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

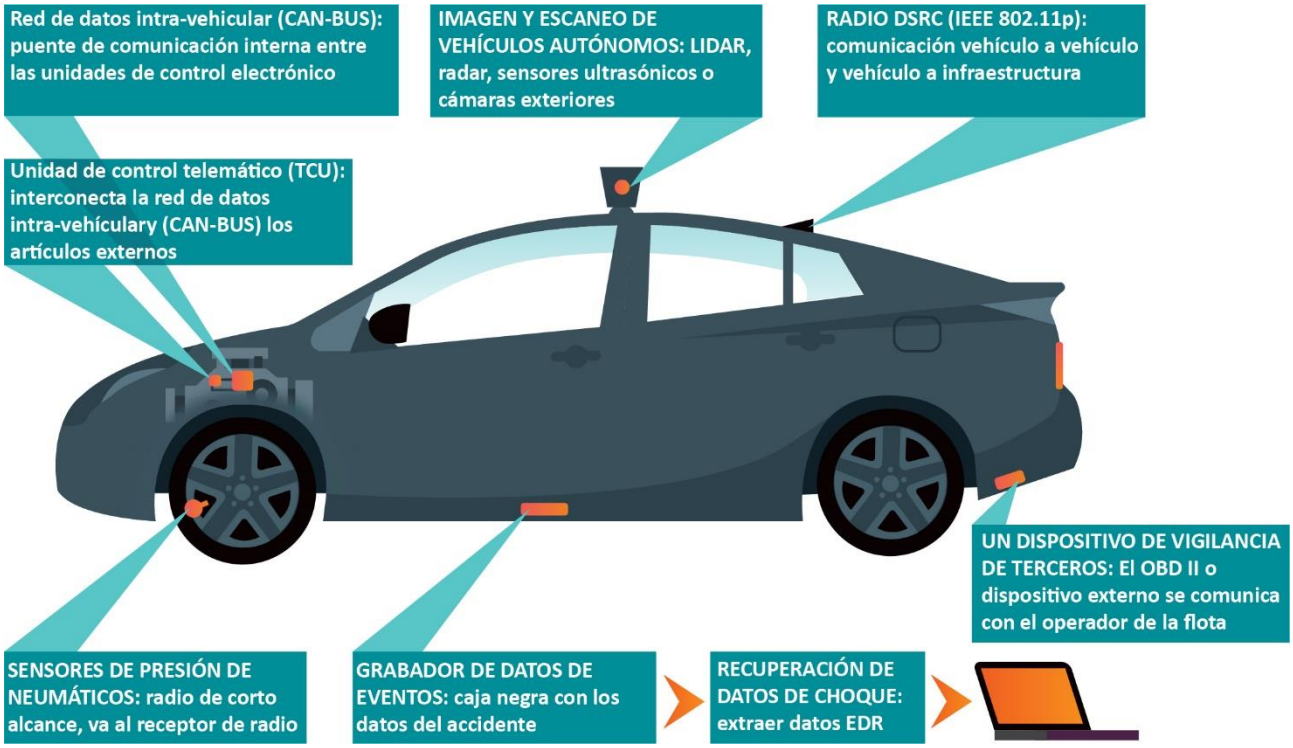


Figura 1: *Vehículo conectado con diferentes funciones*
(Fuente: Foro sobre el Futuro de la Privacidad, modificado)

