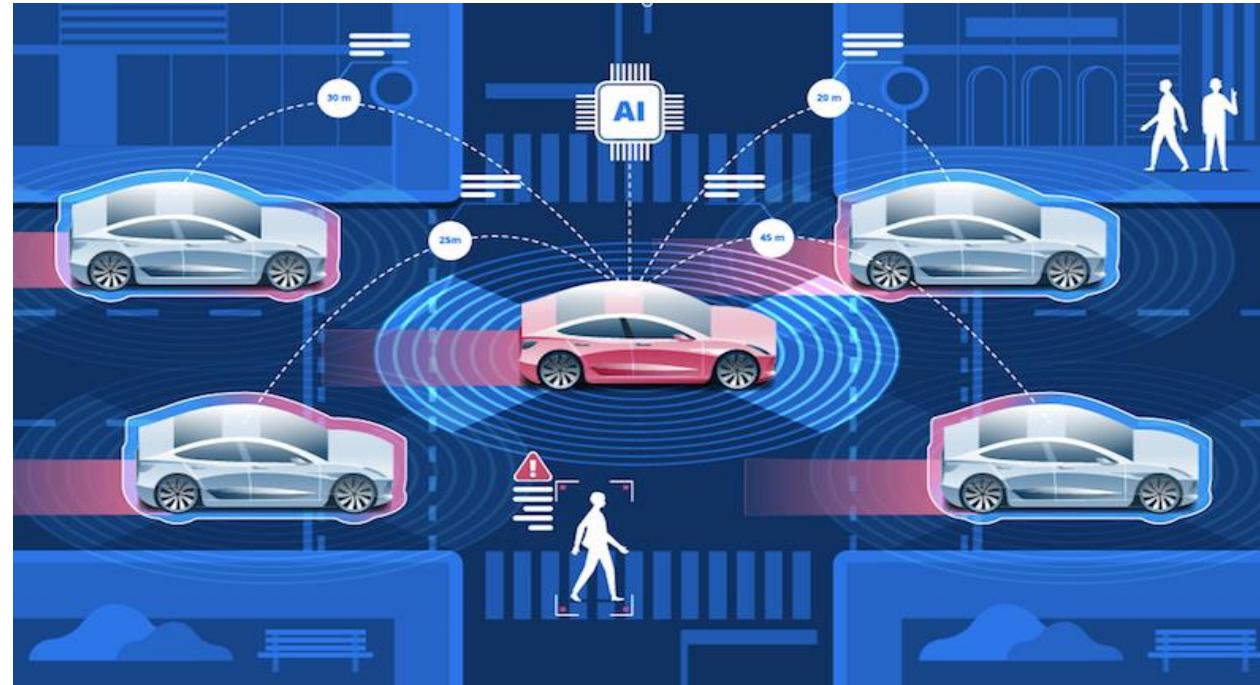


CIBER_CAR Ciberseguridad en los vehículos



CFP SAN VIATOR - CIFP SOMORROSTRO

CIBER-CAR Ciberseguridad en los vehículos

1.- Contexto.

2.- Objetivos generales.

3.- Desarrollo del proyecto.

3.1 – Estandarización del sector

3.2 – Ecosistema de empresas

3.3 – Proyectos relevantes

3.4 – Comunicaciones 5G y ciberseguridad

5.- Conclusiones.

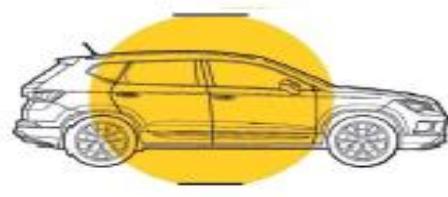
Contexto

Pasado



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

Presente



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

Futuro



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

LOC: Lines of Code (Líneas de código)

100M Millones

ECU: Electronic Control Unit (Unidad de control electrónica)

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

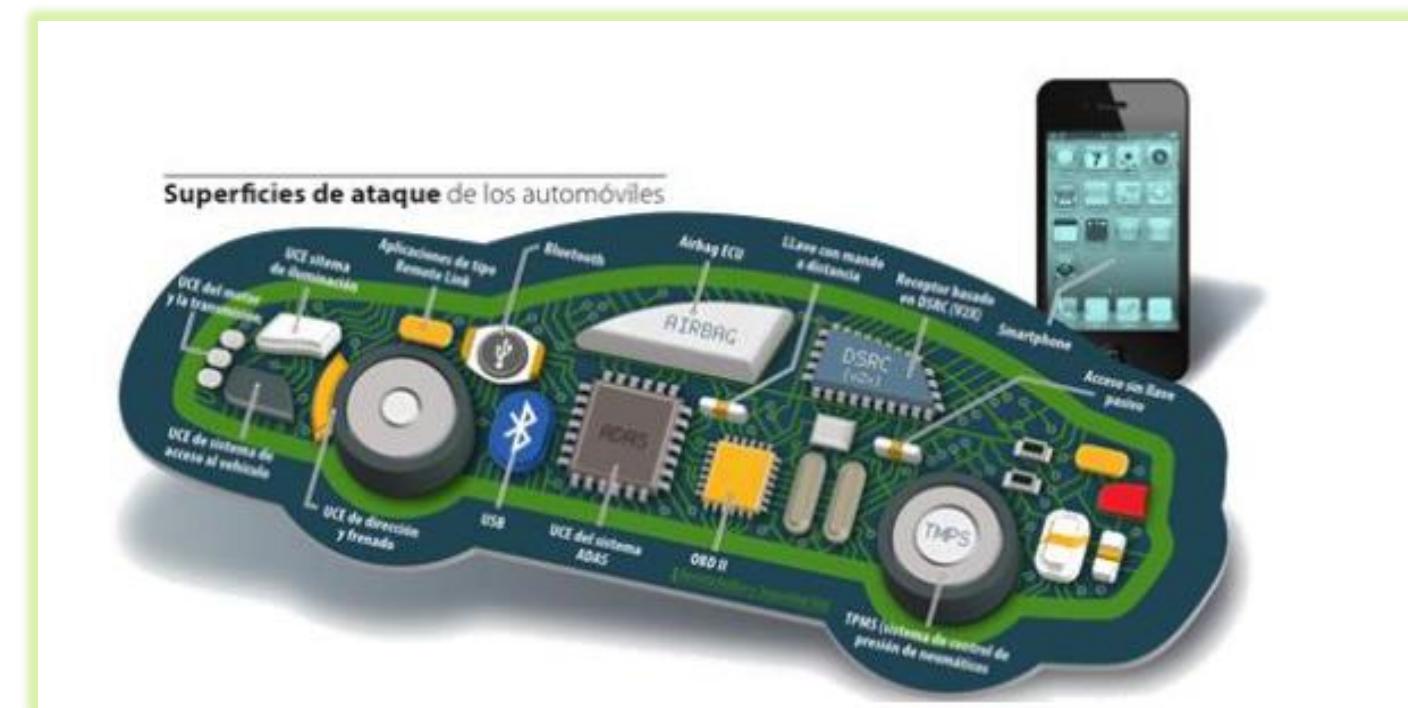
<https://site.ieee.org/connected-vehicles/ieee-connected-vechicles/connected-vehicles/>

- (1) Fuente EUROCYBCAR
- (2) Excepción TESLA: 1 sola ECU ultra potente

Contexto

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

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



Objetivos generales

Primera aproximación a la ciberseguridad en el ámbito de la automoción.

Se ha tratado de **identificar los órganos técnicos de normalización, estándares, proyectos e iniciativas más relevantes**, relativos a la ciberseguridad, en el ámbito de la movilidad Conectada y Automatizada, en particular en los vehículos conectados y Automatizados, sistemas inteligentes de transporte y las tecnologías de comunicación y conectividad involucradas.

1. Capacitación del profesorado
2. Identificación de nuevas competencias profesionales
3. Diseminación de conocimientos



Estandarización del sector

¿Qué norma regula la ciberseguridad de los vehículos?

- ✓ Reglamento UNECE/R155

“Reglamento de las Naciones Unidas sobre disposiciones uniformes relativas a la homologación de vehículos a motor en lo que respecta a la ciberseguridad y el sistema de gestión de ciber-seguridad”.

Es por todo ello que la Unión Europea (UE) ha establecido como requisito para la homologación de tipo de vehículos de motor el REGLAMENTO (UE) 2019/2144 cuyas fechas clave son:

- Fecha de denegación de la homologación tipo UE: 6 julio 2022
- Fecha de prohibición de la matriculación de vehículos. 7 julio 2024

Estandarización del sector

A qué vehículos afecta...

Categorías de vehículos afectados por la UNECE



Categoría M:
Coches y autobuses.



Categoría N:
Furgonetas y camiones.



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



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

Estandarización del sector

Proporciona un marco para que el sector automotriz establezca los procesos necesarios para...

-  Identificar y gestionar los riesgos de ciberseguridad en el diseño de vehículos
-  Verificar que se gestionen los riesgos, incluidas las pruebas.
-  Asegurar que las evaluaciones de riesgos se mantengan actualizadas.
-  Monitorizar los ciberataques y que se responda efectivamente a ellos
-  Evaluar si las medidas de ciberseguridad siguen siendo efectivas a la luz de las nuevas amenazas y vulnerabilidades
-  Analizar los ataques exitosos o intentados.

Estandarización del sector

Para cumplir con la normativa, los fabricantes tendrán que crear para sus vehículos un sistema de gestión de ciberseguridad CSMS...

Es un sistema de procesos que, en conjunto, deben gestionar la ciberseguridad de sus modelos a lo largo de todo su ciclo de vida: desarrollo, producción y postproducción.

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

Estandarización del sector

7 apartados relacionados con

Servidores BACK-END

Canales de comunicación que usa el vehículo para conectarse a su entorno

Conexiones y conectividad externa

Datos/código del vehículo

Posibles explotaciones si no se protegen o refuerzan lo siguiente

Con acciones humanas no intencionadas

Procedimientos de actualización de los vehículos

Estandarización del sector

Servidores BACK-END



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

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

Descripciones generales y específicas de vulnerabilidades/amenazas		Ejemplo de vulnerabilidad o método de ataque	
	3	Los datos relacionados con el vehículo que se almacenan en los servidores back-end se pierden o se ven comprometidos (violación de la seguridad de los datos)	3.1 Abuso de privilegios por parte del personal (ataque interno) 3.2 Pérdida de información en la nube. Pueden perderse datos sensibles debido a ataques o accidentes cuando el almacenamiento de los datos corre a cargo de terceros proveedores de servicios en la nube 3.3 Acceso no autorizado al servidor a través de Internet (posibilitado, por ejemplo, por backdoors, vulnerabilidades de un software del sistema sin parches, ataques SQL u otros medios) 3.4 Acceso físico no autorizado al servidor (por ejemplo, mediante memorias USB u otros medios de conexión al servidor) 3.5 Violación de la seguridad de los datos por un intercambio de datos no intencionado (p. ej., errores administrativos)

Estandarización del sector

Servidores BACK-END



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

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

Estandarización del sector

Canales de comunicación que usa el vehículo para conectarse a su entorno



por ejemplo, otros vehículos o la infraestructura, se deberán evitar, entre otras amenazas, que se pueda suplantar la identidad de otros vehículos, injectar malware-programas que dañan los sistemas informáticos por los canales de comunicación y manipular o eliminar los datos y códigos del software del vehículo.

