-ENISA - Cybersecurity and resilience of smart cars -NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations -SAE J3061
Security management	**Consider defining an internal task force involving board-level management to guide security-related strategic decisions.** OEM should consider the definition of an internal task force which should gather on a regular basis, e.g. once every 3 months or more frequently when necessary, to discuss security-related strategic decisions. Board-level management shall be involved in this task force so as to discuss	All	-Avoid Unnecessary Pain with a Security Champion -Security Champions Playbook

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	the different topics and make appropriate decisions. Such approach would help with accountability in case of security incidents.		
Incident management	**Establish an incident handling process**. Establish a process for incidents handling that enables the identification of affected assets, identification and classification of vulnerabilities, escalation and notification. Make a revision of the process at least annually and as soon as possible in case of a major change, e.g. change in organizational hierarchy, contracts, etc. Update the process with lessons learned from analysing and resolving security incidents. Test the process at least annually and consider different possible incidents.	All	-Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary -Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance -ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls -NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations -NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security -NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile -SANS Institute - Vulnerability Management: Tools, Challenges and Best Practices -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Incident management	**Consider establishing a CSIRT and a PSIRT.** OEMs and third-party suppliers/providers (i.e. Tier 1and Tier 2) should consider building a CSIRT and PSIRT. Working closely with the SOC, the CSIRT and PSIRT ultimate goal is to minimize and control the damage resulting from an incident. They do not only consist in addressing the threat itself,	All	-Cybersecurity Best Practices for Modern Vehicles – NHTSA -CSIRTs in Europe -Cybersecurity Best Practices for Modern Vehicles

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	but also communicate to customers, the organisation board, and public relevant information about the incident.		
Incident management	**Incident Report to back-end servers.** OEMs and third party providers should implement cybersecurity monitoring and reporting to back-end servers to ensure systems are secure over their lifetime. Incident reporting enables the correction of the situation, and through incident analysis and corrective action, similar incidents are avoided.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking	UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security
Incident management	**Relevant cyber incidents definition and classification.** Consider defining cybersecurity incidents relevant for your organisation based on the company's area and range of operation and classify them according to applicable standards. By ensuring the distinction between specific attack vectors and methods, the effects such incident may produce on the targeted networks, the financial impacts or their broader effects on society, it will be easier to identify the most critical incidents, prioritise and respond to them in an efficient way.	All	-ENISA - Good practices for Security of Internet of Things in the context of Smart Manufacturing -Survey and Classification of Automotive Security Attacks – MDPI -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Incident management	**Consider the establishment of a secure and reliable process for detecting and handling misbehaving ITS stations.**	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -PRESERVE - Security Requirements ofVehicle Security Architecture v1.1

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	ITS-S (e.g. vehicle) can misbehave, either unintentionally due a system failure or intentionally as a result of malicious actions, and thus disrupt other vehicles and/or infrastructure. To prevent this, consider the establishment of a process enabling to collect information provided by ITS Stations (e.g. through cooperation between the infrastructure and other vehicles), detect and handle any misbehavior. For instance, the credentials of misbehaving ITS-S may be revoked.		-ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis -C-ITS Platform, WG5: Security & Certification - Final Report - Annex 2: Revocation of Trust in C-ITS (https://smartmobilitycommunity.eu/sites/default/files/Security_WG5An2_v1.0.pdf)
Detection	**Deploy Intrusion Detection Systems (IDS) at vehicle and back-end levels.** An IDS is a device or software application designed to automatically detect malicious activities or policy violations. An IDS should be able to detect various types of cyber-attacks (e.g. DDoS). To do so, the IDS requires the ability to capture and do a thorough examination of every packet which has been received or transferred between vehicles and infrastructures, as well as packets exchanged over in-vehicle buses. Such systems can rely on artificial neural networks to classify malicious vehicles and sensors and exclude them from communicating with the system.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks	-PRESERVE - Security Requirements ofVehicle Security Architecture v1.1 -Safety First for Automated Driving -SCOUT - Report on the state of the art of connected and automated driving in Europe
Detection	**Maintain properly protected audit logs.** Security events must be logged, and	• Nefarious activity / Abuse	-ENISA - cybersecurity resilience of smart cars -UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	access to the logs must be documented and protected from disclosure to unauthorized users. Logs are also needed for device integration. Typically, Tier-2 suppliers must provide Tier-1 suppliers with the opportunity to understand security events happening in their products. However, logs may also provide valuable information to an attacker, which is a serious security drawback. For this reason, the audit trail must be protected. Since logs can be very resource-intensive and require a large storage space, OEMs should define where to store them (i.e. in the car or on a back-end server) and how long the stored data should be retained.	• Failures/Malfunctions • Hijacking • Physical attacks • Unintentional damages • Outages	and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -ACEA Principles of Automobile Cybersecurity -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Detection	**Conduct periodic reviews.** Consider periodically reviewing network logs, access control privileges and asset configurations to detect any event that may represent a potential security threat to smart cars ecosystem.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks • Unintentional damages • Outages	-Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things -ENISA - Baseline Security Recommendations for IoT -IEC - IEC 62443-3-3:2013 System security requirements and security levels -IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices -IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines -NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security -NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks -OWASP (Open Web Application Security Project) - IoT Security Guidance