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

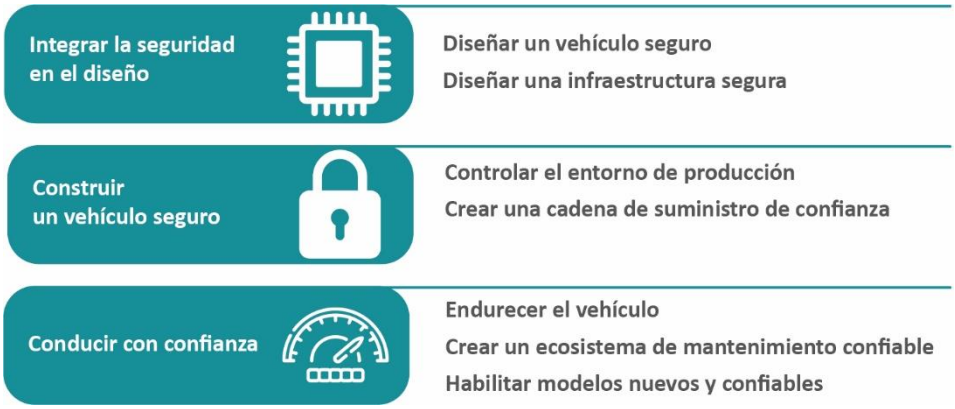


Figura 2: *Enfoque de Diseño, Construcción y Conducción de IBM*[14]
(Fuente: IBM)

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.

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)

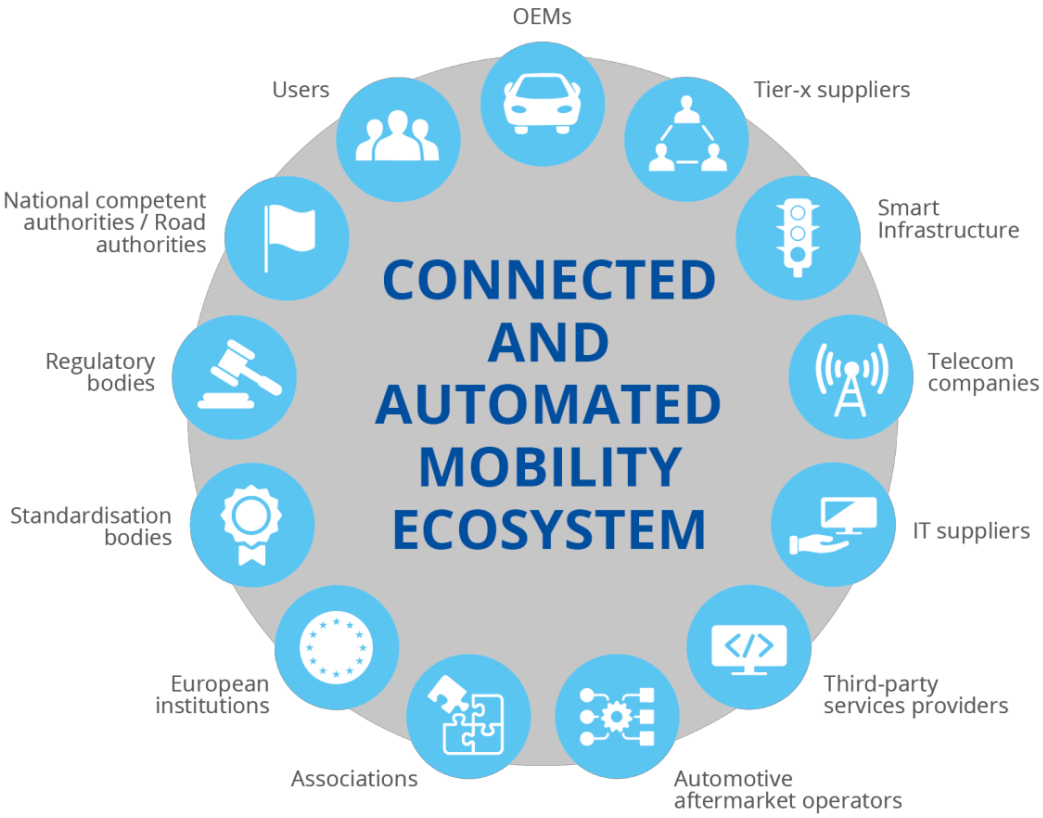
La industria de la Movilidad Conectada y Automatizada (CAM) se basa en un amplio ecosistema de actores que cubren las diferentes áreas de la cadena de valor desde I + D y fabricación, venta minorista y prestación de servicios, operaciones, mantenimiento y gestión de infraestructuras y flotas, así como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



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).

