Ciberseguridad en vehículos conectados y autónomos: estudio de las comunicaciones V2X

Nombre Estudiante: Alexander González Prieto

Programa: Máster Universitario en Ciberseguridad y Privacidad

Nombre Profesor: Jordi Serra Ruiz

Fecha entrega: 06/2022

FICHA DEL TRABAJO FINAL

Título del trabajo:	Ciberseguridad en vehículos conectados y autónomos: estudio de las comunicaciones V2X
Nombre del autor:	Alexander González Prieto
Nombre del consultor:	Jordi Serra Ruiz
Fecha de entrega:	06/2022
Área del Trabajo Final:	Seguridad en redes y sistemas
Titulación:	Máster Universitario en Ciberseguridad y Privacidad

Resumen del Trabajo:

Los vehículos conectados y autónomos se están convirtiendo en una realidad. Impulsados por el desarrollo de la tecnología, se prevé que en 2030 uno de cada diez vehículos sea completamente autónomo.

Los grandes grupos industriales automovilísticos están apostando decididamente por su desarrollo y a ellos se les han unido grandes multinacionales tecnológicas. Por su parte, los gobiernos y las administraciones, siempre interesados en formas de mejorar la seguridad de las carreteras y la sostenibilidad de las grandes ciudades, han mostrado su interés en una tecnología de la que se espera que acabe con la mayoría de los accidentes, la congestión del tráfico y la polución de los grandes núcleos urbanos.

En este contexto, las comunicaciones vehiculares V2X se presentan como uno de los habilitadores esenciales de los vehículos conectados y autónomos y, por extensión, del *Internet of Vehicles*. El aumento de la digitalización y la conectividad de los vehículos es inevitable, pero también los va a volver más *hackeables*; por tanto, es primordial conocer los riesgos y las vulnerabilidades de los sistemas desde el punto de vista de la ciberseguridad.

En este TFM se analizan las tecnologías de comunicación V2X que se están investigando hoy en día. Se estudian las vulnerabilidades y las amenazas a las que están expuestas, y se proponen las correspondientes contramedidas. Finalmente, se hace una recopilación de las normas y regulaciones en materia de ciberseguridad que dentro de poco van a ser de obligado cumplimiento para que los vehículos sean, además de conectados y autónomos, ciberseguros.

Abstract:

Autonomous and connected vehicles are slowly becoming a reality. Boosted by technology development, it is expected that by 2030 one out of ten vehicles will be fully autonomous.

Traditional automobile manufacturers are seriously involved and supporting the development of connected and autonomous vehicles, and recently big technology multinationals have also joined the challenge. On the other hand, Governments and Regulators have been struggling for decades against the rise of accident rates and air pollution in big cities, and have also showed interest in a technology which promises an extensive reduction in car crashes, traffic jams and air emissions.

With this background, V2X communications have a main role in the development of the autonomous and connected vehicles and thus, in the Internet of Vehicles. With the digitalization of vehicles, essential to make them more connected, also comes and increase in the exposure of their vulnerabilities to attackers, making them more hackables. Hence, it is paramount to assess the potential cybersecurity risks of vehicle connectivity.

This TFM is a survey of current V2X communication technologies. Under a cybersecurity point of view and using a threat, vulnerability and risk approach, critical weaknesses are identified and countermeasures are proposed to remove or mitigate the risks. Finally, a summary of recently published security norms and standards is presented, as well as cybersecurity regulations which soon will be mandatory for manufacturers to comply with. In the near future vehicles will be connected and autonomous, but also cybersecure.

Palabras clave:

Ciberseguridad, vehículos conectados y autónomos, V2X, DSRC, ITS-G5, C-V2X, UNECE R155

Índice

1. introducción 1
1.1. Contexto y justificación del Trabajo 1
1.2. Objetivos del Trabajo 2
1.3. Enfoque y método seguido 3
1.4. Planificación del Trabajo 3
1.5. Breve sumario de productos obtenidos 6
1.6. Breve descripción de los otros capítulos de la memoria 6
2. Tecnología CAV y comunicaciones V2X 7
2.1. Historia de la conducción automatizada y la comunicación V2X 7
2.2. Terminología: vehículos automatizados, autónomos y conectados 9
2.3. Niveles de conducción automatizada 11
2.4. Arquitectura de sistemas en vehículos conectados y autónomos 12
2.4.1. Redes de sensores 13
2.4.2. Redes internas vehiculares 17
2.5. Comunicaciones vehiculares 19
2.5.1. Las comunicaciones V2X 19
2.5.2. Redes VANET 21
2.5.3. Arquitecturas V2X basadas en Wi-Fi 24
2.5.4. Arquitecturas V2X basadas en redes celulares 31
2.5.5. Rendimiento de los estándares: limitaciones y evolución 33
2.6. Guerra comercial 35
3. Ciberseguridad en comunicaciones V2X 37
3.1. Introducción y metodología 37
3.2. Identificación de los activos 40
3.3. Vulnerabilidades 41
3.3.1. Vulnerabilidades asociadas al diseño del sistema 41
3.3.2. Vulnerabilidades asociadas al medio inalámbrico 42
3.3.3. Vulnerabilidades asociadas a los protocolos 42
3.4. Modelado de atacantes 43
3.5. Amenazas y ataques 44
3.5.1. Denegación de servicio (DoS) 45
3.5.2. Interferencia intencionada (*jamming*) 45
3.5.3. Aislamiento (*black hole*) 45
3.5.4. Malware 46
3.5.5. Escucha secreta (*eavesdropping*) 46
3.5.6. Repudio 47
3.5.7. Falsificación o envenenamiento de paquetes (*spoofing*) 47
3.5.8. Ataques de suplantación y enmascaramiento 48
3.5.9. *Man-in-the-middle* 49
3.5.10. Ataque Sybil 50
3.6. Análisis de riesgos 50
3.7. Contramedidas 54
3.7.1. Diseño seguro de la red RF 54
3.7.2. Estudio de señales electromagnéticas 54
3.7.3. Detección de interferencias y ataques DoS 55

3.7.4. Protección contra el GPS *spoofing* 55
3.7.5. Actualizaciones OTA (*Over-the-Air update*) 56
3.7.6. Autenticación y cifrado 56
3.7.7. Marcado temporal y resumen de paquetes 57
3.7.8. Pruebas de plausibilidad de mensajes recibidos 57
3.8. Nuevas tecnologías aplicadas a la ciberseguridad CAV 59
3.8.1. Inteligencia artifical 59
3.8.2. Blockchain 61
4. Normas de seguridad y organizaciones de estandarización 62
4.1. SAE 62
4.2. ISO 62
4.3. NHTSA 65
4.4. ETSI 66
4.5. 3GPP 66
4.6. UNECE 68
4.6.1. UNECE R155 69
5. Conclusiones 72
6. Glosario 74
7. Bibliografía 75

Lista de figuras

Imagen 1. Comparación de líneas de código 8
Imagen 2. Niveles de conducción automatizada SAE J3061 11
Imagen 3. Arquitectura basada en dominios de un CAV 13
Imagen 4. Redes de sensores de un CAV 14
Imagen 5. Reconocimiento y detección mediante cámaras y LIDAR 15
Imagen 6. Ejemplo de arquitectura de adquisición de datos de un CAV 17
Imagen 7. Esquema de buses de una red interna vehicular 18
Imagen 8. Interconexión de redes internas vehiculares 19
Imagen 9. Ejemplo de ecosistema de comunicaciones V2X 21
Imagen 10. Vehicular *ad-hoc* network (VANET) 22
Imagen 11. Asignación de canales en DSRC 25
Imagen 12. Mensaje BSM 26
Imagen 13. Mensajes DSRC/WAVE definidos en la SAE J2735 27
Imagen 14. Pilas de protocolos DSRC/WAVE y C-ITS 28
Imagen 15. Asignación de canales en ITS-G5 29
Imagen 16. Arquitectura de una PKI C-ITS Trust Model 30
Imagen 17. Sidelink LTE 31
Imagen 18. Interfaces C-V2X 32
Imagen 19. Elementos del análisis de riesgos 39
Imagen 20. Activos de los sistemas V2X 40
Imagen 21. Superficies y vectores de ataque en CAV 41
Imagen 22. Aplicación del ML/DL a la ciberseguridad en CAV 60
Imagen 23. Seguridad funcional en ISO 26262 63
Imagen 24. Modelo V de la ingeniería de sistemas 64
Imagen 25. Modelo de ciberseguridad en SAE/ISO 21434 65
Imagen 26. Identificativo de cumplimiento con la norma R155 70