Security Domain	Security Measures/ Good Practices	Threat Groups	References
			-SANS Institute - An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity
Detection	**Perform data validation.** Data validation techniques, such as plausibility checks are non-cryptographic measures which use rules and other mechanisms to determine the correctness likelihood of received data. For instance, AI-based techniques can be used to measure the likelihood of incoming information (e.g. node misbehaviour detection using machine learning based detector, "object existence" metrics) to counter spoofing attacks on V2X communications or malicious alteration of the physical world (e.g. fake speed limit sign).	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Unintentional damages	-“My autonomous car is an elephant”: A Machine Learning based Detector for Implausible Dimension -Safety First for Automated Driving -ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Detection	**Define forensic procedures.** OEMs should define forensics procedures for incident investigation so as to enable events reconstruction, facilitate crash investigation, identify the leveraged weakness and prevent similar attacks, as well as for accountability purposes. Such procedure should follow proven principles to ensure that reconstructed traces are authentic, have not been altered and can be analysed.	• Nefarious activity / Abuse • Failures/Malfunctions • Threats against (semi-) autonomous systems • Unintentional damages • Outages • Legal • Physical attacks	-A survey on open automotive forensics -ENISA - Cyber Security and Resilience of Smart Cars -Log your car: the non-invasive vehicle forensics

Security Domain	Security Measures/ Good Practices	Threat Groups	References
Protection of networks and protocols	**Protect remote monitoring and administration interfaces.** The protection of remote monitoring and administration interfaces is crucial since they often provide a highly-privileged entry point into a device. Thus, monitoring and administration interfaces must not only be protected by whitelisting, but also through mutual authentication and access control mechanisms. This protection includes access control for both the gateway and ECU level and authentication mechanisms.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking	-ENISA - Cyber Security and Resilience of smart cars -AUTOMOTIVE WORKING GROUP
Protection of networks and protocols	**Protect in authenticity and integrity all critical internal communications.** Authentication is essential to prevent spoofing or replay attacks. At the sensor level, authentication mechanims can be used to allow ECUs/TCUs to authenticate each other over the CAN bus before reacting on their commands or sensor data.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -PRESERVE - Security Requirements of Vehicle Security Architecture v1.1 -Safety First for Automated Driving -European Commission -- Access to In-vehicle Data and Resources -SCOUT - Report on the state of the art of connected and automated driving in Europe
Protection of networks and protocols	**Protect in authenticity and integrity all external communications.** Authentication is essential to prevent spoofing or replay attacks. Regarding V2V and V2X communications, authentication is crucial to ensure the trustworthiness of incoming/outgoing information.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -PRESERVE - Security Requirements of Vehicle Security Architecture v1.1 -European Commission -- Access to In-vehicle Data and Resources -SCOUT - Report on the state of the art of connected and automated driving in Europe

Security Domain	Security Measures/ Good Practices	Threat Groups	References
Protection of networks and protocols	**Enforce session management policies to avoid session hijacking.** Session management contributes to making sure that the authorized user is the one using a given session. This covers the different communication sessions such as administration sessions. Typically, the following rules should be followed: • Sensitive functions such as administration via web services should require re-authentication. • No data should be transmitted before authorization. • Strong (random) session handlers should be used to avoid replay. • The user must know at any time if, and why, they are logged on a particular service, meaning that no passive sign-up for third party services should be performed.	• Nefarious activity / Abuse • Hijacking	-ENISA - Cyber Security and Resilience of smart cars -OWASP: Session Management Cheat Sheet Session fixation
Protection of networks and protocols	**Timestamp all messages.** Including a timestamp in all messages makes it easier for a receiving ITS-S to judge whether a message is recent, and thus valid (or not). It also prevents replay attacks. If the time is derived from an external source such as Universal Coordinated Time (UTC) or GNSS, it should be	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking	-PRESERVE - Security Requirements of Vehicle Security Architecture v1.1 -ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	ensured that each ITS-S uses the same time source as every other ITS-S. Consequently, it is quite simple for the plausibility of the timestamp in a message to be validated. The use of a precision timing source (e.g. hardware clock source, NTP) to provide accurate time may be considered as well.		
Protection of networks and protocols	**Manage radio spectrum frequencies as well as the frequency of beaconing and other repeated messages.** The use of beaconing messages in V2V/V2X communications and the repetition of some non-beacon messages generates considerable background radio traffic in high-density road-traffic environments. In order to prevent DDoS attacks, consider reducing the frequency of the beacon and other safety-of-life messages in order to reduce congestion. Adaptive frequency control, where messages would be sent at different frequencies depending upon the nature of the message and potentially other local conditions, may be a good alternative as well.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks	-ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis -PRESERVE - Security Requirements of Vehicle Security Architecture v1.1
Protection of networks and protocols	**Implement frequency agility.** A radio transmission broadcast at the same frequency at all times can be easily overwhelmed by a higher-power signal at	• Nefarious activity / Abuse • Hijacking	-ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	the same frequency. However, it is much more difficult to jam a transmission in which the radio frequency changes frequently within its defined band. If the changes in frequency and the intervals between changes are both determined on pseudo-random basis, it becomes even more difficult to jam the signal. There needs to be synchronization between the legitimate transmitter and the receiver, and both need to use the same algorithms for determining frequency steps and the intervals between changes in frequency.		-CAR 2 CAR Communication Consortium - FAQ regarding Data Protection in C-ITS v1,0,0
Protection of networks and protocols	**Packet filtering.** Filter communications at each network layer: ECU and sensor networks, VANET, 2-5G communications. During network communication, a node transmits a packet that is filtered and matched with predefined rules and policies. Once matched, a packet is either accepted or denied.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -SCOUT - Report on the state of the art of connected and automated driving in Europe
Protection of networks and protocols	**Provide end-to-end protection in confidentiality and integrity using secure protocols.** Favor methods providing forward secrecy whenever possible. This should be true even for the communication of already encrypted data; encryption must cover not only external communications (e.g. V2X), but also in-vehicle networks.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking	-ENISA - Cyber Security and Resilience of smart cars -ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis -European Commission -- Access to In-vehicle Data and Resources