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

Estandarización del sector

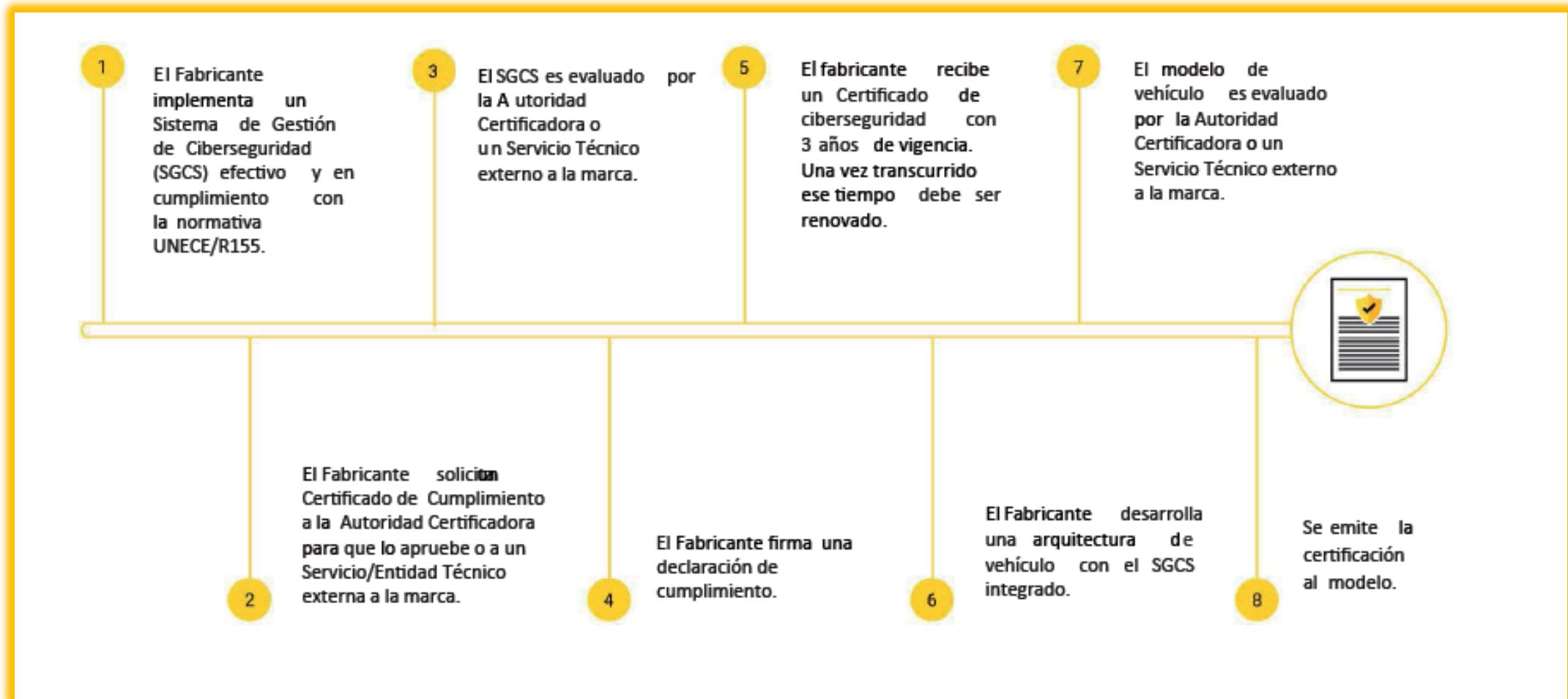
Canales de comunicación que usa el vehículo para conectarse a su entorno



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

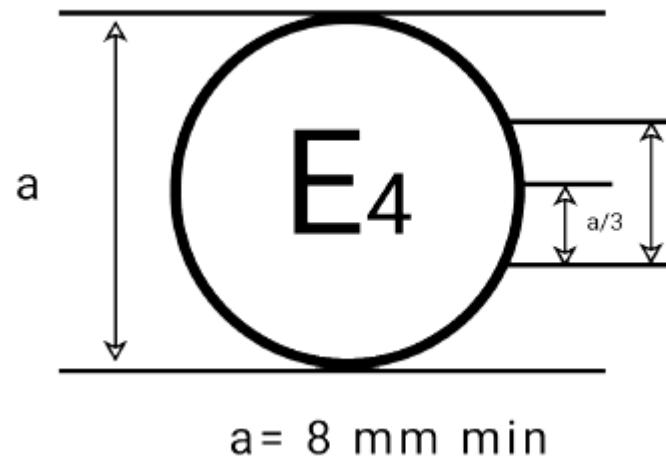
Estandarización del sector

Proceso de certificación...



Estandarización del sector

Etiqueta de vehículo ciberseguro...



155 R - 001234

- Una letra "E" seguida del número distintivo del país que ha concedido la certificación, rodeados ambos por un círculo.
- A la derecha de esa marca se situará el número del reglamento de la ONU.

- A ese número lo seguirá una letra "R", un guion y el número de homologación.

Esta marca deberá situarse de forma visible y fácilmente accesible dentro o cerca de la placa de identificación del vehículo. La imagen de la parte superior es un ejemplo de marca de homologación para mostrar que un vehículo tiene un CSMS cuyo funcionamiento ha sido certificado según los requisitos de la UNECE/R155. En este ejemplo, los elementos que componen esta marca de homologación indican lo siguiente:



Euskadiko LHren Ikerketa Aplikatuko Zentroa
Centro de Investigación Aplicada de FP Euskadi
Basque VET Applied Research Centre

Ecosistemas de empresas



EUSKO JAURLARITZA
HEZKUNTZA SAILA
Loreak eta Hezkuntza Sailburuordetza

GOBIERNO VASCO
DEPARTAMENTO DE EDUCACIÓN
Viceconsejería de Formación Profesional



Proyectos relevantes

Proyecto OMSP (Open Mobility Security Project)

<https://github.com/zerolynx/omsp>

Proyecto abierto dedicado a estandarizar un marco de controles técnicos para evaluar la seguridad a nivel de hacking en todo tipo de vehículos. Este proyecto nació como un proyecto interno de [Zerolynx](#) para realizar revisiones de seguridad sobre varios sistemas integrados en diferentes vehículos, como automóviles y trenes.

Control categories

- OMSP-BUSLOGIC: Business Logic
 - OMSP-BUSLOGIC-01: Unexpected behavior
- OMSP-SHARE: Car Sharing Systems
 - OMSP-SHARE-01: Attacks to expansion kits
- OMSP-CHARGE: Chargers
 - OMSP-CHARGE-01: Car
 - OMSP-CHARGE-02: Charger Points
 - OMSP-CHARGE-03: ID Card/Pysical Token
 - OMSP-CHARGE-04: Mobile Charging Apps
- OMSP-CONTROL: Control Center
 - OMSP-CONTROL-01: Distributed Control Core
 - OMSP-CONTROL-02: Monolithic Control Core
- OMSP-IFACE: Driving Interface
 - OMSP-IFACE-01: Physical Interfaces
 - OMSP-IFACE-02: Touchscreens
- OMSP-EXTNET: External Network
 - OMSP-EXTNET-01: Cellular Connection
 - OMSP-EXTNET-02: Remote Control Apps
 - OMSP-EXTNET-03: Wireless
- OMSP-INFO: Infotainment
 - OMSP-INFO-01: Applications
 - OMSP-INFO-02: Driving Information
 - OMSP-INFO-03: GPS Navigator
 - OMSP-INFO-04: Screen
 - OMSP-INFO-05: Web Browser
- OMSP-INTNET: Internal Network
 - OMSP-INTNET-01: Physical Access to Network
 - OMSP-INTNET-02: Base Network/CAN bus
 - OMSP-INTNET-03: Guest Wi-Fi Network
 - OMSP-INTNET-04: Bluetooth
 - OMSP-INTNET-05: Network Electronics
- OMSP-OPCLOSE: Opening And Closing Systems
 - OMSP-OPCLOSE-01: Physical Key
 - OMSP-OPCLOSE-02: Radiofrequency
 - OMSP-OPCLOSE-03: Bluetooth
 - OMSP-OPCLOSE-04: NFC
 - OMSP-OPCLOSE-05: Internet
- OMSP-SENSOR: Sensors
 - OMSP-SENSOR-01: Tire-Pressure Monitoring System (TPMS)
 - OMSP-SENSOR-02: Proximity Sensors
 - OMSP-SENSOR-03: Driving Cameras
 - OMSP-SENSOR-04: Security Cameras
 - OMSP-SENSOR-05: External beacons
 - OMSP-SENSOR-06: Cabin Safety Sensors
 - OMSP-SENSOR-07: Remote Detection Systems
- OMSP-TESTENV: Testing Environments
 - OMSP-TESTENV-01: Hardening review
 - OMSP-TESTENV-02: SSDLC

Proyectos relevantes

Eurocybcar Standard Test Protocol

Dispone de un test que evalúa y certifica si el vehículo cumple con los 70 requisitos de ciberseguridad que exige la norma UNECE/R155: EUROCYBCAR. aplicando la metodología ESTP- a vehículos de organismos públicos y OEMs.

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

DE ACCESO FÍSICO: Manipulaciones -a través del **puerto OBD** del vehículo- el airbag, sus frenos o su dirección; o si a través del **puerto USB** se puede introducir un virus que provoque la paralización de los sistemas del vehículo y ponga en riesgo la vida de los pasajeros.

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

PRUEBAS DE APLICACIONES: Se evalúan las vulnerabilidades de las **aplicaciones que ya están integradas** en el vehículo, y también las **apps oficiales de la marca** que el usuario se descarga en su móvil. Esto, obviamente, es un peligro si un ciberdelincuente consigue vulnerar dichas aplicaciones, ya que podría acceder a sistemas del vehículo y llegar incluso a provocar un accidente..

COMUNICACIONES 5G Y VULNERABILIDADES

Sendoa Florez, Alberto Laza y Vicente Llarena

Índice

- Vehículo conectado y autónomo. Definición.
- Los sistemas de transporte inteligente (ITS).
- Los sistemas cooperativos de transporte inteligente (C-ITS).
- Tecnologías de comunicación vehicular.
- Ciberseguridad en las comunicaciones V2X.
- Normas de seguridad.
- Organizaciones de estandarización.

¿Qué entendemos por “vehículo conectado” y “vehículo autónomo”?

Vehículo Conectado - Autónomo

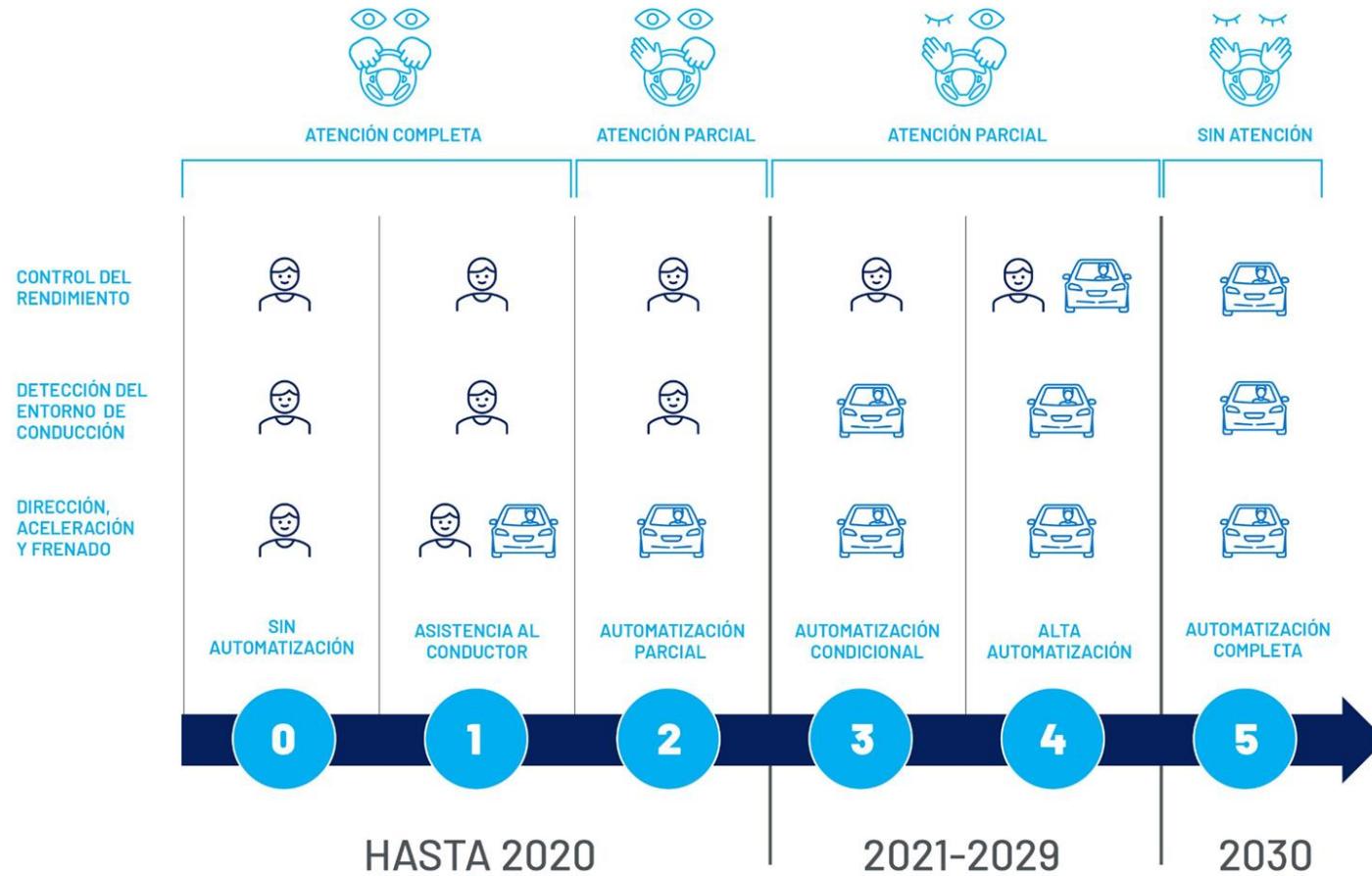
- Minimizar la siniestralidad: información del estado del vehículo en tiempo real.
- Maximizar la seguridad