Tabla 1. Planificación de hitos y entregables del TFM 4
Tabla 2. Repartición de tareas por cada nivel de conducción 12
Tabla 3. Características de redes de sensores 16
Tabla 4. Aplicaciones de seguridad en redes VANET 23
Tabla 5. Aplicaciones de comodidad en redes VANET 24
Tabla 6. Requisitos y casos de uso para comunicaciones C-V2X 33
Tabla 7. Comparación de estándares de comunicación vehicular 34
Tabla 8. Cuantificación de daños 51
Tabla 9. Estimación de intención, capacidad y oportunidad 51
Tabla 10. Cálculo y valoración de la probabilidad de ataque 52
Tabla 11. Tabla de valoración de riesgos 52
Tabla 12. Ponderación de las amenazas V2X 53
Tabla 13. Reconocimiento pasivo entre estaciones 54
Tabla 14. Comparación clave simétrica vs clave pública 57
Tabla 15. Contramedidas 58
Tabla 16. Requisitos UNECE R155 de seguridad de las comunicaciones 71

1. INTRODUCCIÓN

1.1. Contexto y justificación del Trabajo

El desarrollo de tecnologías TIC aplicadas a los automóviles ha adquirido una gran importancia en el sector de la automoción en los últimos tiempos. El desarrollo de los vehículos conectados y autónomos, o CAV (*Connected and Autonomous Vehicle*), se ha convertido en uno de los grandes desafíos de empresas automovilísticas como Ford, Toyota, Tesla, Volkswagen, Renault y PSA, así como de otras empresas tecnológicas, como Uber, Apple o Google, que han irrumpido en el sector y se han unido al reto de la conducción autónoma. La nueva regulación que la Unión Europea prevé implantar a partir del 1 de julio de 2022 para la homologación de nuevos modelos viene a complementar los desafíos en materia de ciberseguridad a los que se enfrenta la industria en el corto y medio plazo.

Por su parte, las administraciones y los gobiernos han mostrado su interés en la tecnología de vehículos CAV como habilitadores de los sistemas integrados de gestión de transporte (*Intelligent Transport Systems*), una extensión del IoT aplicado al transporte que promete una mejora sustancial de la seguridad vial y de la sostenibilidad energética. Ciertamente, el impacto socio-económico que podrían traer estos sistemas es transcendente. Pensemos en una sociedad donde se han reducido en gran medida los accidentes de tráfico, los embotellamientos en las horas punta, y donde el consumo energético y la sostenibilidad de las ciudades rozan lo óptimo.

Dentro de las tecnologías habilitadoras de los vehículos conectados y autónomos, una de las más relevantes son las comunicaciones vehiculares: V2V (*Vehicle-to-Vehicle*), V2I (*Vehicle-to-Infrastructure*) o, genéricamente, V2X (*Vehicle-to-Everything*). Éstas conectan a los vehículos entre ellos y con la infraestructura para recibir información de todo tipo: situación del tráfico, accidentes en las proximidades, datos de navegación, intención de los vehículos circundantes, *infotainment*[1], etc. Para que los sistemas de conducción automatizada puedan tomar la decisión correcta es primordial un flujo constante de datos exactos y actualizados.

Por tanto, es de vital importancia que las comunicaciones sean seguras y confiables, de lo contrario las consecuencias podrían ser muy graves. Es necesario determinar con la mayor antelación posible las vulnerabilidades y amenazas en materia de ciberseguridad

[1] *Information + entertainment*

de los sistemas V2X, así como proponer las correspondientes medidas para eliminarlas o, en su caso, mitigarlas.

El resto de este documento está dividido de la siguiente manera. En el capítulo 2 se realiza un estudio de las tecnologías V2X más relevantes hoy en día. En el capítulo 3 se realiza un análisis de las vulnerabilidades, amenazas y riesgos, desde el punto de vista de la ciberseguridad, de dichas tecnologías y se proponen contramedidas. En el capítulo 4 se presentan las normas en materia de seguridad más relevantes en la actualidad y las entidades de estandarización involucradas en el desarrollo de la tecnología. En particular, se pone énfasis en la norma UNECE R155, que será de obligado cumplimiento en la Unión Europea a partir del 1 de julio de 2022. Finalmente, en el capítulo 6 se exponen las conclusiones del TFM y se proponen futuras líneas de investigación.

1.2. Objetivos del Trabajo

El objetivo de este TFM es realizar un estudio de las vulnerabilidades, amenazas y riesgos, desde el punto de vista de la ciberseguridad, que afectan a las comunicaciones V2X, aplicadas al campo de los vehículos conectados y autónomos, y proponer contramedidas que las subsanen o las mitiguen.

Este objetivo principal se divide en 3 sub-objetivos:

1. Aportar una visión de la arquitectura de los sistemas de información de los vehículos conectados y autónomos (CAV) y de las tecnologías de comunicaciones V2X dominantes actualmente. Este sub-objetivo se cubre en el capítulo 2.
2. Evaluar, desde el punto de vista de la ciberseguridad, las vulnerabilidades, amenazas y riesgos asociados a las comunicaciones V2X. Realizar un análisis de riegos y proponer contramedidas o elementos de diseño que ayuden a paliar o mitigar dichas amenazas, tomando como punto de partida las premisas y conocimientos adquiridos durante el máster. Este sub-objetivo se cubre en el capítulo 3.
3. Presentar las organizaciones de estandarización involucradas actualmente en el desarrollo de la tecnología y valorar las normativas y estándares aplicables en materia ciberseguridad de CAV disponibles hoy en día: ISO 26262, SAE J3061, ISO/SAE 21434 y UNECE R155/156, poniendo especial énfasis en ésta última por su carácter regulatorio y su obligado cumplimiento en la UE a partir de julio de 2022. Este sub-objetivo se cubre en el capítulo 4.

Respecto al alcance del TFM, en él se cubren las amenazas cuyo vector de ataque sean las comunicaciones V2X y los sistemas de posicionamiento del vehículo; es decir, ataques cuyo origen sea externo al vehículo.

Quedan por tanto fuera del alcance del TFM los ataques originados en la red interior del vehículo (*In-Vehicle Network*) o que necesiten acceso físico al mismo, como la inyección de paquetes en el bus CAN, la manipulación de sensores o el abuso de puertos USB y OBD (*On-Board Diagnostic*). Tampoco se cubren los ataques a los sistemas remotos de apertura de puertas RKE (*Remote Keyless Entry*).

1.3. Enfoque y método seguido

Para la realización del TFM se propone una metodología cualitativa, basada en la búsqueda e investigación de la documentación existente, y completándola con los conocimientos adquiridos durante el máster.

La aplicación de la metodología, capítulo por capítulo, es la siguiente:

1. Las actividades del capítulo 1 son eminentemente investigadoras; esto es, de búsqueda y análisis de documentación existente.
2. Para el capítulo 2 se plantea, en primer lugar, una metodología de evaluación cualitativa de riesgos y amenazas a partir de la información obtenida en el apartado anterior.
   Posteriormente, se determinarán los riesgos mediante un proceso de ponderación del daño potencial en el caso de la materialización de las amenazas y la probabilidad de ocurrencia de las mismas. Los resultados se presentan en forma tabular asignando un nivel de riesgo en virtud de la ponderación calculada anteriormente.
   En cuanto a la aportación de propuestas de eliminación o mitigación de amenazas, se realizará basándonos en los conocimientos obtenidos durante el máster.
3. La actividad del último capítulo es principalmente de recopilación, resumen y asociación de la información disponible.

1.4. Planificación del Trabajo

La planificación temporal del TFM toma como base el plan docente de la asignatura, donde las fechas de los entregables se equiparan a los hitos de un proyecto.