Security Domain	Security Measures/ Good Practices	Threat Groups	References
Software security	**The default configuration of devices and services should be secured.** The operation mode of the device (or service) should be the most secure one by default. A user might arguably want to disable a given security function, but this should be the consequence of a deliberate action from the user, and the user should be warned that this change reduces the security of the solution. Default passwords and usernames be changed on first use (of the vehicle, service, etc).	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Unintentional damages	-ENISA - Cyber Security and Resilience of Smart Cars -Secure Device Configuration Guideline -Cybersecurity Best Practices for Modern Vehicles -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Software security	**Software authenticity and integrity checked before installation.** By validating the authenticity and integrity of software it is possible to ensure that only authorized updates and extensions can be downloaded and installed. Mechanisms for restricting the applications that can be installed should be in place. In general, a signature is included over the application package together with a certificate of the signing trusted third party.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking	-ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Software security	**Implement and document changes in configuration according to a change management policy developed by the organisation based on risk analysis.** This policy should include responsibility (i.e. system owner, approvers, etc.) and	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks	-IEC - IEC 62443-3-3:2013 System security requirements and security levels -ISA - ANSI/ISA-95 Part 1: Models and Terminology -ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements -NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	security aspects. The business owners of assets should approve all changes.		Information Systems and Organizations -NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security -NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor
Software security	**Use of secure OTA firmware updates.** OTA updates are essential to patch vulnerabilities identified once vehicles are in the field. They should rely on strong authentication mechanisms (e.g. digital signature) to ensure the authenticity and integrity of the firmware to prevent the installation of rogue firmware and the spread of malwares. Rollback to vulnerable versions should be prevented as well. Encryption is also a good practice to prevent binaries analysis in order to protect the IP and the discovery of zero-day vulnerabilities.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Unintentional damages	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practices -Gowling WLG & UK Autodrive - Connected and Autonomous Vehicles: A Hacker's Delight? -SCOUT - Report on the state of the art of connected and automated driving in Europe -Safety First for Automated Driving -European Commission -- Access to In-vehicle Data and Resources
Software security	**Protect OTA update process.** Because poorly executed OTA updates can result in malfunctioning vehicles and significant inconvenience to consumers, as well as reputational damage to the OEM, dedicated security measures should be implemented to ensure a secure OTA update process. Access controls to OEM back-end servers as well as recovery measures in case of errors (e.g. reversion	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks • Unintenational damages	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practices -Gowling WLG & UK Autodrive - Connected and Autonomous Vehicles: A Hacker's Delight? -SCOUT - Report on the state of the art of connected and automated driving in Europe

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	if the OTA image fails to boot successfully) should be considered.		-Safety First for Automated Driving -European Commission -- Access to In-vehicle Data and Resources
Software security	**Use of secure boot mechanisms.** Secure boot is essential to ensure the trustworthiness (i.e. authenticity and integrity) of the executed software. Secure boot mechanisms essentially consist in signing the software with a private key owned by the manufacturer. The signature is verified during the secure boot procedure with the help of the corresponding certificate. If verification fails because the software has been altered, the boot process should react accordingly (e.g. run emergency program to guarantee the functional safety of the vehicle).	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Unintentional damages	-Cybersecurity Solutions for Connected Vehicles -Securing Self-Driving Cars -Safety First for Automated Driving -European Commission -- Access to In-vehicle Data and Resources
Software security	**Mitigate vulnerabilities and limitations of libraries for standard protocols, or address them in risk assessment.** Using an open source security library (e.g. OpenSSL) or proprietary software does not mean that the product will automatically be secure. Developers must be aware of the vulnerabilities (e.g. due to a flawed implementation) and limitations (e.g. vulnerability of the protocol itself) of the used software. They should mitigate	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks	-ENISA - Cyber Security and Resilience of Smart Cars -Using Open Source for security and privacy protection