- Imitar las competencias humanas
- Toma de decisiones: AI
- No se necesitan personas en su interior



Vehículo Autónomo- Niveles



Movilidad autónoma = Grandes desafíos

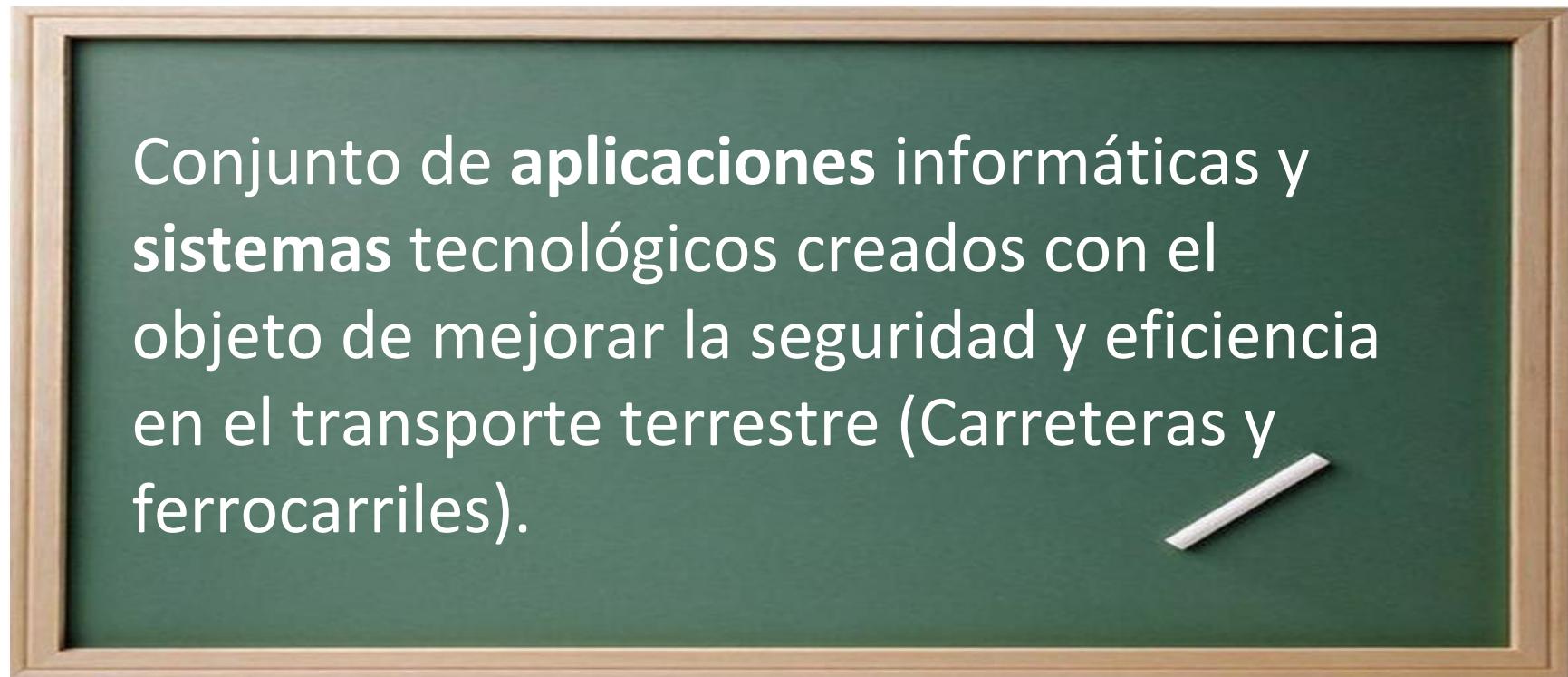
- Aspectos legales.
- Infraestructura conectada.
- Desarrollo de algoritmos de AI específicos.
- Vehículos comerciales viables.
- Ciberseguridad.

**¿Qué necesitamos para llegar al coche
conectado y autónomo?**

**¿Qué tecnologías de comunicación van a ser
necesarias?**

Los Sistemas de Transporte Inteligente (Intelligent Transportation Systems) ITS

Los Sistemas Inteligentes de Transporte



Los Sistemas de Transporte Inteligente

- Aumentan la seguridad en l@s conductor@s.
 - Seguridad preventiva/Seguridad instantánea/reactiva.
- Mejoran la eficiencia del tráfico.
- Permiten llevar a cabo un control detallado de los elementos de la carretera.
- Facilitan la labor de l@s conductor@s.

Los Sistemas de Transporte Inteligente



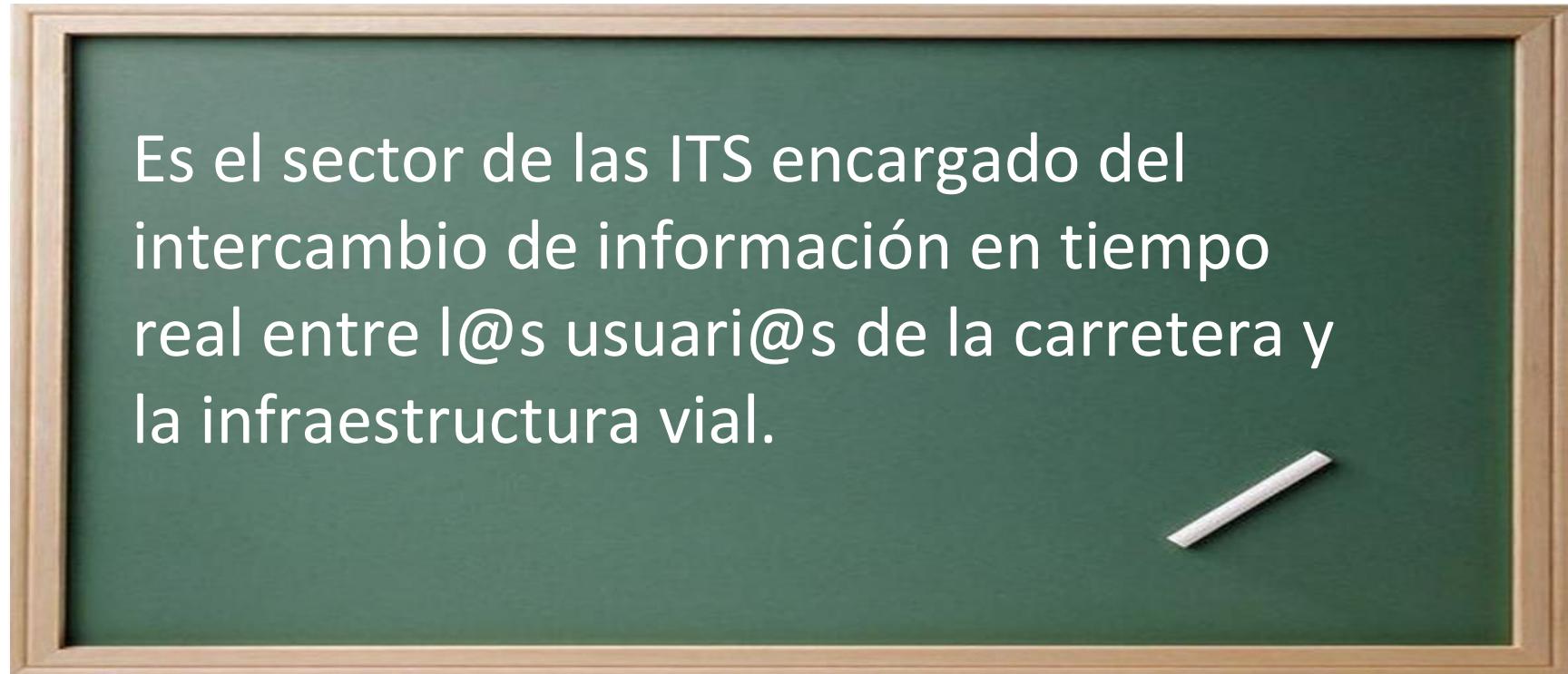
¿Qué pasaría si el propio vehículo aportara información relevante a los ITS?

Cooperative-ITS

Sistemas Cooperativos de Transporte Inteligente

(C-ITS)

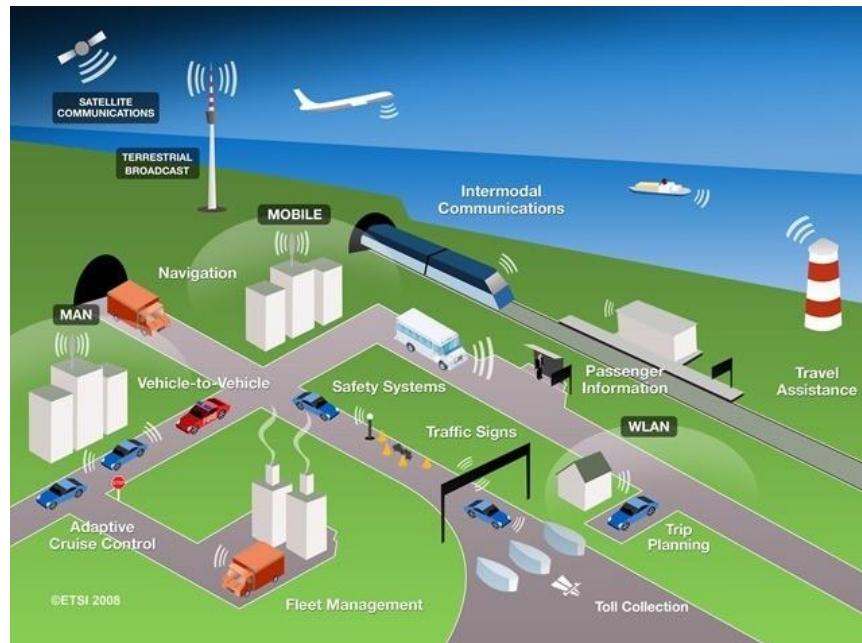
Cooperative ITS



Es el sector de las ITS encargado del intercambio de información en tiempo real entre l@s usuari@s de la carretera y la infraestructura vial.

¿Y cómo se consigue ésto?