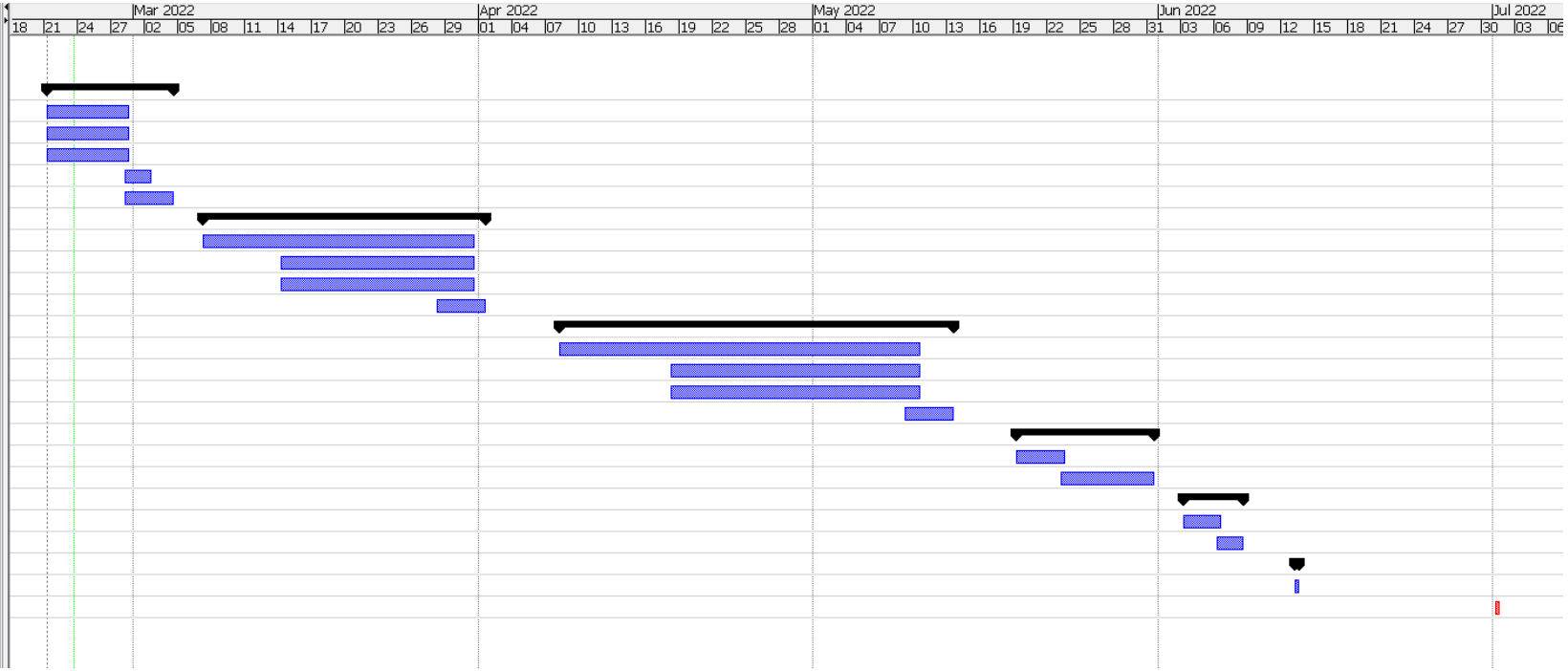
Tabla 1. Planificación de hitos y entregables del TFM

Hito	Fecha	Entregable	Gestión PMBOK
PEC 1	04.03.2022	Propuesta, objetivos y planificación	INIT + PLAN
PEC 2	03.04.2022	Informe de avance	EXEC + CTRL
PEC 3	15.05.2022	Informe de avance + conclusiones	EXEC + CTRL
Entrega memoria	31.05.2022	Memoria TFM	EXEC + CTRL
Entrega presentación	07.06.2022	Presentación vídeo	EXEC + CTRL
Defensa	13.06.2022	Defensa frente al tribunal	CTRL
Entrega notas	07.2022	Cierre de la asignatura	CLOSE

La matriz de entregables asocia cada hito del trabajo, de acuerdo a las fechas del plan docente, con un grupo de actividades de gestión de proyectos PMBOK.

Finalmente, con este plan maestro de hitos y fechas de entrega como base, creamos el siguiente cronograma de actividades con la herramienta Project Libre.

	Name	Start	Finish
1	**PEC 1**	**2/21/22 8:00 AM**	**3/4/22 5:00 PM**
2	Revisión contenidos	2/21/22 8:00 AM	2/28/22 5:00 PM
3	Planificación	2/21/22 8:00 AM	2/28/22 5:00 PM
4	Definición objetivos	2/21/22 8:00 AM	2/28/22 5:00 PM
5	Creación cronograma	2/26/22 8:00 AM	3/2/22 5:00 PM
6	Redacción PEC 1	2/28/22 8:00 AM	3/4/22 5:00 PM
7	**PEC 2**	**3/7/22 8:00 AM**	**4/1/22 5:00 PM**
8	Búsqueda de documentación	3/7/22 8:00 AM	3/31/22 5:00 PM
9	Metodología	3/14/22 8:00 AM	3/31/22 5:00 PM
10	Análisis	3/14/22 8:00 AM	3/31/22 5:00 PM
11	Redacción PEC 2	3/28/22 7:00 AM	4/1/22 5:00 PM
12	**PEC 3**	**4/8/22 8:00 AM**	**5/13/22 5:00 PM**
13	Búsqueda de documentación	4/8/22 8:00 AM	5/10/22 5:00 PM
14	Metodología	4/18/22 8:00 AM	5/10/22 5:00 PM
15	Análisis	4/18/22 8:00 AM	5/10/22 5:00 PM
16	Redacción PEC 3	5/8/22 8:00 AM	5/13/22 5:00 PM
17	**Entrega memoria**	**5/19/22 8:00 AM**	**5/31/22 5:00 PM**
18	Análisis final	5/19/22 8:00 AM	5/23/22 5:00 PM
19	Redacción memoria	5/22/22 8:00 AM	5/31/22 5:00 PM
20	**Entrega presentación**	**6/3/22 8:00 AM**	**6/8/22 5:00 PM**
21	Preparación vídeo	6/3/22 8:00 AM	6/6/22 5:00 PM
22	Preparación presentación	6/5/22 8:00 AM	6/8/22 5:00 PM
23	**Defensa TFM**	**6/13/22 8:00 AM**	**6/13/22 5:00 PM**
24	Presentación y defensa	6/13/22 8:00 AM	6/13/22 5:00 PM
25	Entrega notas	7/1/22 7:00 AM	7/1/22 5:00 PM



1.5. Breve sumario de productos obtenidos

En cuanto al análisis de las tecnologías de comunicaciones V2X, actualmente existen dos alternativas: las basadas en Wi-Fi (DSRC/WAVE y C-ITS) y las basadas en redes celulares (C-V2X). Cada una presenta sus ventajas e inconvenientes, así como vulnerabilidades derivadas de los protocolos en las que están basadas, y a día de hoy no existe una candidata clara para ser elegida como estándar mundial.

En cuanto a las amenazas, los más importantes son los ataques que se aprovechan de la exposición inherente del canal inalámbrico. Asimismo, los exigentes requisitos de latencia que demanda el sistema hacen que cualquier ataque destinado a degradarla impacte en el funcionamiento del mismo. Los ataques DoS y la interferencia intencionada (*jamming*) son amenazas a tener en cuenta por las consecuencias que pueden tener y la relativa facilidad para su ejecución. También los ataques de *malware* o los destinados a degradar el rendimiento del sistema (*spamming* y *timing attack)*. En cuanto a las contramedidas, la autenticación de usuarios y la detección temprana de ataques DoS y *jamming* son las principales a tener en cuenta.

Finalmente, en cuanto a las normas y regulaciones en materia de ciberseguridad, existen varias llamadas a convertirse en estándar en la industria, como la SAE/ISO 21344 y la UNECE R155, que será de obligado cumplimiento en la UE en julio de 2022. Todas las normas revisadas otorgan gran importancia a la ciberseguridad durante todo el proceso de diseño y ciclo de vida de los productos.

1.6. Breve descripción de los otros capítulos de la memoria

- Capítulo 1. Introducción, descripción del TFM y objetivos.
- Capítulo 2. Estudio sobre las tecnologías CAV y V2X.
- Capítulo 3. Ciberseguridad en comunicaciones V2X y análisis de riesgos.
- Capítulo 4. Normativa y organizaciones de estandarización.
- Capítulo 5. Conclusiones y futuras líneas de investigación.
- Capítulo 6. Glosario.
- Capítulo 7. Bibliografía.