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	them whenever possible by performing patching and by securing the configuration of the communication stacks.		
Software security	**Protect mobile applications against reverse engineering and tampering of their binary code.** Code obfuscation techniques may be used to prevent the reverse engineering of smart cars mobile applications. To enable the detection of the tampering of mobile application binary code, mobile applications should be signed. Root detection mechanisms may be implemented as well to check if the device was rooted.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks	- OWASP – Mobile Application Security Verification Standard - ENISA – Smartphone Secure Development Guidelines
Software security	**Securely store sensitive data on mobile devices, and protect local files created by the mobile application.** No sensitive data (e.g. passwords, credentials, cryptographic keys etc.) should be stored outside the application container or mobile operating system credential storage facility (e.g. Keystore, Keychain). In particular, no sensitive data should be written in application logs. Access to data stored in the credential storage facility should be limited to authorized users. Local files created by the mobile application should also be protected and deleted when no longer needed.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks	- OWASP – Mobile Application Security Verification Standard - ENISA – Smartphone Secure Development Guidelines

Security Domain	Security Measures/ Good Practices	Threat Groups	References
Cloud security	**Include security and availability aspects in agreements with cloud security providers.** Responsibilities for cloud security aspects shall be clearly defined and allocated to particular parties or persons. Availability of service shall be measurable and defined through specified parameters.	• Nefarious activity / Abuse • Outage • Legal	-Federal Office for Information Security (BSI) - BSI-Standards 100-4 - Business Continuity Management -GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems -Online Trust Alliance - IoT trust framework 2.5 -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Cloud security	**Avoid single points of failure.** In the context of cloud-based application and centralised systems, single points of failure should be avoided. Redundancy techniques (e.g. several clusters) and data replication may be used to avoid single points of failure.	• Failures/Malfunctions • Outages	-NIST - NIST SP 800-146 Cloud Computing Synopsis and Recommendations -Online Trust Alliance - IoT trust framework 2.5 -SANS Institute - Building the New Network Security Architecture for the Future -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Cloud security	**Operate critical systems and applications within the private or at least hybrid deployment models.** Privilege the use of a private cloud, or at least a hybrid cloud which combines both private and public cloud. When considering the use of a public cloud, a risk analysis should be performed beforehand.	• Nefarious activity / Abuse • Hijacking • Failure/Malfunctions	-Cloud Security Alliance - Future Proofing the connected world -Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance -Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things -GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT -Online Trust Alliance - IoT trust framework 2.5 -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Cloud security	**To mitigate the risk related to cloud attacks, adopt a zero-knowledge**	• Nefarious activity / Abuse • Hijacking	-Federal Office for Information Security (BSI) - BSI-Standards 100-4 - Business Continuity Management

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	security approach. Cloud services providers should store and manage data without access to the decryption keys. All the data should be protected during transfer as well as when at rest (i.e. stored within the cloud). Ideally, all data should be encrypted to ensure its confidentiality. Application and interfaces should be secured as well.		-IoT Alliance Australia - Internet of Things Security Guidelines v1.2 -ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements -NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations -NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile
Cryptography	**Encrypt sensitive data as well as personal and private data.** Sensitive data include, amongst other, data needed to enforce security such as the configuration, different keys and certificates used for several purposes (e.g. encrypt/sign communications), as well as IP-related data. The disclosure of keys and know-how for instance may be prevented through their encryption. Moreover, authenticated encryption may be used to additionally ensure data integrity. Personal and private data covers all pieces of information that can be used to positively identify a vehicle, an ITS user, the location and behavior of a particular vehicle or its route. By encrypting personal and private data it is possible to ensure that traffic analysis and eavesdropping alone cannot reveal	• Nefarious activity/abuse •Eavesdropping/Interception /Hijacking • Legal	-ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis -CAR 2 CAR Communication Consortium - FAQ regarding Data Protection in C-ITS v1,0,0

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	sufficient information to directly extract or indirectly deduce private information.		
Cryptography	**Do not use proprietary cryptographic schemes and protocols, but rather state-of-the-art standards instead.** Even a home-brewed implementation of a standard is not a good practice when standard implementations are available. If needed, consider getting advice from security experts or your national cybersecurity agency. This applies also to random number generation which is a critical part of the cryptographic support. A possible recommendation would be the use of cryptographically secure pseudorandom number generators.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks • Unintentional damages	-ENISA - Cyber Security and Resilience of smart cars -European Commission -- Access to In-vehicle Data and Resources
Cryptography	**Use storage encryption.** Encrypted storage is not only useful to protect user data, but also to protect data that is needed to enforce smart cars security. Internal data may be just as sensitive as user data, but are often not protected enough, leading for example, to situations where hardcoded root credentials, API keys, URLs never meant to be known to end-users, and manufacturing network configurations are found in cleartext and may be disclosed to unauthorised entities. As a general rule, configuration data should be encrypted at rest and in transit.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Legal	-ENISA - Cyber Security and Resilience of smart cars Safety First for Automated Driving -ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis

Security Domain	Security Measures/ Good Practices	Threat Groups	References
Cryptography	**Implement a secure key management process.** Cryptographic keys should be securely generated, provisioned, used, stored, and deleted/revoked. Badly implemented key management can introduce vulnerabilities that may easily be exploited. Devices without direct user interfaces are particularly vulnerable to PKI compromising. While users can easily delete or install certificates on a PC, embedded devices (e.g. ECUs) rely mostly on remote administration, and do not even allow end-users to perform such administration tasks. For this reason, OEMs as well as Tier-1/Tier-2 should pay careful attention to the key management system, especially when the key provisioning and management are performed over-the-air. If needed, consider getting advice from security experts or your national cybersecurity agency.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks • Unintentional damages	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis -European Commission -- Access to In-vehicle Data and Resources -SCOUT - Report on the state of the art of connected and automated driving in Europe European Commission - Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport System (C-ITS)
Cryptography	**Consider using dedicated and tamper resistant hardware security modules.** HW-based cryptographic solutions may help avoid the incorrect implementation of cryptographic algorithms by software vendors, as well as the coexistence of multiple implementations of the same algorithms. They eventually provide implementations that are more resource-	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks	-Safety First for Automated Driving -UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis -European Commission -- Access to In-vehicle Data and Resources

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	efficient. Choosing HW accelerated cryptography means that a reasonable assurance must be obtained on the quality of the HW implementation, since “bad cryptography” on HW will be leveraged on all the SW using these functions. Devices vendors should be aware of tamper evident or tamper-resistant mechanisms. While they are not mandated in any case, vendors should consider using them depending on the level of sensitivity of the assets stored on the device. In particular, even constrained devices could be able to implement some kind of tamper evidence, even if they are not able to implement resistance and response.		-SCOUT - Report on the state of the art of connected and automated driving in Europe
Access Control	**Application of security controls to back-end servers.** Such controls have to be at different levels: • physical (e.g. physical and environmental security) • logical (e.g. secure configuration using system hardening, firewalls) • people (e.g. security training for OEMs staff)	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -Secure Device Configuration Guideline -IoT Security Awareness -Consumers don't care if their connected car can get hacked - here's why that's a problem -Shifting gears in cyber security for connected cars -What is physical security? How to keep your facilities and devices safe from on-site attackers

Security Domain	Security Measures/ Good Practices	Threat Groups	References
Access Control	**Apply least privileges principle and use individual accounts to access devices and systems.** Ensure that roles (e.g. user, administrator, etc.) are clearly defined and that access rights are provided following a need-to-know/access and least-privilege principles. A distinct account should be created for each user for accountability reasons (i.e. track performed actions).	• Nefarious activity / Abuse • Eavesdropping/ Interception/ Hijacking • Unintenational damages • Physical attack	-Principle of least privilege (POLP) -Improving security through least-privilege practices -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Access Control	**Segregate remote access.** Develop a set of rules for control of remote communication. Remote access should be only limited to the required systems, and must be monitored.	• Nefarious activity / Abuse • Eavesdropping/ Interception/ Hijacking • Unintentional damages • Failures/Malfunctions	-GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems -GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems -NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations -NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks -OWASP (Open Web Application Security Project) - IoT Security Guidance -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Access Control	**Allow and encourage the use of strong authentication mechanisms.** Rely on Multi-factor authentication (MFA) mechanisms which require users to provide at least two different proofs of the claimed identity (e.g. password and security token) so as to be authenticated	• Nefarious activity / Abuse • Eavesdropping/ Interception/ Hijacking • Physical attacks	-Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance -ENISA - Baseline Security Recommendations for IoT -GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems -GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	and granted access to the resource or service (e.g. authentication to cloud services or mobile interfaces, local/remote administration sessions). This mitigates the risks associated with passwords-only authentication. An account lockout functionality should be implemented to automatically lockout an account for a given time period after a number of successive authentication failures.		-IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines -NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations -OWASP (Open Web Application Security Project) - IoT Security Guidance
Self protection and resilience	**Implement differential monitoring on the GNSS system.** Differential GNSS is a way of correcting various inaccuracies in a GNSS system and, thus, providing more accurate position information. The benefit of differential GNSS is that it is capable of positioning things very precisely and this feature can be used to detect even small anomalies in position errors.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking	-ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis - Autonomous integrity monitoring of navigation maps on board intelligent vehicles

Security Domain	Security Measures/ Good Practices	Threat Groups	References
Self protection and resilience	**Perform hardening to reduce the attack surface.** Remove unused services or interfaces, integrate dedicated security software, activate memory or control flow protections. For devices that have a complete operating system, several measures can be considered to harden the device, such as ASLR, non-executable memory, process segregation or sandboxing. Another measure is removing unused tools, services and libraries. Unnecessary services should not be present on the device (typically telnet must always be deactivated, but even SSH or FTP can be deactivated in many cases). This type of measures is also applicable at a network level: the device should not leave open ports, especially ports that could be exposed via plug-n-play protocols. The default configuration of the device should be based upon the most secure parameters, and users should be warned if they have the possibility to roll back to less secure parameters.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks • Unintenational damages	-Cloud Security Alliance - Identity and Access Management for the I+E68nternet of Things - Summary Guidance -ENISA - Baseline Security Recommendations for IoT -GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems -GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems -IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines -NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations -OWASP (Open Web Application Security Project) - IoT Security Guidance
Self protection and resilience	**Reinforce interfaces robustness.** Software can contribute to self-protection measures, such as for robustness of interfaces against bad inputs. Secure implementation, thoroughly tested, will protect against common attack	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking	-ENISA - Cyber Security and Resilience of smart cars -Symantec - Insecurity in the Internet of Things -OWASP Internet of Things Project – OWASP- -OWASP Top Ten Project – OWASP