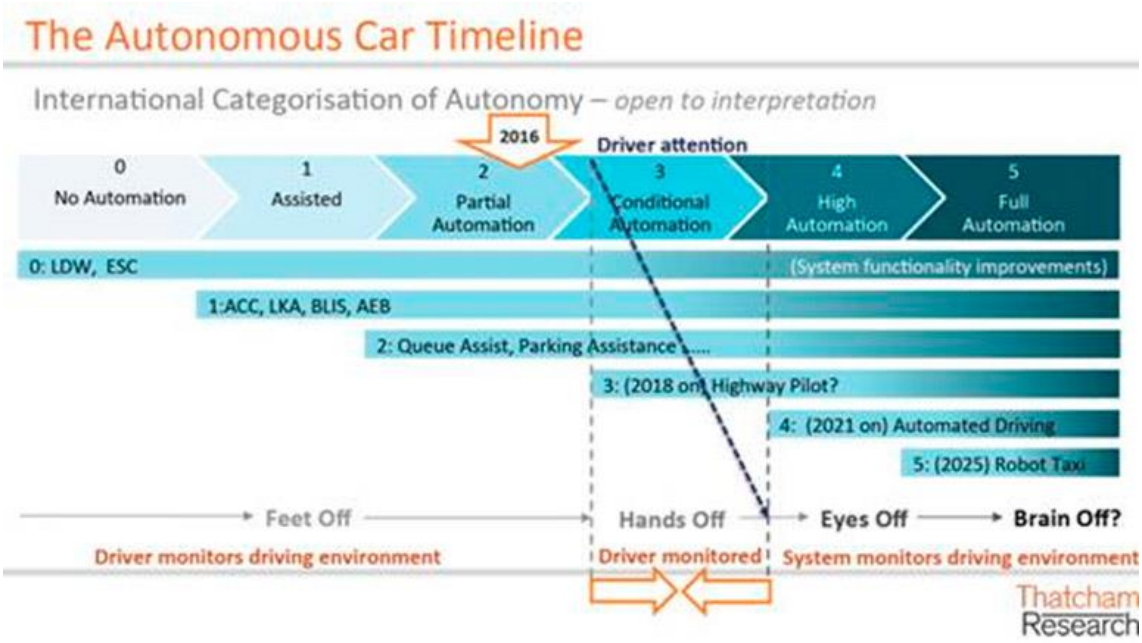


Imagen correspondiente a la: Charla coloquio: "Cómo afectará la conducción autónoma a los conductores"

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 estandarización dentro de IEEE e ISO para definir tecnologías de comunicación para vehículos basados en Ethernet.

De este modo, el estándar **ISO/IEC/IEEE 8802-3:2017** y la familia de estándares **ISO 21111** definen sistemas de comunicación de hasta 1 Gb/s, conectores, cables y pruebas de conformidad concebidos para ser utilizados en el entorno hostil de un vehículo. Pruebas de resistencia en temperatura, torsión, humedad, ataque químico, inflamabilidad, tensiones, repeticiones de ciclos de conexión/desconexión, etc., han sido definidos para garantizar la robustez de las comunicaciones internas en el vehículo.

El hardware en este caso, ya está disponible e implementado en modelos de automóvil que actualmente ruedan en nuestras carreteras.

Sin embargo, los requisitos en cuanto a conectividad de los OEMs siguen creciendo, y ahora los esfuerzos de estandarización se centran en sistemas de comunicación intra-vehiculares con velocidades que llegan hasta los 50 y 100 Gb/s. De este modo, se encuentran en desarrollo los estándares IEEE 802.3cy e IEEE 802.3cz, para sistemas de comunicaciones Ethernet sobre varios cables de cobre apantallados, o sobre fibra óptica para dentro de vehículos de hasta 100 Gb/s.

A lo largo de 2021 se espera que comiencen los esfuerzos de estandarización, en IEC e ISO, para conectores, cables y conformidad para esta nueva ola de comunicaciones dentro del vehículo por encima del 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.