2. TECNOLOGÍA CAV Y COMUNICACIONES V2X

2.1. Historia de la conducción automatizada y la comunicación V2X

Los primeros intentos de construir vehículos autoconducidos datan de 1939, en ese año General Motors presentó en el Futurama de la Exposición Universal de Nueva York un modelo que era capaz de guiarse autónomamente con campos electromagnéticos. En 1958 el modelo fue perfeccionado y se incorporaron sensores que detectaban los cambios en las corrientes inducidas por un conductor instalado en la carretera. En la década de los 70 y 80 se presentaron en Japón y Alemania los primeros vehículos equipados con sistemas de cámaras que tomaban imágenes de la carretera y las analizaban posteriormente con computadores.

Durante el resto del siglo XX se continuó experimentando, pero no ha sido hasta los comienzos del siglo XXI [1] cuando el desarrollo del software y el hardware necesarios ha permitido que los sistemas de conducción automatizada se hayan comenzado a convertir en una realidad.

En 2004, la agencia DARPA organizó su primer Grand Challenge [2], en el cual se ofrecía 1$ millón a quien consiguiera diseñar un ingenio robótico capaz de realizar un trayecto de 240 km en el desierto de Mojave de manera automática. Aquel año ningún participante consiguió terminar el trayecto; sin embargo, al año siguiente, cinco participantes lo consiguieron utilizando navegación GPS y sensores LIDAR.

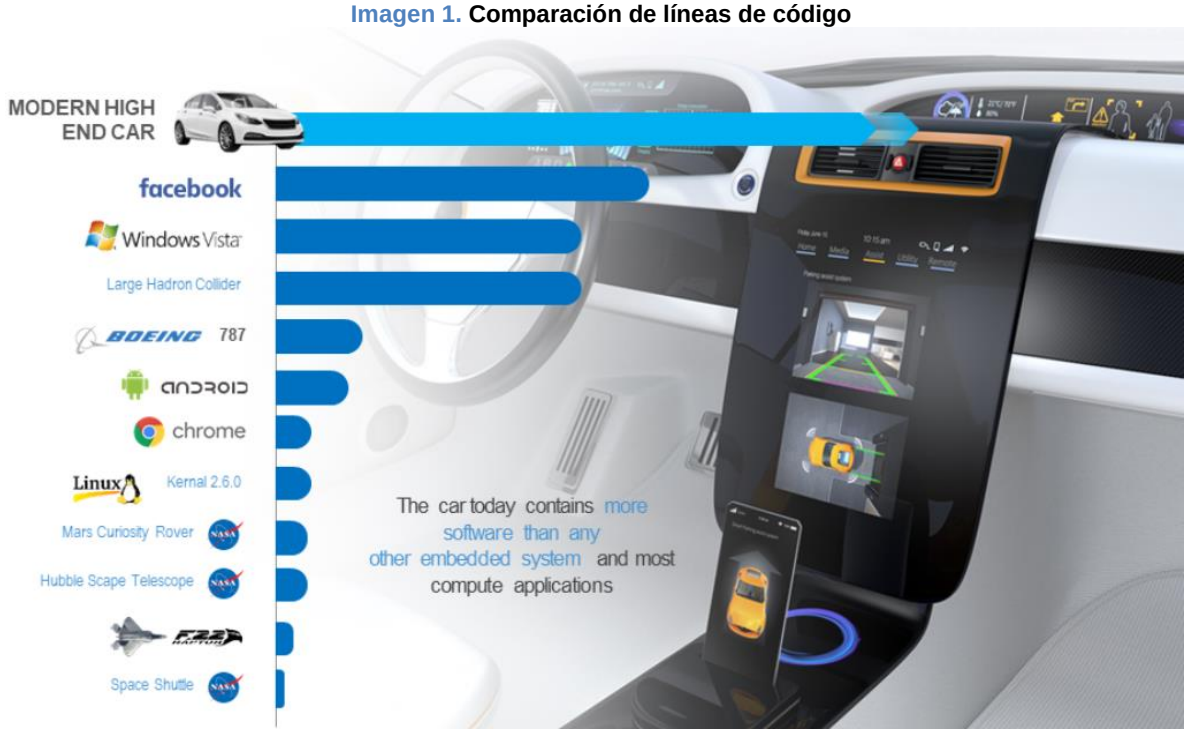
La década de 2010 ha sido decisiva para el desarrollo de la tecnología en el campo de los vehículos autónomos. Google ya había empezado a trabajar discretamente en el proyecto en 2009, y grandes grupos industriales como General Motors, Ford, Volkswagen, Audi, Nissan y Toyota se han ido uniendo al desafío que supone diseñar y construir vehículos que se conduzcan autónomamente y se comuniquen entre ellos, y la infraestructura, de manera segura y coste-eficiente.

El primero en anunciar, en 2014, una primera versión funcional del software de autopiloto fue Tesla Motors, un fabricante de automóviles fundado en 2003. Este software permite al vehículo mover la dirección, acelerar, frenar y aparcar autónomamente basándose en algoritmos de reconocimiento de imagen [3]. Desde mediados de 2015 el autopiloto está disponible a los vehículos Tesla por medio de una actualización de software.

El hecho de que grandes grupos tecnológicos como Google, Apple o Uber hayan entrado en el sector da una idea del papel que juegan los sistemas informáticos en el desafío del coche autónomo: algoritmos de reconocimiento de imágenes, sensores de varios tipos, capacidad de procesamiento en tiempo real, inteligencia

artificial, etc. Además de ingenios mecánicos, los vehículos del futuro serán plataformas de sistemas de tecnologías de la información y gestión de volúmenes de datos. Los grandes grupos industriales que han dominado el sector automovilístico en el siglo XX – General Motors, Ford, Renault, Volkswagen o Toyota – tienen que competir a partir de ahora en el dominio de las multinacionales tecnológicas, o arriesgarse a que una innovación disruptiva les saque del mercado.

Imagen 1. Comparación de líneas de código



Fuente: https://choice.com.au

El punto de partida de la investigación en materia de comunicaciones vehiculares V2X se sitúa en torno al año 1970 en Estados Unidos y Japón, y los avances se han desarrollado en paralelo a la investigación de tecnologías de conducción automatizada. El hito que marca el punto de inflexión en la investigación es la asignación en 1999, por parte de la FCC[2], de una banda de frecuencias en torno a los 5.9 GHz para la experimentación de comunicaciones inalámbricas de corto alcance (DSRC) para vehículos.

El desarrollo subsiguiente culminó en 2010 con la publicación por parte del IEEE del primer estándar específicamente creado para las comunicaciones vehiculares inalámbricas, IEEE 802.11p. Poco después se definió la arquitectura completa de protocolos DSRC/WAVE basada en IEEE 802.11p. La versión europea, desarrollada por el ETSI durante los años 2010, se denomina C-ITS y también está basada en IEEE 802.11p. Por su parte, en Japón se ha desarrollado el estándar ARIB STD-

[2] La *Federal Communications Commisison* (FCC) es una agencia gubernamental encargada de regular las radiocomunicaciones y administrar el espectro radioeléctrico en EE.UU. https://www.fcc.gov/

T109, basado igualmente en IEEE 802.11p pero con diferencias importantes respecto a las versiones estadounidense y europea.

En 2016, el grupo 3GPP publicó en su Release 14 la posibilidad de que redes celulares basadas en LTE (precursor del 4G) pudieran dar soporte a las comunicaciones vehiculares, e inmediatamente varios grupos de investigación comenzaron a explorar las posibilidades que ofrecía. El 3GPP ha ido perfeccionando el estándar en sucesivas actualizaciones hasta incluir soporte a las comunicaciones V2X en la norma de 5G. De acuerdo a los últimos estudios hechos hasta la fecha, éste igualaría, e incluso mejoraría, el rendimiento de DSRC/WAVE y C-ITS. Sea como fuere, las comunicaciones V2X se han convertido en un capítulo fijo en próximas Releases de 3GPP, y se espera que se siga desarrollando y perfeccionando en la próxima publicación de 6G.