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	vectors such as buffer/heap overflows or OWASP's Top Ten Web Vulnerabilities. This typically includes robustness of network interfaces against buffer overflows or fuzzing.		-PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Self protection and resilience	**Consider strengthening applications isolation at runtime.** Trusted software technologies, such as Trusted Execution Environments (TEEs), hypervisors and virtualisation, may be used to ensure secure execution of applications in a segregated and trusted environment.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking	-ENISA - Cyber Security and Resilience of smart cars -Symantec - Insecurity in the Internet of Things -Secure hypervisor versus trusted execution environment -Isolated Execution in Many-core Architectures
Self protection and resilience	**System, sub-domain and network segregation.** Use of logical and physical isolation techniques to separate processors (e.g. OS virtualization techniques, hypervisors), vehicle domains and networks (e.g. use of an in-vehicle gateway for physical separation between safety and non-safety related domains), and external connections (e.g. firewall to filter all the incomming traffic received from outside the vehicle). These techniques should be used where appropriate (based on risk assessment) to limit and control pathways from external threat vectors to cyber-physical features of vehicles, as well as ensure suitable separation of in-vehicle systems.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking	-U.S. Department of Transportation - Cybersecurity Best Practices for Modern Vehicles -UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -European Commission -- Access to In-vehicle Data and Resources -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification

Security Domain	Security Measures/ Good Practices	Threat Groups	References
(semi-) Autonomous systems self protection and cyber resilience	**Consider using INS or existing dead-reckoning methods to provide positional data.** In order to have other source of location information in the case of GNSS failure, consider the use of an onboard Inertial Navigation System (INS) or dead-reckoning derived from simple accelerometers such as those found in modern mobile phones. Thus, it would be possible for the ITS-S to determine its position from purely internal sources with only brief and infrequent references to GNSS for waypoint corrections. Such security measure would prevent GNSS jamming and other related attacks.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Outages • Threats against (semi-) autonomous systems	-ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis -An Autonomous Vehicle Navigation System Based on Inertial and Visual Sensors
(semi-) Autonomous systems self protection and cyber resilience	**Protect critical sensors in order to prevent attacks that may alter their perception of the environment.** The protection mechanisms are specific to each sensor type, and mainly depends on the type of threats targeting the sensor. For instance, Integration of near-infrared-cut filters or photocromic lenses on cameras could filter specific types of light to mitigate sensor blindness attacks. Regarding LiDARs, the emission of light pulse could be done in an unpredictable manner (e.g. pseudo-randomly) so that it will be harder for an attacker to inject a fake echoe in the right window.	• Physical attack • Nefarious activity/abuse • Outage • Threats against (semi-) autonomous features/components	-Security Innovation - Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR -SCOUT - Report on the state of the art of connected and automated driving in Europe -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification

Security Domain	Security Measures/ Good Practices	Threat Groups	References
(semi-) Autonomous systems self protection and cyber resilience	**Hardening against Adversarial Machine Learning.** Protect Artificial Intelligence (AI) and Machine Learning (ML) components in order to prevent them from being tricked by adversarial attacks. The model need to be hardened by using, for instance, adversarial data as part of algorithm training, to make the model more robust with regard to adversarial attacks. Pre-processing techniques may also be used as a protection mechanism.	• Threats against (semi-) autonomous systems	-Towards deep learning models resistant to adversarial attacks (https://openreview.net/pdf?id=rJzIBfZAb) -Explaining and harnessing adversarial examples (http://arxiv.org/abs/1412.6572). -Pixeldefend: Leveraging generative models to understand and defend against adversarial examples. In International Conference on Learning Representations (ICLR),2018 (https://openreview.net/forum?id=rJUYGxbCW) -The robust manifold defense: Adversarial training using generative models. (https://arxiv.org/abs/1712.09196). -Thermometer encoding: One hot way to resist adversarial examples. In International Conference on Learning Representations (ICLR), 2018
(semi-) Autonomous systems self protection and cyber resilience	**Prevent data falsification/manipulation in regard to Artificial Intelligence (AI)/Machine Learning (ML).** Ensure that data used to train the model are originating from a trusted entity. After any training cycle, the model should be tested to ensure that there are no considerable changes in classifications for instance.	• Threats against (semi-) autonomous systems	-The robust manifold defense: Adversarial training using generative models. (https://arxiv.org/abs/1712.09196). -Securing the Future of AI and ML
(semi-) Autonomous systems self protection and cyber resilience	**Use of data redundancy mechanisms.** Data redundancy mechanisms (e.g. sensor data fusion) consist in correlating data acquired from different sensors (e.g. LiDAR and camera) and V2X communications so as to allow the mitigation of the physical or DoS attacks against sensors.	• Physical attack • Nefarious activity/abuse • Outage • Threats against (semi-) autonomous systems	-Groupe PSA - Attacker model for Connected and Automated Vehicles Security Innovation - Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR -SCOUT - Report on the state of the art of connected and automated driving in Europe -Safety First for Automated Driving