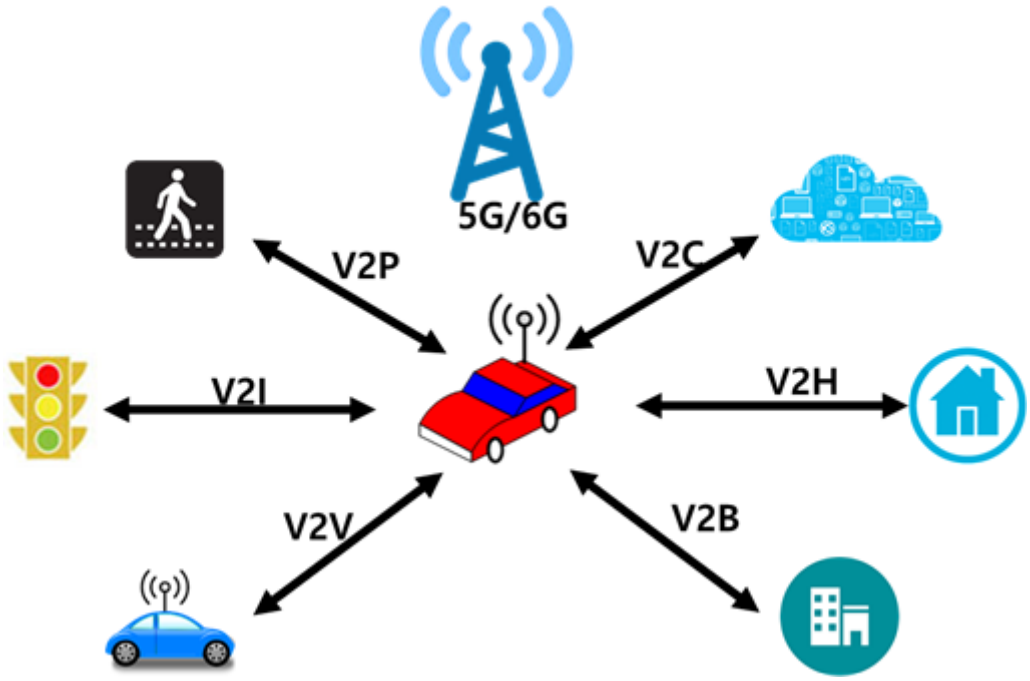
En cuanto a redes intra-vehiculares, el estado de la implementación tecnológica y de la estandardización se encuentra más avanzada.

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. **Estandarizado 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. **Estandarizado en la familia de estándares ISO 17987**.

- **MOST:** Del inglés *Media Oriented Systems Transport*. Se trata de un bus que utiliza fibra óptica plástica (POF) o pares de cobre trenzado. Hay tres tipos de MOST dependiendo de la velocidad máxima que pueden alcanzar. De este modo, MOST25, MOST50 y MOST 150 pueden alcanzar 25, 50 y 150 Mb/s respectivamente. Los dos primeros tipos estaban muy orientados a la distribución de video y audio dentro del coche para sistemas de entretenimiento, mientras que el segundo soportaba el transporte de tramas Ethernet. **Estandarizado en la familia de estándares ISO 21806**.

- **K-Line:** Protocolo de diagnóstico de muy baja velocidad **descrito en las normas ISO 9141 e ISO 14230-1** que se utiliza para conectar un dispositivo externo con el vehículo a través del puerto OBD-II.

- **Ethernet:** Las necesidades cada vez más exigentes de transmitir datos dentro del vehículo dan lugar a la utilización de Ethernet dentro del vehículo, asegurando así una latencia muy baja y alta disponibilidad. Además, su implementación en el vehículo permite la reutilización de protocolos altamente utilizados de forma extensiva en otras redes Ethernet (WiFi, centros de datos, comunicaciones basadas en TCP/IP), incluyendo aquellos de encriptación y autenticación ya desarrollados para redes más extensas. Vehículos que ruedan hoy en carretera utilizan velocidades de hasta 1 Gb/s basadas en fibra óptica plástica (POF) o cable de cobre trenzado y apantallado. **Estandarizado en la familia de estándares ISO 21111 e ISO/IEC/IEEE 8802-3**. Hay desarrollos en estandarización para comunicaciones intra-vehiculares de hasta 100 Gb/s en IEEE sobre fibra óptica y cable de cobre trenzado y apantallado.

- Etc…

No se conoce si en el futuro se utilizará un mismo estándar para todos los fabricantes o si cada uno seguirá (como hasta ahora) implementando las tecnologías que mejor se adapten a sus vehículos. Sin embargo, la tendencia actual es el uso cada vez más extendido de las soluciones basadas en Ethernet debido a que permite la reutilización de protocolos de gestión, control de latencia, autenticación y cifrado entre otros ya probados extensamente en todo tipo de redes de comunicaciones.