2.2. Terminología: vehículos automatizados, autónomos y conectados

Tradicionalmente, se ha venido utilizando el término “vehículo automatizado” para aquellos vehículos en los cuales al menos una acción de control relacionada con la seguridad de la conducción ocurre sin intervención humana; por ejemplo, girar el volante o frenar. Dentro de éstos, se distinguen los vehículos autónomos y los conectados, dependiendo del origen de los datos que se usan para tomar dichas decisiones de control.

En el caso de los vehículos autónomos el origen son los sensores del vehículo; mientras que en el caso de los conectados, los sistemas del vehículo obtienen los datos por medio del intercambio de comunicaciones inalámbricas con otros vehículos o con la infraestructura de la vía. Los vehículos conectados y autónomos, o CAV, son aquellos que obtienen su información simultáneamente de los sensores instalados y de las comunicaciones V2X.

En 2021, la SAE (*Society of Automotive Engineers*), una asociación estadounidense de fabricantes de automóviles dedicada a la estandarización, consideró necesaria una reformulación de la terminología al considerar que algunos términos se estaban quedando desfasados. En la norma se considera discontinuado el término “conducción autónoma”, al juzgarlo obsoleto y proveniente del ámbito de la robótica y la inteligencia artificial, y se recomienda sustituirlo por el concepto de “conducción automatizada”. También desaconseja el uso de términos como auto-conducido (*self-driving*), no tripulado (*unmaned*) o sin conductor (*driveless*), ya que podrían llevar a confusión al lector.

Si bien la propuesta de la SAE puede llegar a implantarse en el sector dentro de un tiempo, en este TFM seguiremos empleando las definiciones habituales para facilitar

la lectura y no sobrecargar en exceso la terminología. Por consiguiente, emplearemos la clasificación “vehículo automatizado”, “vehículo autónomo” y “vehículo conectado y autónomo” (CAV) en los términos que hemos descrito anteriormente.

Además, hay otros términos empleados en el mundo de la conducción autónoma que conviene definir.

Advanced Driver Assistance Systems (ADAS). Sistemas software y hardware instalados en el vehículo que, de manera continuada, están activos y conducen el vehículo.

Dynamic Driving Task (DDT). Todas las acciones implicadas en el proceso de conducción en condiciones normales en una carretera y que pueden ser ejecutadas por un humano o por un elemento del ADAS. Dentro de esta categoría se incluye todo lo relacionado con el movimiento del vehículo (aceleración, frenado, movimiento de la dirección, etc.).

Fallback. Una respuesta que puede ser ejecutada por un humano o por un ADAS destinada a sacar el vehículo de una condición de riesgo (por ejemplo, detener el vehículo en el arcén ante un fallo del sistema). Por definición, una DDT no puede incluir una acción de *fallback*.

Minimal Risk Condition (MRC). Condición de mínimo riesgo de un vehículo (por ejemplo, detenido o parado). Las *fallback* son acciones destinadas a situar al vehículo en condición MRC.

Object and Event Detection and Response (OEDR). Procesos destinados a la monitorización del entorno (estado de las vías, acciones de los otros usuarios, etc.).

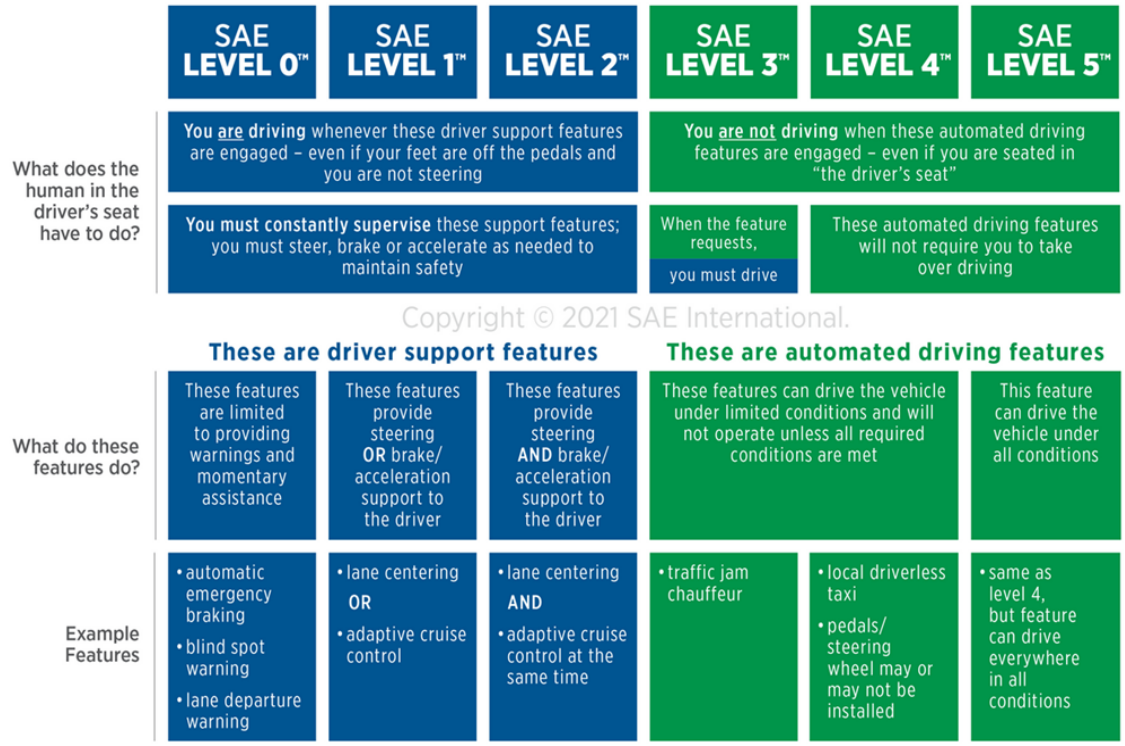
Operational Design Domain (ODD). Son el conjunto de condiciones de la vía, del trazado o meteorológicas que el ADAS está habilitado para gestionar por diseño. Cuando el vehículo sale fuera del ODD se entiende que circula en condiciones para las que no fue diseñado, lo que puede ser motivos de que una maniobra de *fallback* sea requerida. Por ejemplo, un ADAS puede estar diseñado para funcionar en una vía seca, recta y en condiciones de día y sin inclemencias meteorológicas.

Active Safety Systems (ASS). Son sistemas de asistencia al conductor que intervienen en situaciones de peligro o emergencia. Si bien pueden realizar alguna función automática, no se consideran sistemas de conducción automatizada porque no descargan al conductor de ejecutar ninguna de sus tareas, ni total ni parcialmente; además, actúan de manera temporal y momentánea, esto es, no continuada. Ejemplos: *Electronic Stability Control* (ESC), *Automatic Emergency Braking* (AEB), y ciertos tipos de asistencia a la conducción como los sistemas de ayuda para mantenerse dentro del carril *Lane Keeping Assistance* (LKA).

2.3. Niveles de conducción automatizada

En 2014, la SAE clasificó, en la primera edición de la norma SAE J3016, las tecnologías de conducción autónoma en una escala de 6 niveles (de 0 a 5) en base al nivel de intervención humana requerido.

Imagen 2. Niveles de conducción automatizada SAE J3061



Fuente: SAE International

En la tabla I de la SAE J3016 se definen los niveles de conducción del 0 al 5, donde el 0 es un vehículo sin ningún tipo de asistencia y el 5 corresponde a un vehículo que es capaz de conducir automáticamente sin ninguna intervención humana.

- **Nivel 0** (*no automation*). Sin sistemas de automatización de la conducción, todas las DDT son ejecutadas por el conductor. No obstante, los vehículos pueden equipar sistemas ASS.
- **Nivel 1** (*hands-on*). Asistencia al conductor. Equipa sistemas automáticos de control longitudinal o lateral.
- **Nivel 2** (*hands-off*). Automatización parcial de la conducción. Equipa sistemas automáticos de control longitudinal y lateral que actúan siempre bajo la supervisión del conductor.
- **Nivel 3** (*eyes-off*). Automatización condicional de la conducción. El ADAS ejecuta varias DDT y supervisa posibles errores o situaciones de emergencia, en cuyo caso avisa al conductor para que ejecute manualmente la maniobra de *fallback* correspondiente.