Security Domain	Security Measures/ Good Practices	Threat Groups	References
(semi-) Autonomous systems self protection and cyber resilience	**Use of hardware redundancy mechanisms.** Hardware redundancy mechanisms consist in duplicating sensors (e.g. several cameras, several sensors to collect the same data) in order to mitigate physical attacks or DoS attacks against sensors.	• Physical attack • Nefarious activity/abuse • Outage • Threats against (semi-) autonomous systems	-Groupe PSA - Attacker model for Connected and Automated Vehicles Security Innovation - Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR -SCOUT - Report on the state of the art of connected and automated driving in Europe -Safety First for Automated Driving
Continuity of operations	**Notifications should be easy to understand and help users find a remediation or workaround.** HW and embedded systems should provide clear error data that can be leveraged upon by the SW vendors. The user must be notified in case of security errors, updates or compromised data in a device or service they use. In particular, users must be notified in the case of security events. Notification might vary greatly depending on the type of software considered. Mobile applications notification, messaging such as SMS or e-mail, hardware interfaces such as LEDs, dedicated error messages to a gateway, etc.	• Nefarious activity / Abuse • Failures/Malfunctions • Unintentional damages	-ENISA - Cyber Security and Resilience of smart cars -Duo Security - The Internet of Fails ; Where IoT Has Gone Wrong -A Hard Problem with No Easy Answers | Decipher - IoT Security
Continuity of operations	**Create a Business Continuity Plan (BCP) and a Business Recovery Plan to ensure the resilience of smart cars systems.** To ensure business continuity (even in the case of security crisis or disaster situations), a Business Continuity	• Failures/Malfunctions • Unintentional damages	-Center for Internet Security (CIS) - Critical Security Controls -Federal Office for Information Security (BSI) - BSI-Standards 100-4 - Business Continuity Management -IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	Plan (BCP) and a Business Recovery Plan that cover third party aspects should be created and periodically tested, at least annually, to ensure their effectiveness and improve them when required. Appropriate Third Party management and control over its involvement is essential to ensure the continuity of operations of the organisation.		-NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations -NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security -NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile
Continuity of operations	**Define Business Continuity parameters.** Define important parameters for business continuity of the organization, such as the recovery time objective (RTO), recovery point objective (RPO), maximum tolerable outage (MTO) and minimum business continuity objective (MBCO).	All	-IEC - IEC 62443-3-3:2013 System security requirements and security levels -IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices -IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines -oneM2M - Standards for M2M and the Internet of Things - TR 0008 Security V2.0.0 - Security. Technical Report

TP-02-19-881-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. ENISA works with the EU, its member states, the private sector and Europe's citizens to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Since 2019, it has been drawing up cybersecurity certification schemes. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-317-9
DOI: 10.2824/17802

CYBENTIA GRUPO

CONSULTORA DE INVESTIGACIÓN, CONCIENCIACIÓN Y COMUNICACIÓN ESTRATÉGICA

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_i] convention and "Technical best practices" elements are enumerated using the [T.n_j] convention, where n_i, and n_i respectively represent the "i^{th}" and "j^{th}" 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

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[1] 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.[2]

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[3] and motor vehicle equipment (including software)[4] 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,

[1] 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.

[2] 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/.

[3] "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).

[4] "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,"[5] 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."[6] 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[7] 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;

[5] National Highway Traffic Safety Administration (2016), *Cybersecurity Best Practices for Modern Vehicles*, available at: https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf.

[6] ISO/SAE 21434:2021 *Road vehicles – Cybersecurity engineering*, available at: https://www.iso.org/standard/70918.html and https://www.saemobilius.sae.org

[7] 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[8]] The automotive industry should follow the National Institute of Standards and Technology's (NIST's) documented Cybersecurity Framework,[9] 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.

[8] Throughout this document, "General best practices" elements are enumerated using the [G.n_i] convention and "Technical best practices" elements are enumerated using the [T.n_j] convention, where ni, and ni respectively represent the "ith" and "jth" element of the general and technical best practices covered in this document.

[9] 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.[10]

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

[10] 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[11] 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,[12] road sign modification,[13] Lidar/Radar jamming and spoofing,[14] camera blinding,[15] and excitation of machine learning false positives.[16]

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.

[11] 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.

[12] 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/

[13] 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/.

[14] Mark Harris, IEEE Spectrum Sept 4, 2015, *Researcher Hacks Self-driving Car Sensors.*

[15] 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.

[16] 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.

4.2.5 Protections

[G.8] For remaining functionality and underlying risks, layers of protection[17] 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.[18]

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[19,20] 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,[21] such that when a newly identified vulnerability is identified related to an open source or off-the-shelf software,[22] 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.[23,24,25]

[G.13] Manufacturers should also pursue product cybersecurity testing, including using penetration tests, as part of the development process.[26]

[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.

[17] See the appendix's Terms and Definitions entry for "Layered Protections"

[18] 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.

[19] 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.

[20] Multistakeholder Process on Promoting Software Component Transparency, 83 Fed. Reg. 110 (June 4, 2018).