Gracias a la CONECTIVIDAD entre vehículos e infraestructura



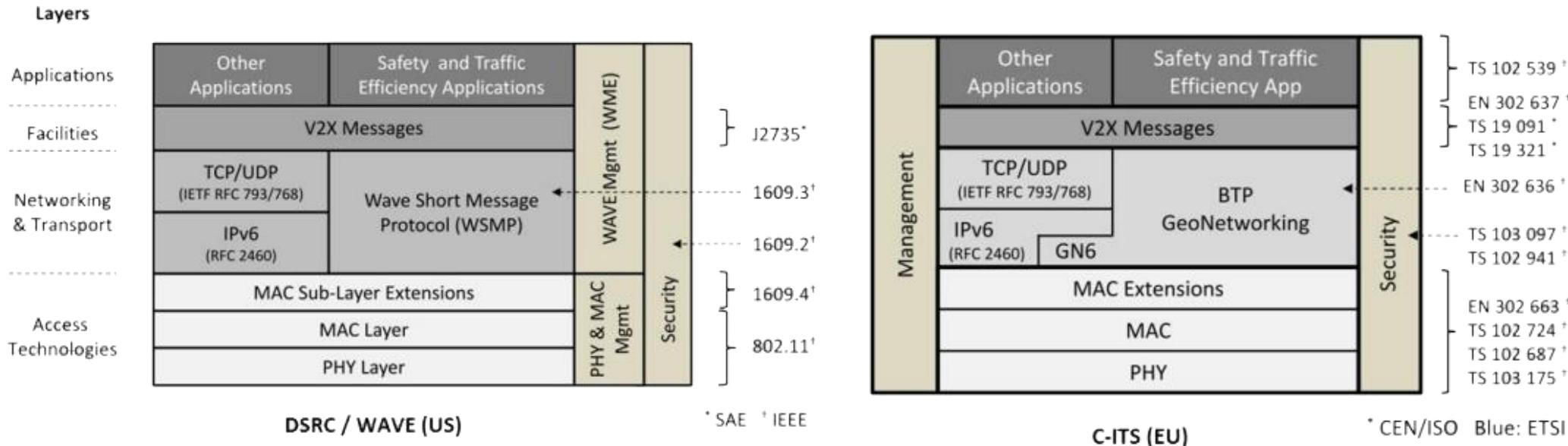
Y esa conectividad ha de ser INALÁMBRICA!!!!

Las tecnologías de comunicación vehicular

Las tecnologías de comunicación vehicular

- **Tecnologías V2X** (Vehicle-to-Everything).
- Elemento de seguridad complementario a los **ADAS**.
- V2X avisa al conductor de peligros **NO VISIBLES**.
- Existen **dos tecnologías** de comunicación V2X:
 - Arquitecturas V2X basadas en “Wifi”: **DSRC** (ITS-G5)
 - Arquitecturas V2X basadas en redes celulares: **C-V2X**.

Las tecnologías de comunicación vehicular



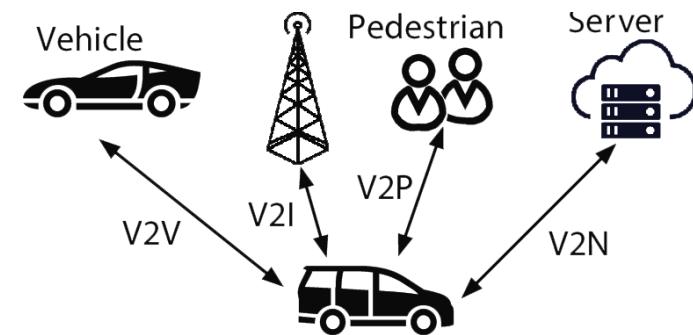
Fuente: Festag

Pilas de protocolos en DSRC y en C-ITS

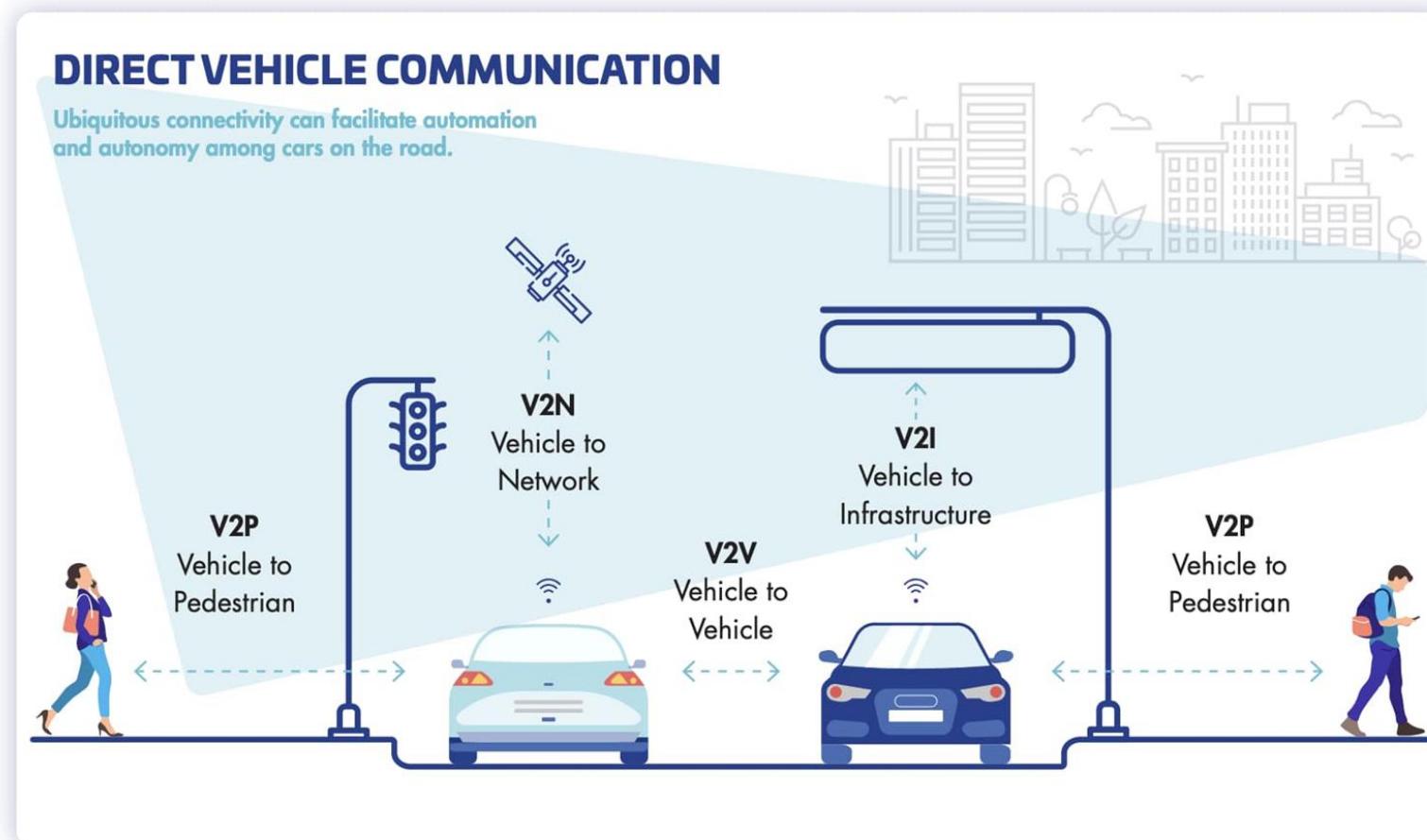
Las tecnologías de comunicación vehicular (V2X)

- Existen varios componentes:

- Comunicaciones Vehículo a vehículo (**V2V**).
- Comunicaciones Vehículo a infraestructura (**V2I**).
- Comunicaciones Vehículo a peatón (**V2P**).
- Comunicaciones Vehículo a red (**V2N**).



Las tecnologías de comunicación vehicular (V2X)



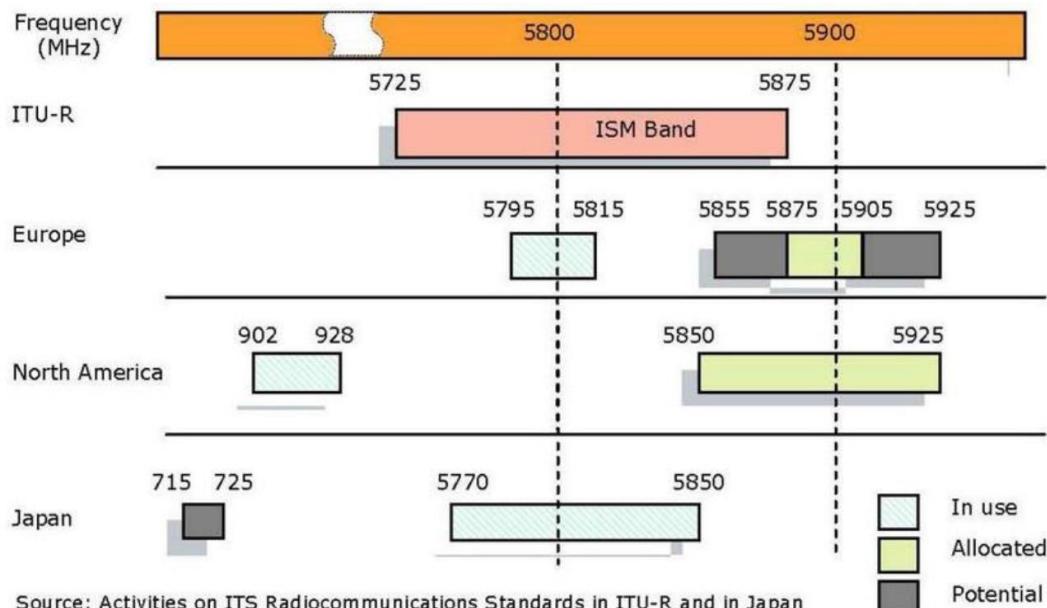
Tecnología V2X “DSRC/C-ITS (ITS-G5)”

- **DSRC = Dedicated Short Range Communication**

- Tecnología de comunicación inalámbrica que permite **comunicación directa** entre vehículos e infraestructura.
- Se basa en el **estándar IEEE 802.11p**. No se usan “Puntos de Acceso”. Red vehicular “Ad hoc”.
- Trabaja en la **banda licenciada** de 5,9 GHz.
- Características funcionales:
 - **Corto alcance** (1 Km), **Baja latencia** (2 msg).
 - **Alta confiabilidad** (interoperatividad), **rendimiento** resistente a condiciones climáticas extremas y a la alta movilidad.