6.1 Seguridad en CAN-BUS

Es importante destacar que, en la actualidad, uno de los elementos principales de comunicación intra-vehicular (entre los distintos elementos, sensores, ECUs y TCUs en el vehículo) es el CAN-BUS.

Los riesgos de seguridad asociados al CAN-BUS son evidentes, ya que a fecha de hoy no existen mecanismos de seguridad básicos como pueden ser la segmentación de la red, validación de los componentes de la misma o el filtrado de comportamientos anómalos, por lo que cualquier dispositivo que se conecta a la red es capaz de enviar tráfico a través de ésta.

Además, dado que los servicios de 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 (*safety*) del vehículo.

Para proteger el CAN-BUS no sería suficiente con un dispositivo que incorporara reglas para analizar el tráfico del bus como si de un antivirus convencional se tratara, debería incorporar también un motor de Inteligencia Artificial (IA) para el análisis del comportamiento y el conocimiento del entorno, ya que en algunas ocasiones detener un ataque puede suponer un impacto en la seguridad de los ocupantes y del resto de ocupantes de la vía mientras que en otras circunstancias ese mismo ataque podría tener un impacto mínimo. Se necesitaría definir un IDS/IPS adaptado a un automóvil.

6.2 Seguridad en Ethernet

Uno de los puntos destacables de las redes intra-vehiculares basadas en Ethernet es que todos los protocolos previamente desarrollados para la protección de datos en entornos de redes locales (LAN) son directamente reutilizables dentro del vehículo.

De este modo, **protocolos como MACSec, estandarizado dentro del ISO/IEC/IEEE 8802-1AE**, utilizado junto con el **protocolo de autenticación de dispositivo e intercambio y gestión de claves estandarizado dentro del ISO/IEC/IEEE 8802-1X**, garantizan la autenticación y encriptación del tráfico de datos intercambiado entre ECUs.

Adicionalmente, MACSec incluye un chequeo de la integridad del mensaje recibido, por lo que dificulta los ataques "Man-in-the-middle".

En cuanto a la protección ante la inserción de tramas previamente grabadas, MACSec, utilizado en conjunción con **ISO/IEC/IEEE 8802-1X**, rechazará todo el tráfico que no esté cifrado con una clave simétrica 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:

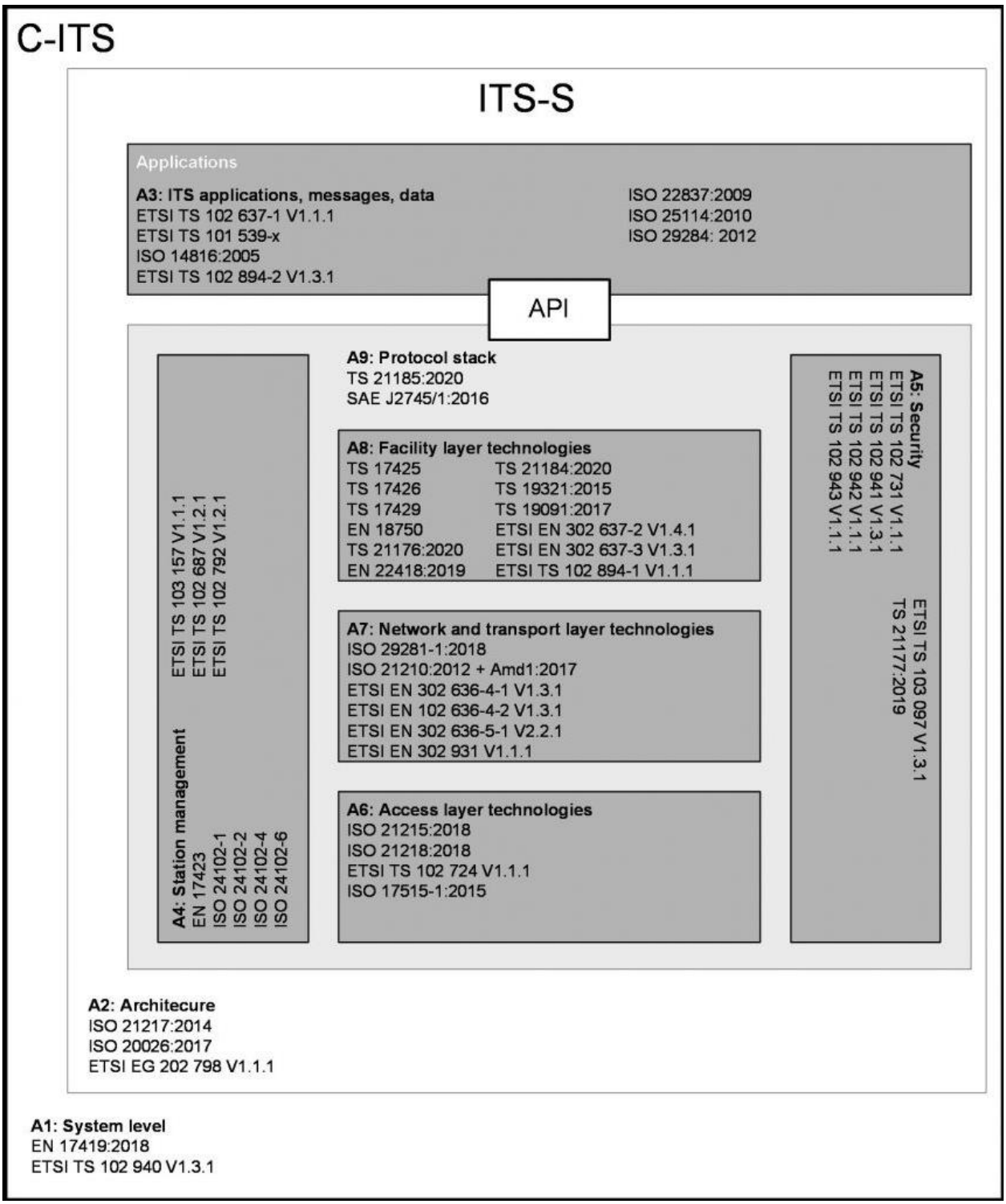
ETSI EN 302 636-4-1 V1.4.1	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking
ETSI TS 103 097 v1.3.	ITS Security; Security header and certificate formats
ETSI TS 102 941 v1.3.11	ITS Security; Trust and Privacy Management
ETSI TS 102 940 v1.3.1	ITS Security; ITS communications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

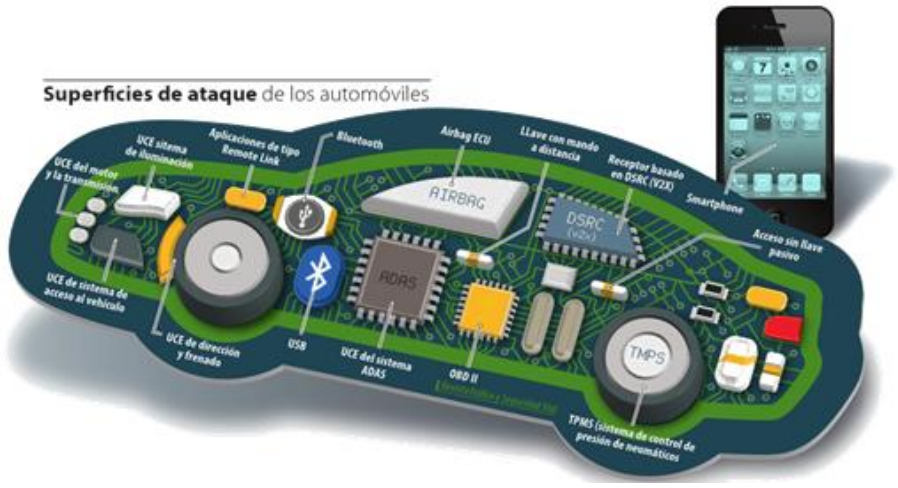
52 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0053

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:



- 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.

UNE es el organismo
de normalización español en:

Asociación Española
de Normalización

(+34) 915 294 900 — **une@une.org**

www.une.org