- **Nivel 4** (*mind-off*). Alto nivel de automatización de la conducción. Idéntico al anterior pero el ADAS es capaz de detectar las situaciones de emergencia y ejecutar automáticamente la acción de *fallback* correspondiente. Sujeto a unas condiciones de entorno ODD determinadas.
- **Nivel 5**. Automatización completa. El ADAS es capaz de manejarse completamente de principio a fin y en todo tipo de condiciones de entorno.

Normalmente, el término ADAS se aplica a los sistemas de niveles 3,4 y 5, dado que son sistemas hardware y software que, colectivamente, son capaces de realizar alguna DDT de forma continuada en el tiempo.

Tabla 2. Repartición de tareas por cada nivel de conducción

Level	J3016 Level Name	Steering & Speed	Objects & Environment	Detect DDT Failures	Detect Vehicle Faults	Perform Fallback	ODD Scope	Other Safety
0	No Driving Automation	Driver	Driver	Driver	Driver	Driver	n/a	Driver
1	Driver Assistance	Split	Driver	Driver	Driver	Driver	Limited	Driver
2	Partial Driving Automation	ADS	Driver	Driver	Driver	Driver	Limited	Driver
3	Conditional Driving Automation	ADS	ADS	ADS	Driver	Driver	Limited	Driver
4	High Driving Automation	ADS	ADS	ADS	ADS	ADS	Limited	Driver
5	Full Driving Automation	ADS	ADS	ADS	ADS	ADS	"Unlimited"	Driver

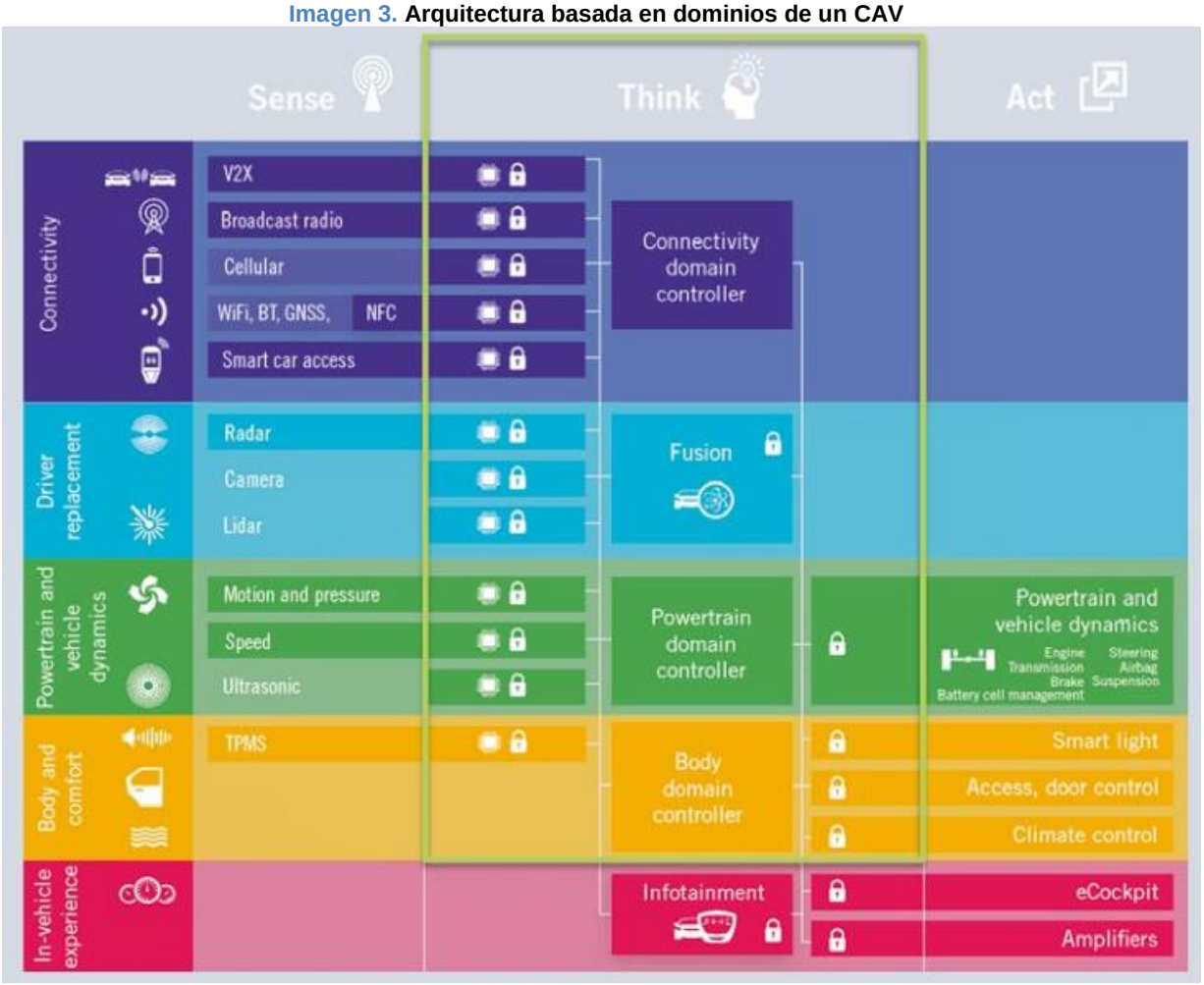
Fuente: https://users.ece.cmu.edu/~koopman/j3016/

2.4. Arquitectura de sistemas en vehículos conectados y autónomos

Un vehículo autónomo es aquel que, basándose en información del entorno recibida por una red de sensores, es capaz de tomar decisiones y ejecutar acciones DDT de una manera segura y sin quebrantar ninguna norma de circulación. Además, si el vehículo soporta comunicaciones V2X, diremos que es un vehículo conectado y autónomo o CAV.

El funcionamiento de un CAV se resume en tres dominios: percepción del entorno mediante sensores y comunicaciones V2X, decisión y acción.

Imagen 3. Arquitectura basada en dominios de un CAV



Fuente: NXP Semiconductor

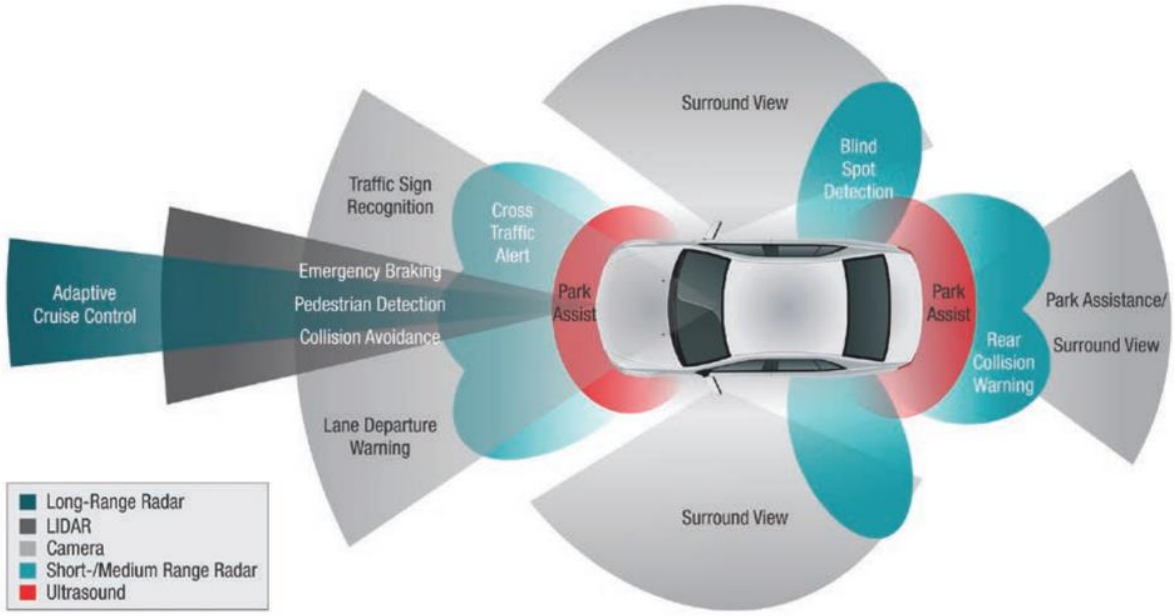
Aunque las fases de decisión y actuación quedan fuera del alcance de este TFM, en los capítulos siguientes daremos una breve introducción a los sistemas de adquisición de información (principalmente redes de sensores) y a la arquitectura de la red interna del vehículo por su estrecha relación con los sistemas V2X.