Tecnología V2X “DSRC”

- A nivel frecuencial:

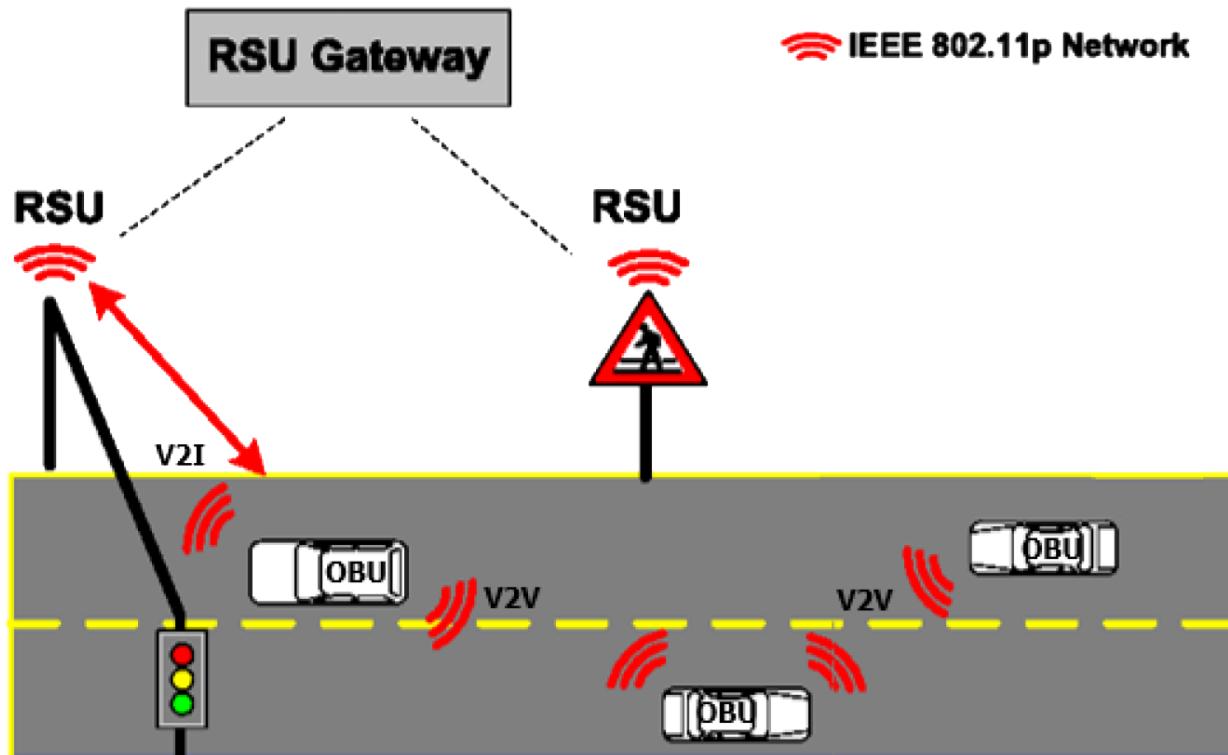


Características enlace físico	WAVE 802.11p
Alcance	1000 m
Tasa de transmisión	3 – 27 Mbps
Potencia transmitida	EE. UU: 760 mW, EU: 2W
Ancho de banda	10 MHz, 20 MHz
Movilidad	Alta
Banda de uso	5.86 GHz – 5.92 GHz
Espectro asignado	EE. UU: 75 MHz EU: 30 MHz
Estándares	IEEE, ISO, ETSI

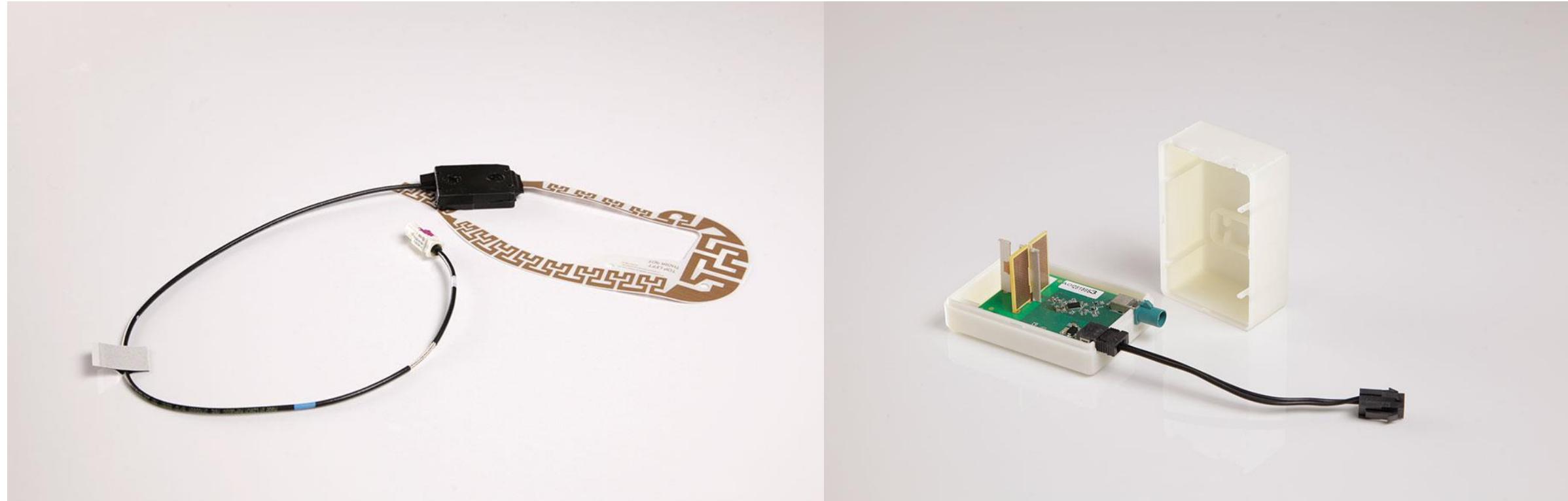
Tecnología V2X “DSRC”

- Dos modos de funcionamiento en DSRC

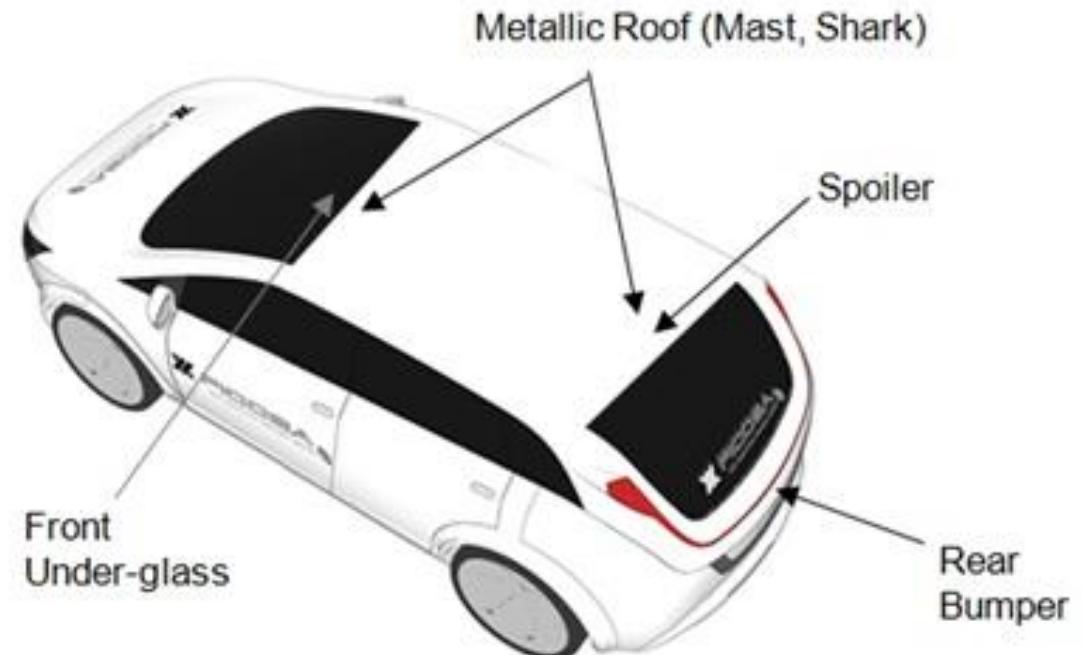
- Vehículo a vehículo (V2V).
- Vehículo a infraestructura (V2I).



Tecnología V2X “DSRC”: soluciones ya implementadas



Tecnología V2X “DSRC”: soluciones ya implementadas

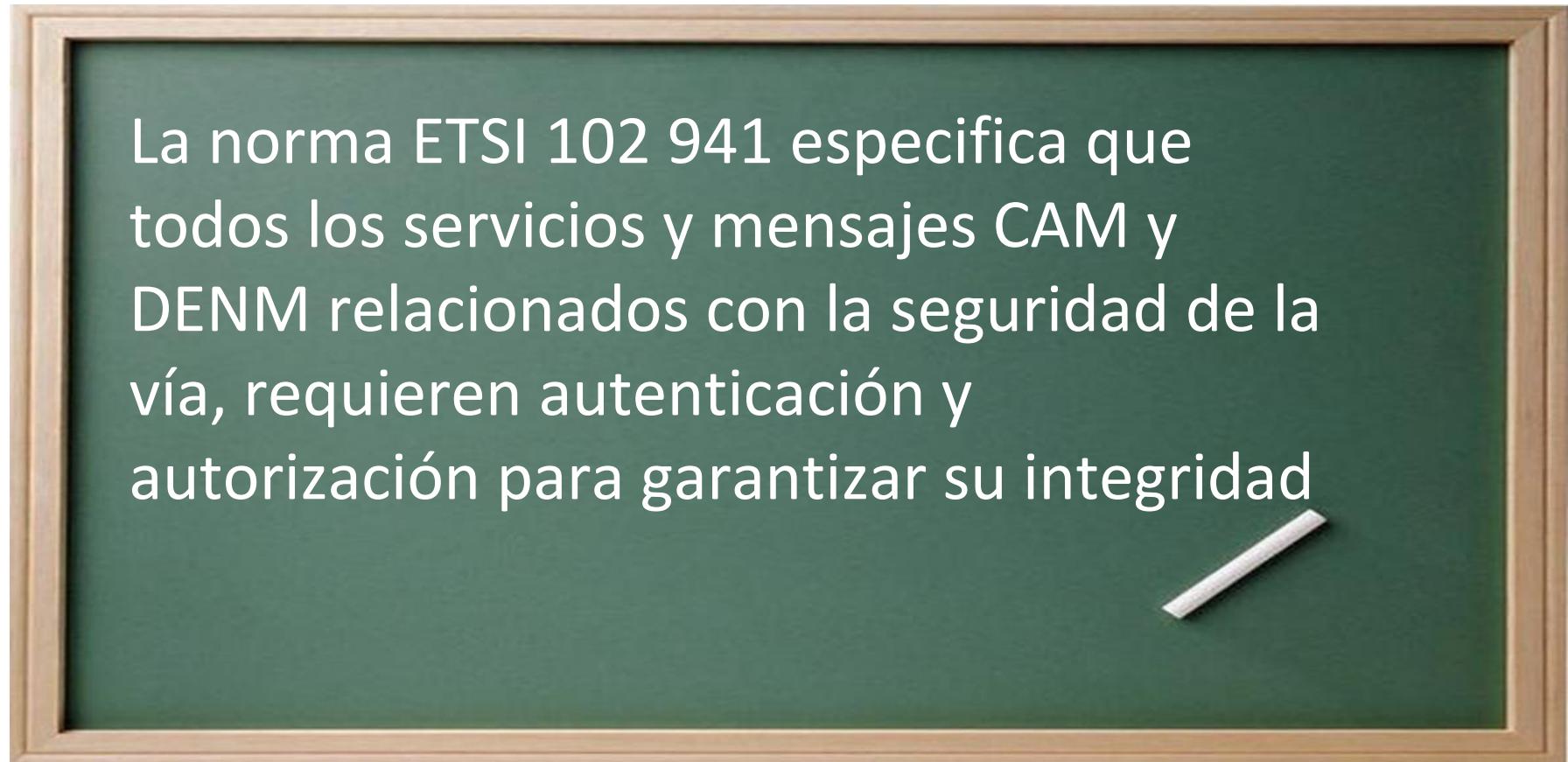




Tecnología V2X “DSRC”

- **Dos tipos de mensajes para el intercambio de información**

- **Mensajes CAM** (Cooperative Awareness Message)
 - Mensajes de “broadcasting” transmitidos con un periodo mínimo de 100 ms y máximo de 1s.
 - Informan a las estaciones cercanas sobre la posición y rumbo del vehículo emisor.
- **Mensajes DENM** (Decentralized Environmental Notification Message)
 - No son periódicos. Se envían únicamente en caso de determinados eventos y en un área determinada. En estos mensajes no se contempla riesgos de privacidad por lo que no van cifrados.



Tecnología V2X “C-V2X”

- **C-V2X = Cellular - V2X**

- Tecnología de comunicación inalámbrica que permite **comunicación directa** entre vehículos, elementos de la infraestructura y **otros usuarios** como peatones, ciclistas, etc ...
- Tecnología creada por el **3GPP**, organización que define los estándares globales de red inalámbrica celular:
 - **Release 14** en LTE-4G
 - **Release 15** soporte 5G para V2N
 - **Release 16** para 5G NR

Tecnología V2X “C-V2X”

- **Modos de comunicación C-V2X**

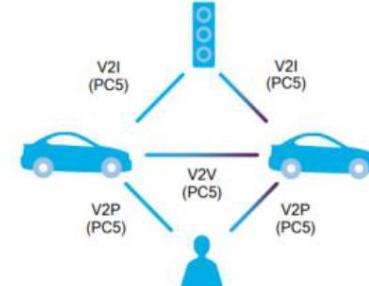
- **Comunicaciones directas (Sidelink).**

- Casos de uso: V2V, V2I y V2P.
- Banda 5,9 GHz.