[21] These details could include: the licenses that govern those components, the versions of the components used in the codebase, and their patch status.

[22] 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.

[23]MITRE Common Vulnerabilities and Exposures (CVE) may be found at: https://cve.mitre.org/.

[24] NIST's National Vulnerability Database may be found at: https://nvd.nist.gov/ .

[25] ISO/SAE 21434's [RQ-06-21] and clause 6 in general discuss the integration of off-the-self components.

[26] 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.[27]

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.[28]

[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,[29] and this information should be analyzed and shared with industry through the Auto-ISAC and other sharing mechanisms.[30]

[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.[31]

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.

[27] 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].

[28] Described in clause 13 of ISO/SAE 21434, "Operations and Maintenance"

[29] ISO/SAE 21434 clause section 8.3 "Cybersecurity Monitoring" describes monitoring activities and potential sources of information.

[30] For example, US-CERT at the Cybersecurity & Infrastructure Security Agency (CISA)

[31] 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[32] [33] and ISO/SAE 21434.[34]

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),[35] NHTSA began encouraging the industry[36] to create the Auto-ISAC.[37] 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

[32] 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.*

[33] Dodson D., Souppaya M., Scarfone K., *Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework*

[34] ISO/SAE 21434 clause 10 discusses software development practices.

[35] Executive Order 13691 *Promoting Private Sector Cybersecurity Information Sharing* encourages the development and formation of Information Sharing and Analysis Centers.

[36] 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.

[37] 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.[38] [39]

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.[40] This process should include:

[38] 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.*

[39] 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/

[40] 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;[41]

[b] Clearly identified roles and responsibilities within the organization;[42]

[c] Clearly identified communication channels and contacts outside the organization;[43] 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.[44]

[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[45] 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.[46]

[41] 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.""

[42] ISO/SAE 21434's [RQ-05-03] requires that "The organization shall assign and communicate the responsibilities to achieve and maintain cybersecurity."

[43] ISO/SAE 21434 section 8.3 "Cybersecurity Monitoring" and [RQ-08-01] discuss potential external sources of information.

[44] Described in clause 8 of ISO/SAE 21434.

[45] Information can be directed to the Auto-ISAC via analyst@automotiveisac.com.

[46] 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,[47] 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[48] 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[49] [50], 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.[51]

[47] For example, DHS' bi-annual "CyberStorm" exercise. See https://www.cisa.gov/cyber-storm-securing-cyber-space.

[48] NHTSA strongly encourages developing the "work products" described in ISO/SAE 21434.

[49] ISO/SAE 21434's requirement [RQ-05-11] discusses a quality management system that encompasses change management and configuration management.

[50] 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".

[51] 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.[52]

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

[52] 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.[53]

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.[54]

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[55] 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.

[53] NIST regularly updates the Federal Information Processing Standards (FIPS) 140 Series "Security Requirements for Cryptographic Modules" that provides guidance on appropriate cryptographic techniques.

[54] In https://github.com/sgayou/subaru-starlink-research/blob/master/doc/README.md, Scott Gayou describes his efforts to hack an infotainment system.

[55] Miller C., Valasek C., *Adventures in Automotive Networks and Control Units,* 2014, available at: 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.[56]

Public key cryptography techniques are more secure than symmetric keys valid across multiple vehicles.[57]

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.[58]

[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.[59]

8.5 Vehicle Internal Communications

Critical safety messages are those that could directly[60] or indirectly[61] 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.

[56] 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.

[57] Miller C., Valasek C., *Adventures in Automotive Networks and Control Units,* 2014, available at: http://illmatics.com/car_hacking.pdf. The paper describes efforts to discover fixed, universal keys from diagnostic software and use them.

[58] Miller C., Valasek C., *Adventures in Automotive Networks and Control Units,* 2014, available at: http://illmatics.com/car_hacking.pdf.

[59] ISO/SAE 21434 requirement [RQ-05-14] states that "Tools that can impact the cybersecurity of an item, system or component shall be managed."

[60] 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.

[61] 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.[62]

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.[63] 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.

[62] 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.)

[63] 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.

[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,[64] dbus,[65] and the Android Debugger[66] 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.[67]

8.7.5 Capability to Alter Routing Rules[68]

[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

[64] 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/

[65] Miller C., Valasek C., *Remote Exploitation of an Unaltered Passenger Vehicle*, 2015, available at: http://illmatics.com/Remote%20Car%20Hacking.pdf.

[66] Android Debug Bridge description may be found here: https://developer.android.com/studio/command-line/adb

[67] Allgemeiner Deutcher 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/assistenzsysteme/sicherheitsluecken-bmw-connected-drive/.

[68] 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.[69] [70]

[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.[71,72]

[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.

[69] Chen Y. et al. "Downgrade Attack on TrustZone" available at:https://arxiv.org/ftp/arxiv/papers/1707/1707.05082.pdf... CVE-2015-6639

[70] "OnePlus OTA Downgrade Vulnerability" Aleph Research Advisory available at: https://alephsecurity.com/vulns/aleph-2017008

[71] 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/.

[72] 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 be 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.

CYBENTIA®

GRUPO