2.4.1. Redes de sensores

La función de los sensores es obtener la mayor cantidad de información del entorno para ser usada por los sistemas de decisión del vehículo.

Principalmente, los datos que se recopilan tienen que ver con el posicionamiento del vehículo y la ubicación de los obstáculos de las inmediaciones [4].

Imagen 4. Redes de sensores de un CAV



Fuente: https://saemobilus.sae.org

Los sistemas de detección y ubicación de obstáculos que se están desarrollando se dividen básicamente en dos grupos: los basados en cámaras y los basados en sistemas de detección remota (RADAR, LIDAR o ultrasonidos).

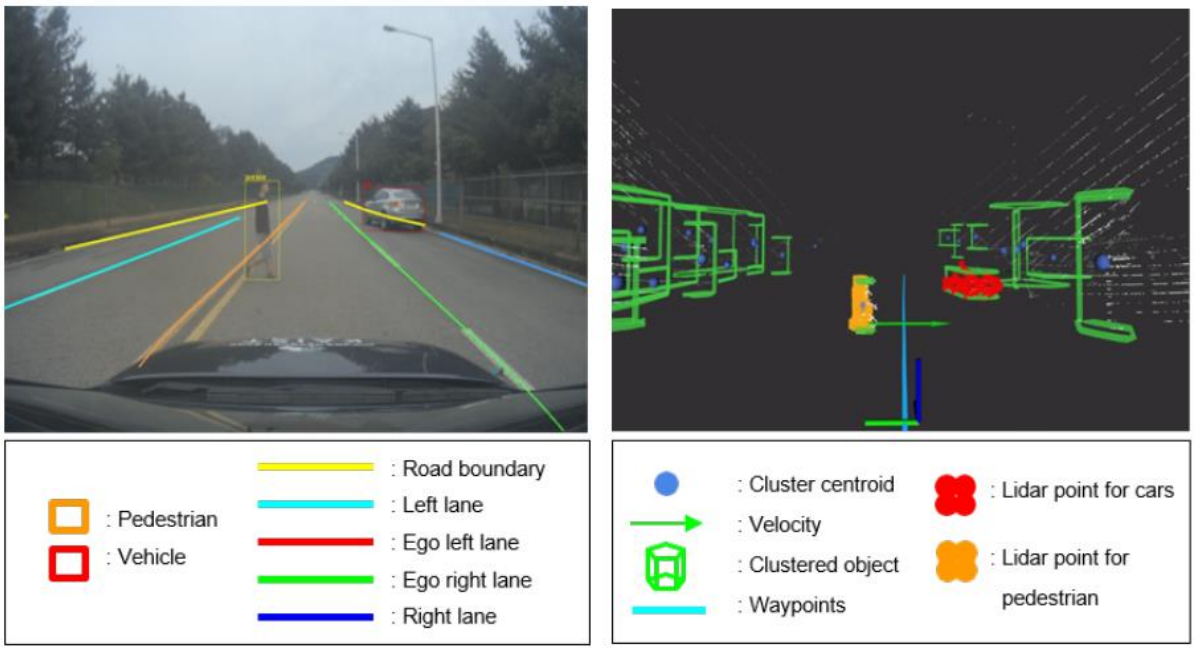
Los sensores que usan ultrasonidos operan en la banda de los 20 KHz – 40 KHz y su funcionamiento se basa en la medición del retardo de señales sonoras de eco. Su alcance limitado (generalmente menor de 3 m) y su direccionalidad les hace adecuados para aplicaciones de corto alcance como ayudas al aparcamiento y detección de proximidad. También, el trabajar en distancias cortas hace que sean relativamente inmunes a las malas condiciones meteorológicas.

Los radares basan su funcionamiento en haces de frecuencia de diferentes bandas: 24 GHz, 60 GHz ó 76-77 GHz [5] y se utilizan principalmente para la detección de obstáculos lejanos en un rango hasta los 200 m. La distancia al objeto se calcula midiendo el retraso entre la señal emitida y el eco recibido. Existe un compromiso entre distancia y campo de visión, distancias más lejanas requieren un campo de visión más estrecho y viceversa. Suelen ser útiles para el control del vehículo en modo “crucero” (*Adaptative Control Cruise*) puesto que permiten el control detectando y siguiendo vehículos en la lejanía.

El funcionamiento del LIDAR es parecido al del RADAR, pero en vez de haces de radiación electromagnética se usan rayos de luz infrarroja, normalmente en torno a los 1550 nm, con un alcance máximo de 200 m aproximadamente. Los sistemas generalmente radian varios haces para mapear el entorno y crear un mapa interno de las inmediaciones. Suelen ser más precisos que los radares en condiciones de baja velocidad, pero también ofrecen peor rendimiento con lluvia o niebla y son más costosos en términos económicos y de espacio (son más caros y necesitan más

espacio para la instalación). Además, la precisión del LIDAR decrece con la velocidad hasta llegar a un límite y por esta razón suele usarse de forma complementaria a los radares y no sustitutiva. El binomio LIDAR/RADAR suele ser habitual en las arquitecturas de los vehículos Waymo de Google.

Imagen 5. Reconocimiento y detección mediante cámaras y LIDAR



Fuente: Jung et al. [6]

Otra forma de complementar los sistemas RADAR es mediante cámaras y sistemas de reconocimiento de imágenes. Particularmente, esta es la opción de referencia adoptada por Tesla en sus vehículos para la detección de obstáculos y mapeo del entorno, aunque en mayor o menor medida todos los vehículos autónomos las usan. Dependiendo de la naturaleza de la lente, las cámaras pueden detectar objetos en un alcance máximo de 250 m.

Los sistemas de reconocimiento de imágenes utilizan varias técnicas; por ejemplo, las aplicaciones de mantenimiento en el carril utilizan algoritmos que detectan los cambios de contraste entre el negro del asfalto y el blanco de las líneas de la carretera. La combinación de las imágenes captadas por pares de cámaras, o visión estéreo [7], sirve para determinar la profundidad y altura de los objetos. Finalmente, también pueden usarse cámaras termografías para obtener imágenes térmicas de las vías.

En general, los sistemas de reconocimiento de imágenes son más baratos y requieren menos espacio que el LIDAR, pero necesitan más capacidad de procesamiento y algoritmos más complejos como por ejemplo creación de imágenes en 3D, detección de movimiento o *tracking*.