- **Comunicaciones de red (Uplink/Downlink).**

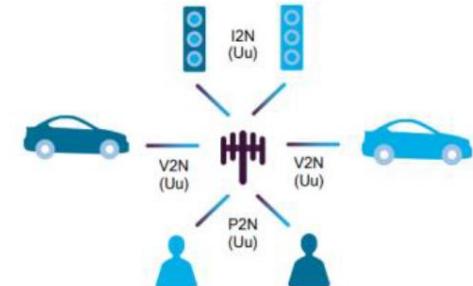
- Caso de uso: V2N.
- Banda móvil.

Direct (= Sidelink)
 V2V, V2I, and V2P operating in ITS bands (e.g. ITS 5.9 GHz) independent of cellular network



Short range (<1 kilometer), location, speed
 Implemented over “PC5 interface”

Network (= Up/Downlink)
 V2N operates in traditional mobile broadband licensed spectrum



Long range (>1 kilometers). e.g. accident ahead
 Implemented over “Uu interface”

Tecnología V2X “C-V2X”

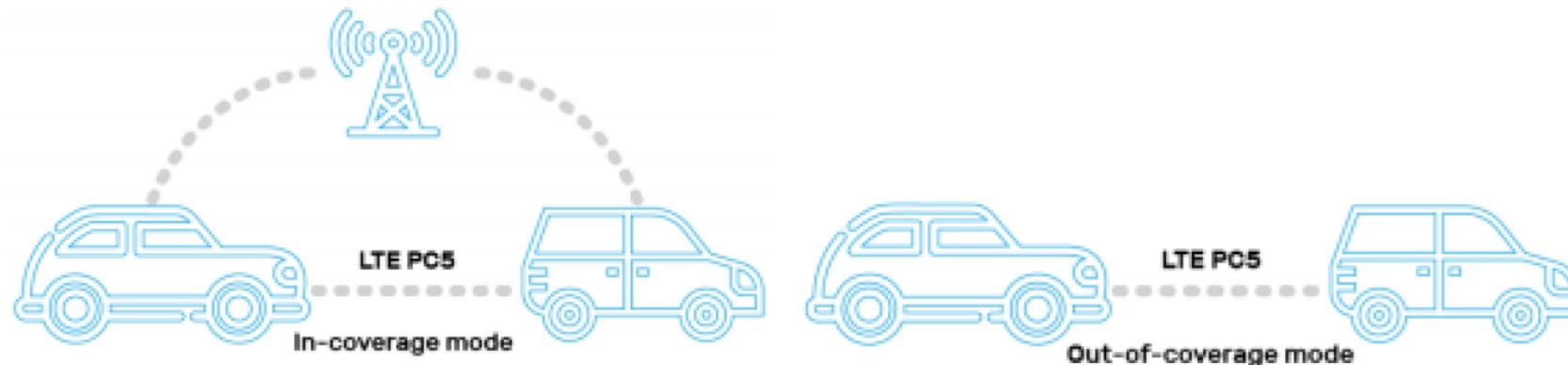
- Modos de comunicación C-V2X

Modos de comunicación	V2V, V2P, V2I	V2N
Interfaz radio	PC5	LTE-Uu
Espectro	5.9 GHz	3.5 GHz
Traffic	Multicast/Broadcast	Unicast/Multicast (eMBMS)
Tipo de tráfico	IPv6, non-IP	IPv6
Modo de acceso	Modos programados y autónomos agregados	Modo heredado

Tecnología V2X “C-V2X”

- **Modo de comunicación C-V2X directa “Sidelink”:**

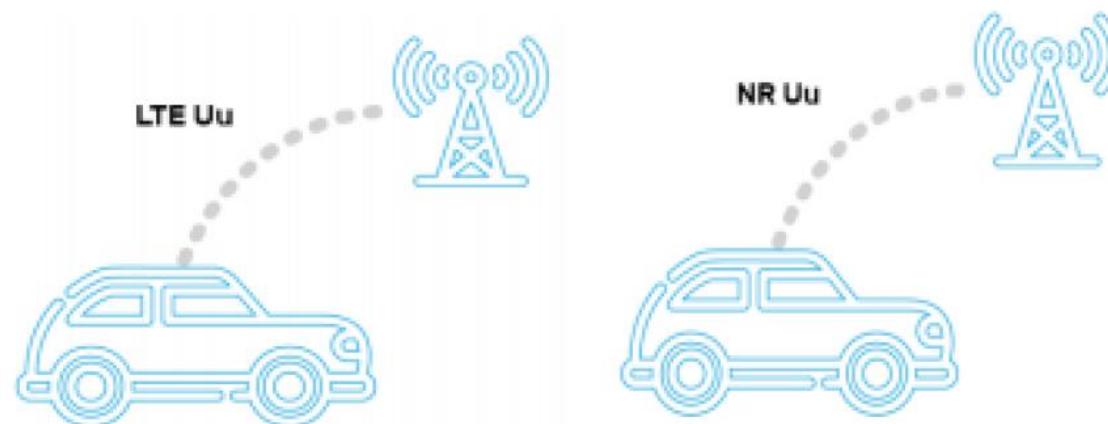
- Uso de la interfaz “**LTE PC5**”
- Contempla dos modos: “**de cobertura**” y “**sin cobertura**”
- Opera en las bandas ITS (**5,9 GHz**) independiente de la red móvil.
- No requieren de **SIM** pero si de **GNSS**.



Tecnología V2X “C-V2X”

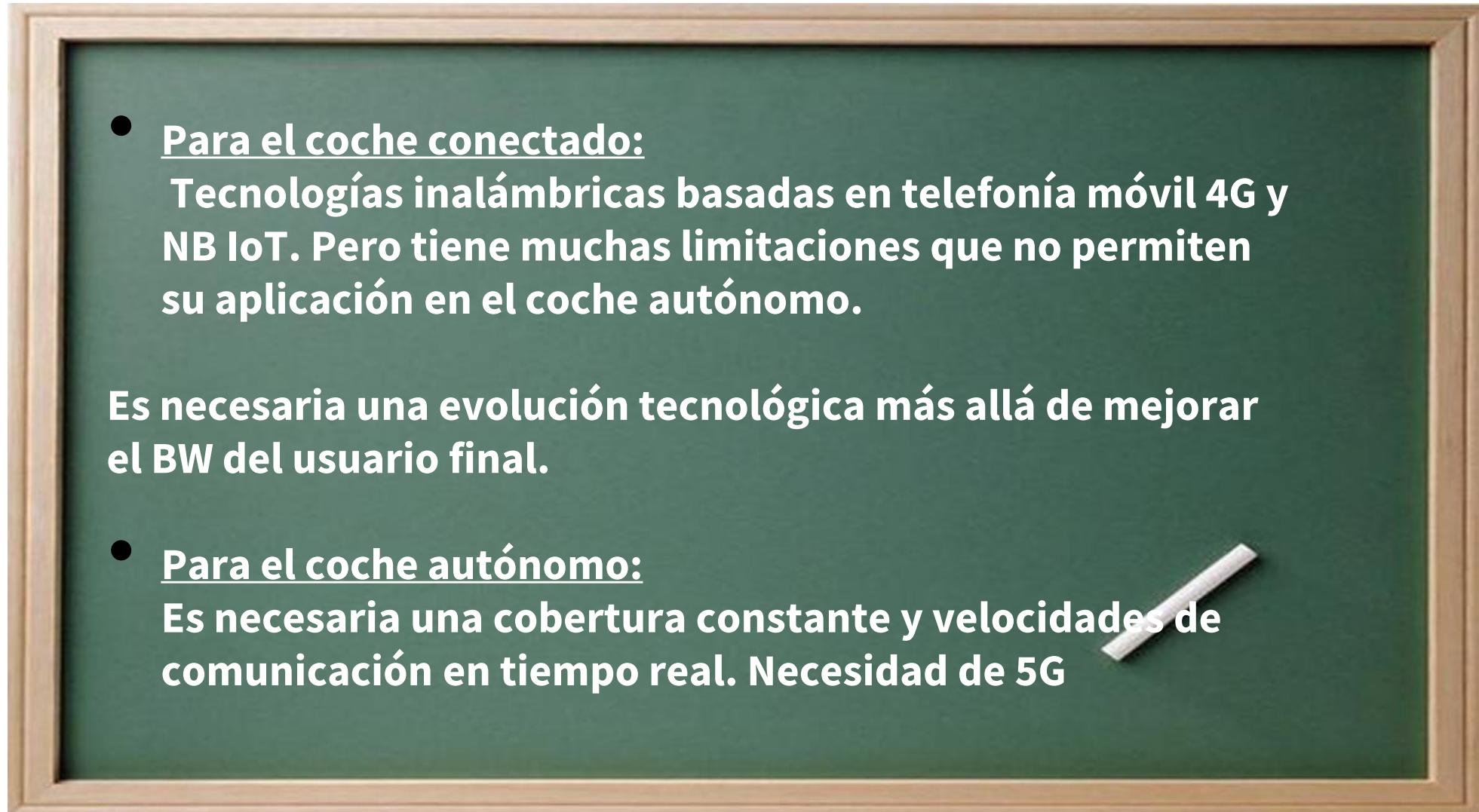
- **Modo de comunicación C-V2X a red “Uplink/Downlink”:**

- Uso de la interfaz “**LTE Uu** y **NR Uu**”. Interfaces para comunicaciones móviles.
- Soportan comunicaciones “**Unicast**” y “**Multicast**”
- Opera en las **bandas licenciadas celulares**
- Requieren de **SIM**



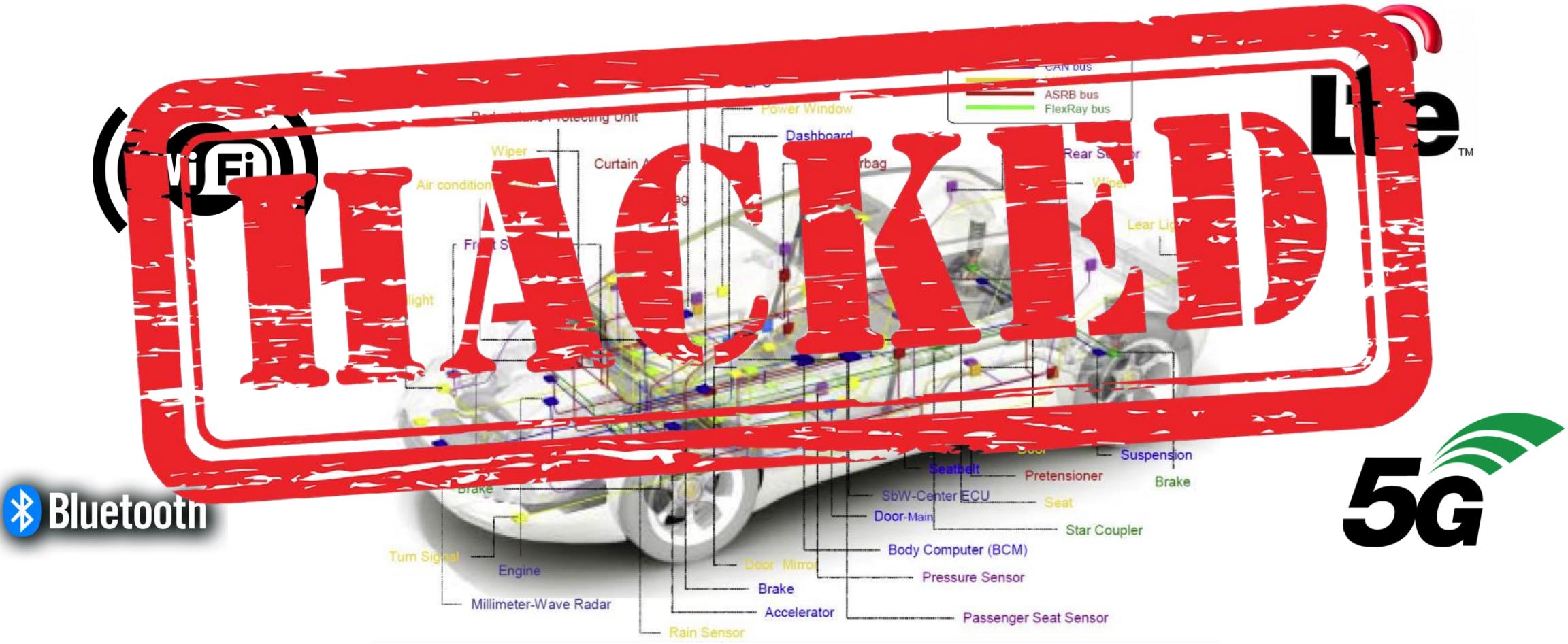
Comparativa de estándares de comunicación vehicular

	802.11p	802.11bd	LTE-V2X	5G NR-V2X
Tecnología base	802.11a	802.11 n/ac	LTE	5G NR
Banda	5.9 GHz	5.9 GHZ 57 – 71 GHz	800/1800 MHz (LTE) 5.9 GHz (<i>sidelink</i>)	410 MHz – 7.125 GHz 24.25 GHz – 52.6 GHz
Modulación	16 QAM 64-QAM	64-QAM 256-QAM	16-QAM 64-QAM	64-QAM 256-QAM
Ancho de banda canal	10 MHz	10 MHz 20 MHz (opcional)	20 MHz	400 MHz
Bit rate	15 Mbit/s	20 Mbit/s	13-15 Mbit/s	30-60 Mbit/s
Latencia (ms)	< 10-100	0.5 - 10 hasta 300 m 10 – 100 a partir de 300m	20 – 100	0.5 -10 hasta 500 m 10 – 100 a partir de 500m
Alcance máximo	~1 km	~1 km	~2 km	~2 km
Vel. relativa máxima	200 km	500 km	200km	500 km
Packet size (bytes)	100 – 1500	100 – 1500	100 – 1500	100 – 1500

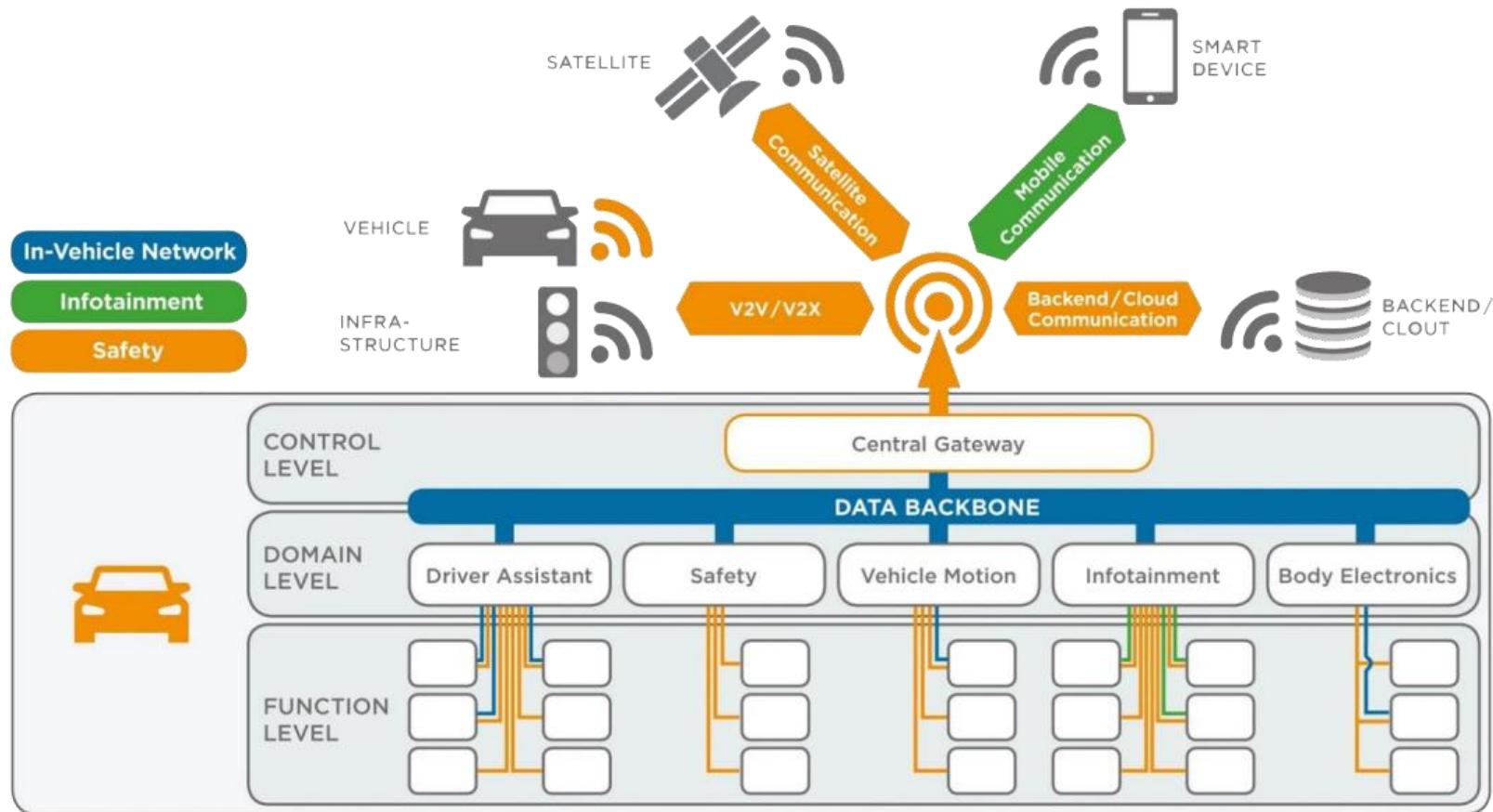


Pero, ¿Qué hay de “malo” en todo esto?

Redes internas y externas vehiculares



Interconexión de redes internas vehiculares



Fuente: TE Automotive

Ciberseguridad en comunicaciones “V2X”

Ciberseguridad en comunicaciones “V2X”

- **Consideraciones previas:**

- V2X representa un **flujo de datos de entrada** equiparable al de cualquier otro sensor.
- Este canal inalámbrico va a suministrar “información” **más allá de la línea de vista** que la red de sensores del propio vehículo.
- La información intercambiada por medio de las comunicaciones V2X condiciona las **decisiones y maniobras** ejecutadas por los sistemas de **conducción autónoma**.
- La **manipulación no autorizada** de los datos ... **GRAVES PROBLEMAS!!!**
- Identificación de los riesgos, vulnerabilidades y amenazas.

Ciberseguridad en comunicaciones “V2X”

- **Identificación de activos:**

- Los activos se suelen dividir en:
 - Activos **físicos** (Hardware).
 - Activos **lógicos** (Software e información).
- En el entorno vehicular una dimensión más:
 - La integridad de **las personas** ocupantes de los vehículos y de la vía pública.

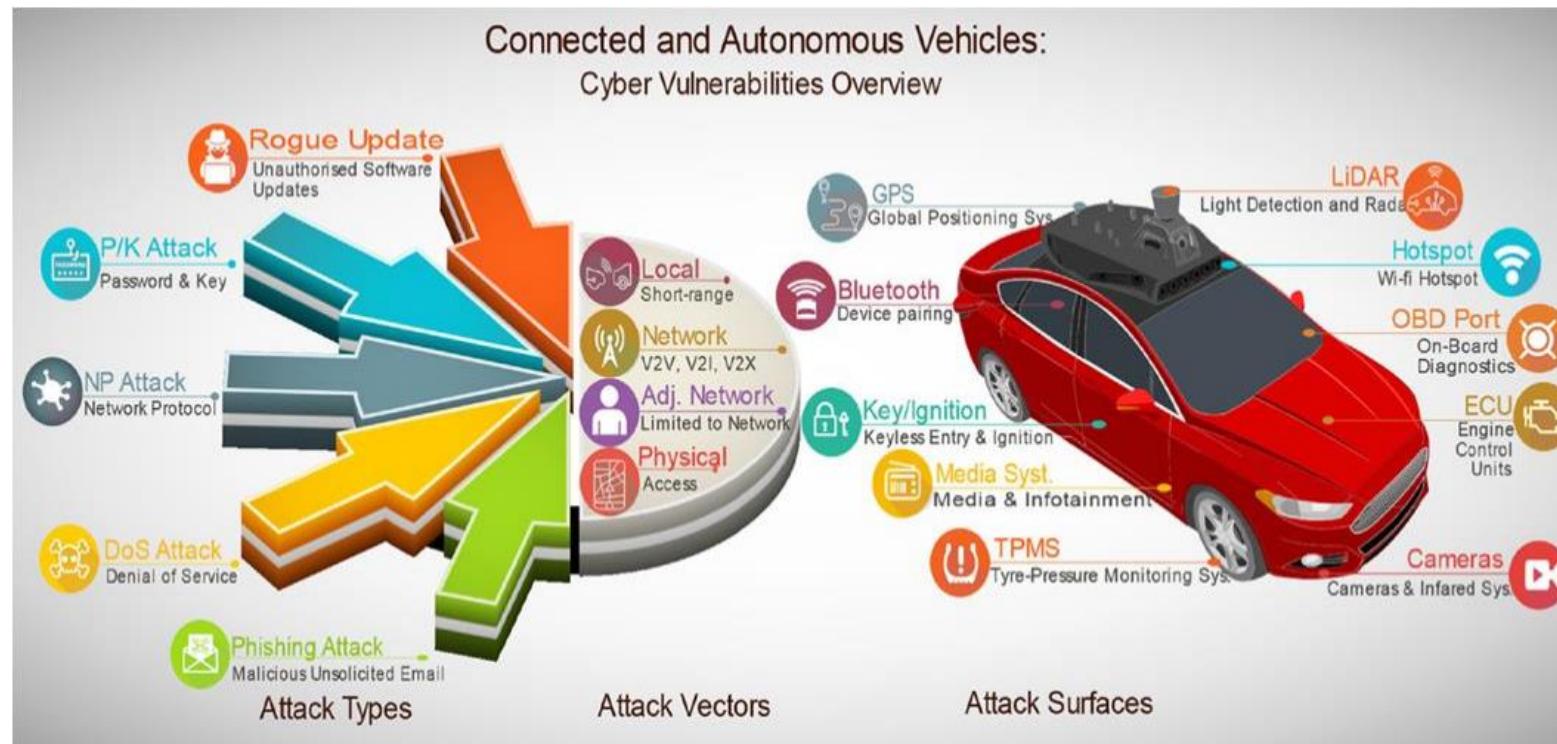
Ciberseguridad en comunicaciones “V2X”

- **Activos de los sistemas V2X:**



Ciberseguridad en comunicaciones “V2X”

- Superficies y vectores de ataque en coche autónomo:



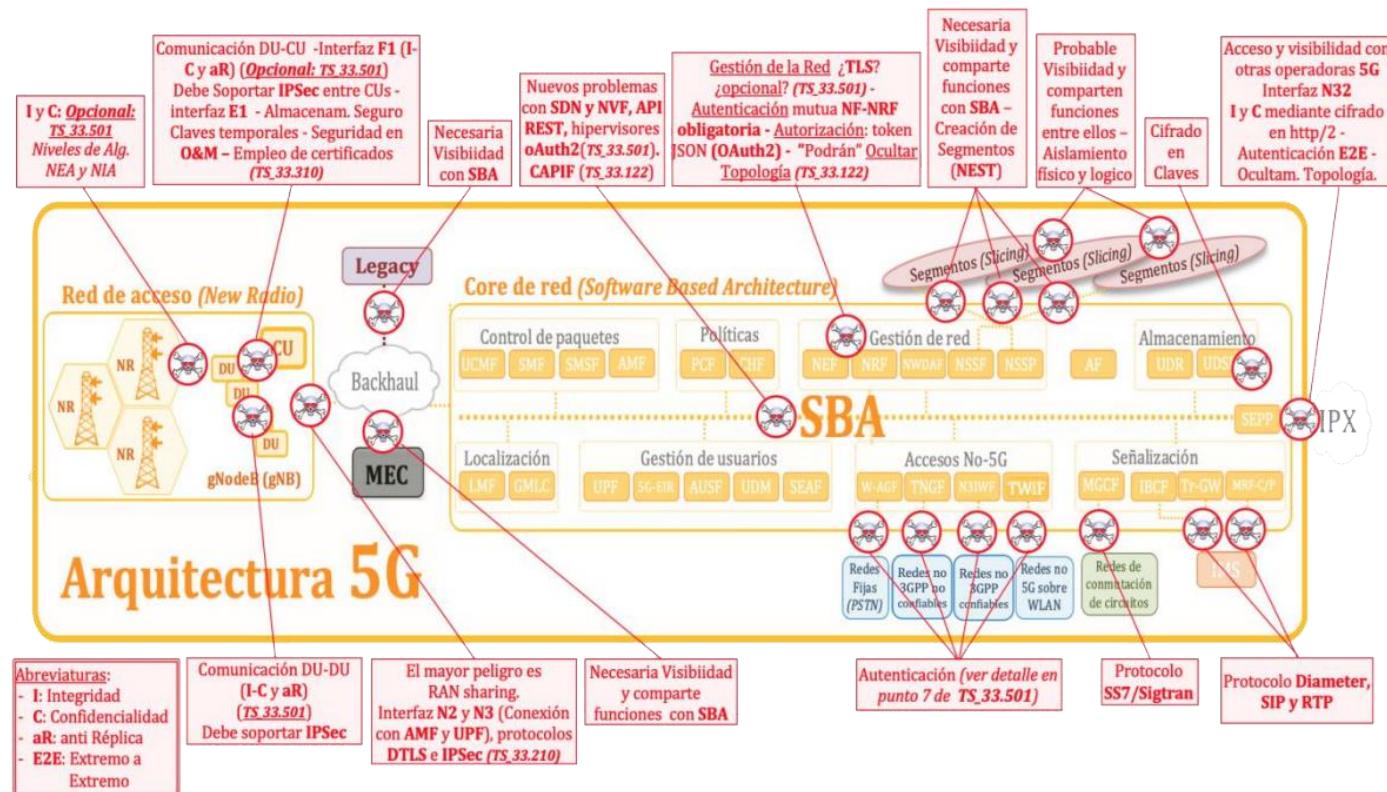
Ciberseguridad en comunicaciones “V2X”

- **Vulnerabilidades:**

- Por la propia **naturaleza** de las comunicaciones inalámbricas.
 - El canal es expuesto y abierto.
 - El medio es cambiante: perdidas de señal, desvanecimientos, etc ...
- Heredadas por los **protocolos** en las que están basadas las arquitecturas **DSRC e V2X**.
 - Propias del estándar Wifi: Denegación de servicio, Man-in-the-Middle, rogue AP, Spamming
 - Autenticación en redes celulares. Sistemas de clave pública y simétrica.
- Por los requisitos impuestos por las **necesidades** de los coches autónomos.
 - La baja latencia (ataques de Timing y Spamming)
 - Limitada capacidad de procesamiento (funciones de seguridad básicas)

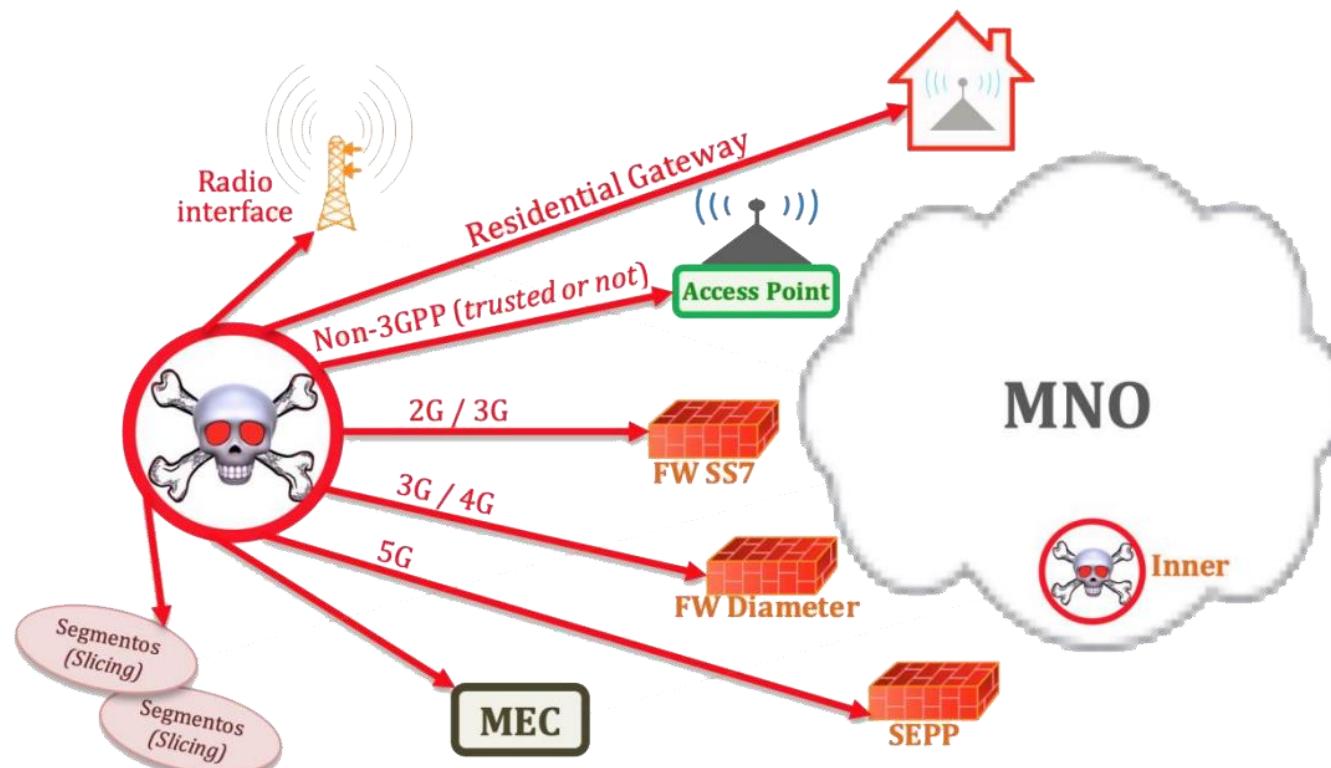
Ciberseguridad en comunicaciones “V2X”

- Vulnerabilidades en la arquitectura celular (redes 4G y 5G):



Ciberseguridad en comunicaciones “V2X”

- Vulnerabilidades: Vectores de intrusión en 5G



Ciberseguridad en comunicaciones “V2X”

- Amenazas y ataques:

- Denegación de servicio (DoS).
 - Dañar la disponibilidad del sistema, mermar la capacidad de procesamiento, ancho de banda ... reenviando masivamente (Spamming) paquetes de Broadcasting.
- Interferencia intencionada (Jamming).
 - Transmisores de señal más potentes. Uso de SDRs.
- Aislamiento (Black Hole). Ataque contra la disponibilidad
 - Incomunicación selectiva de zonas de cobertura.
- Escucha secreta (Eavesdropping). Ataque contra la confidencialidad
 - Interceptar paquetes para obtener información valiosa o re-identificación de usuarios.

Ciberseguridad en comunicaciones “V2X”

- **Amenazas y ataques:**

- **Falsificación o envenenamiento de paquetes (Spoofing).**
 - Ataque contra la integridad de la información. Se crean mensajes falsos. Señales GPS.
 - GPS Spooling, GPS Meaconing, GPS Tuneling.
- **Ataques de suplantación y enmascaramiento.**
 - El atacante finge ser un nodo de la infraestructura, una RSU, una Fentocell.
- **Man in the middle.** Ataque contra la integridad
- **Ataque Sybil.** Ataque contra la autenticidad de la información
 - El atacante crea varias identidades falsas con el objetivo de confundir a los demás vehículos.

Normas de seguridad

- **SAE (Asociación de fabricantes de automóviles).**
 - Norma SAE J3016 = Clasificación de niveles de conducción autónoma.
 - Norma SAE J3061 = Ciberseguridad durante todo el ciclo de vida del producto
- **ISO (Formada por varios organismos de estandarización mundial).**
 - Norma ISO 26262. Seguridad de los automóviles en las fases de desarrollo del software.
- **ISO/SAE (Norma conjunta).**
 - ISO/SAE 21434. Análisis de riesgos de ciberseguridad en el diseño y desarrollo de los sistemas del vehículo.
- **UNECE (Comisión europea para promocionar la cooperación económica)**
 - UNECE R155: marco para la homologación de vehículos en materia de ciberseguridad

Organizaciones de certificación

- **NHTSA (National Highway Traffic Safety Administration).**
 - Agencia estadounidense perteneciente al Departamento de Transportes.
 - Cometido: mejorar la seguridad en las carreteras y reducción de accidentes.
 - Interesada por la ciberseguridad de los vehículos (<https://www.nhtsa.gov/es>).
- **ETSI (European Telecommunications Standards Institute).**
 - Creación del estándar C-ITS: arquitectura completa de comunicaciones V2X basada en IEEE 802.11p.
 - Technical reports (TR): ETSI TR 101 607, ETSI TR 102 638, ETSI TR 103 097, ...
- **3GPP (3rd Generation Partnership Project)**
 - Consorcio de entidades para la creación de estándares de telefonía móvil.
 - Releases: especificaciones técnicas Release 17 (5G NR-eV2X)

Conclusión (conectividad)

- Vehículos = plataformas conectadas con grandes volúmenes de datos.
- Vehículos = objetivos de ataques.
- Muchas superficies de ataque y en especial el inalámbrico.
- Especial hincapié: ataques dirigidos contra la disponibilidad de servicios.
- Redes protegidas contra “malwares” y la falsificación de mensajes.
- Muy importante la implementación de medios de autenticación y de detección de ataques.
- Asegurar el acceso de los vehículos a actualizaciones de software seguras.
- Compromiso: Medios criptográficos de firma digital y de cifrado sobrecargan el sistema

Conclusiones del proyecto

- ✓ La tendencia tecnológica que hace que los vehículos cada vez están más conectados y Automatizados a través de sistemas inteligentes de transporte y de tecnologías de comunicación como el 5G.
- El conjunto de tecnologías de comunicaciones implicadas hace que las vulnerabilidades sean de amplio espectro y que abarquen desde la fase inicial del diseño de un vehículo hasta las actuaciones del usuario final.
- Dificultad para acceder a la tecnología que están implementando las marcas.
- Al converger de muchas tecnologías: oportunidades de aprendizaje transversal para diferentes ciclos relacionados no solo con la ciberseguridad sino con dichas tecnologías.
- ✓ Aparece como reto el desarrollo de entornos de simulación que didáctifiquen los diferentes puntos de ataque o vulnerabilidades del vehículo.

ESKERRIK ASKO – GRACIAS – THANK YOU

Centro San Viator
Barrio San Cristobal nº 2 – 48190 Sopuerta (Bizkaia)
T. (+34) 946 10 48 00

Alberto Laza albertolaza@sanviator.com
Erik Martínez erik.martinez@sanviator.com
<https://www.san-viator.eus/es/>

Centro Formación Somorrostro
San Juan 10- 48550 Muskiz (Bizkaia)
T. (+34) 946 70 60 45

Sendoa Florez sendoa.florez@somorrostro.com
Vicente Llarena vicente.llarena@somorrostro.com
<https://www.somorrostro.com/>