Tabla 3. **Características de redes de sensores**

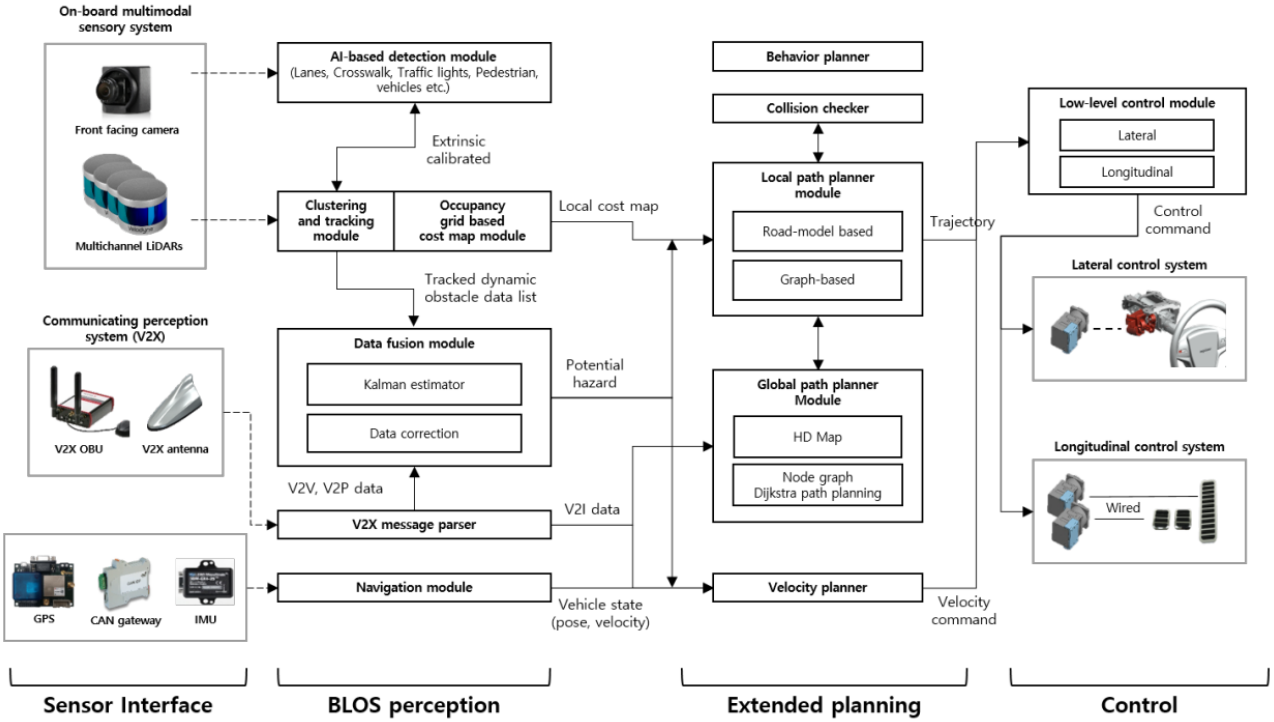
SENSOR	CARACTERÍSTICAS
Cámaras	• Alcance máximo: 250 m • Requiere alta capacidad de procesamiento lo cual puede impactar a las aplicaciones en tiempo real • Mejor resolución que RADAR y LIDAR
RADAR	• Alcance máximo: 200 m • Genera falsos positivos en objetos metálicos • Menor resolución que LIDAR y cámaras
LIDAR	• Alcance máximo: 200 m • Muy dependiente de las condiciones meteorológicas • Alto coste
Ultrasonidos	• Alcance máximo: 3 m • No adecuado para altas velocidades (alta latencia) • Baja resolución comparado con RADAR y LIDAR • Buena relación coste / eficiencia para distancias cortas

Fuente: Ahangar et al.

En cuanto a los sistemas de ubicación del vehículo, lo normal es que se haga uso de alguna tecnología GNSS de posicionamiento satelital, como podrían ser GPS, GLONASS, BDS o GALILEO. Estos sistemas llevan asociado siempre un error de posición que en entornos urbanos puede llegar a los 100 m, por lo que suelen complementarse con sistemas inerciales de posición como giróscopos o acelerómetros. Adicionalmente, los radares o el LIDAR también pueden contribuir a la determinación de la posición.

En conclusión, las redes de sensores son fundamentales para proveer de datos a los vehículos. Sin embargo, los sensores y la información que pueden obtener siempre va a ser limitada: una cámara nunca va a poder obtener imágenes de lo que hay detrás de un obstáculo y un sistema basado en ondas electromagnéticas está limitado por la línea de visión o LOS (*line of sight*). Por consiguiente, es necesario ampliar el alcance más allá de la línea de visión de los sensores y esto lo conseguimos con las comunicaciones vehiculares. V2V pone a disposición del usuario la información obtenida por los sensores de otros vehículos y V2I comunica al vehículo con la infraestructura, ampliando la línea de visión de manera casi ilimitada.

Imagen 6. Ejemplo de arquitectura de adquisición de datos de un CAV



Fuente: Jung et al.

2.4.2. Redes internas vehiculares

Las redes internas vehiculares (*In-Vehicle Network*) están formadas por la interconexión de los sub-sistemas electrónicos internos del vehículo. A las unidades de control se las conoce como ECU (*Electronic Control Unit*), y su número en un vehículo moderno puede llegar al centenar [8]. Un tipo particular de ECU son las OBU (*On-Board Unit*), encargadas de realizar las comunicaciones inalámbricas V2X.

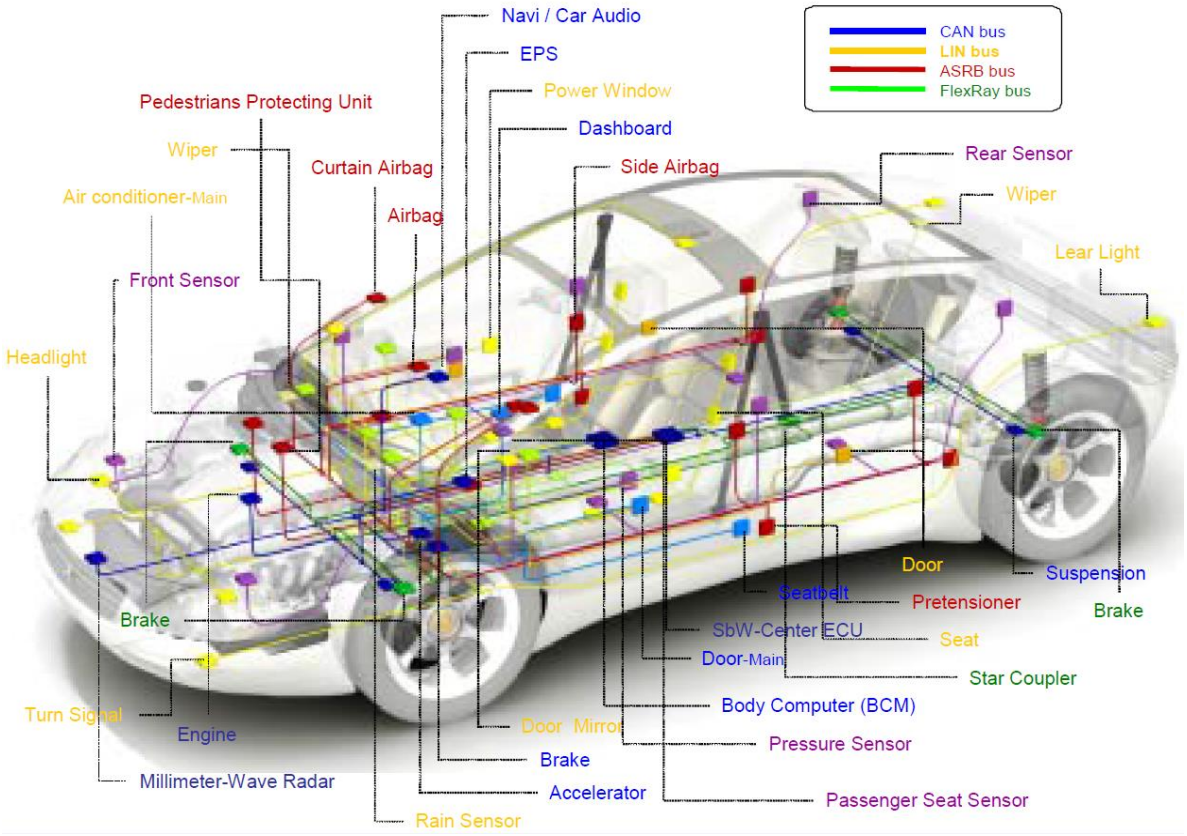
La función de la electrónica de los vehículos ha ido aumentando con los años, y hoy en día controlan varios aspectos relacionados con la conducción, confort del habitáculo, seguridad, etc. Dependiendo de la funcionalidad necesaria se forman diferentes subredes o dominios que se interconectan entre ellos mediante *gateways* o controladores de dominio DCU (*Domain Controller Unit*). En base a los requisitos de velocidad de datos y latencia, cada subred utilizará determinados protocolos y controladores de dominio.

- CAN (*Controller Area Network*), protocolo de alta velocidad para interconectar sistemas críticos del vehículo relacionados con el motor, la transmisión o la dirección;

- LIN (*Local Interconnect Network*), para sistemas con requisitos más bajos de latencia como apertura de puertas o climatización;

- FlexRay, para sistemas de control de frenado, dirección y *airbag*, y
- MOST (*Media Oriented Systems Transport*), para sistemas de *infotainment*.

Imagen 7. Esquema de buses de una red interna vehicular

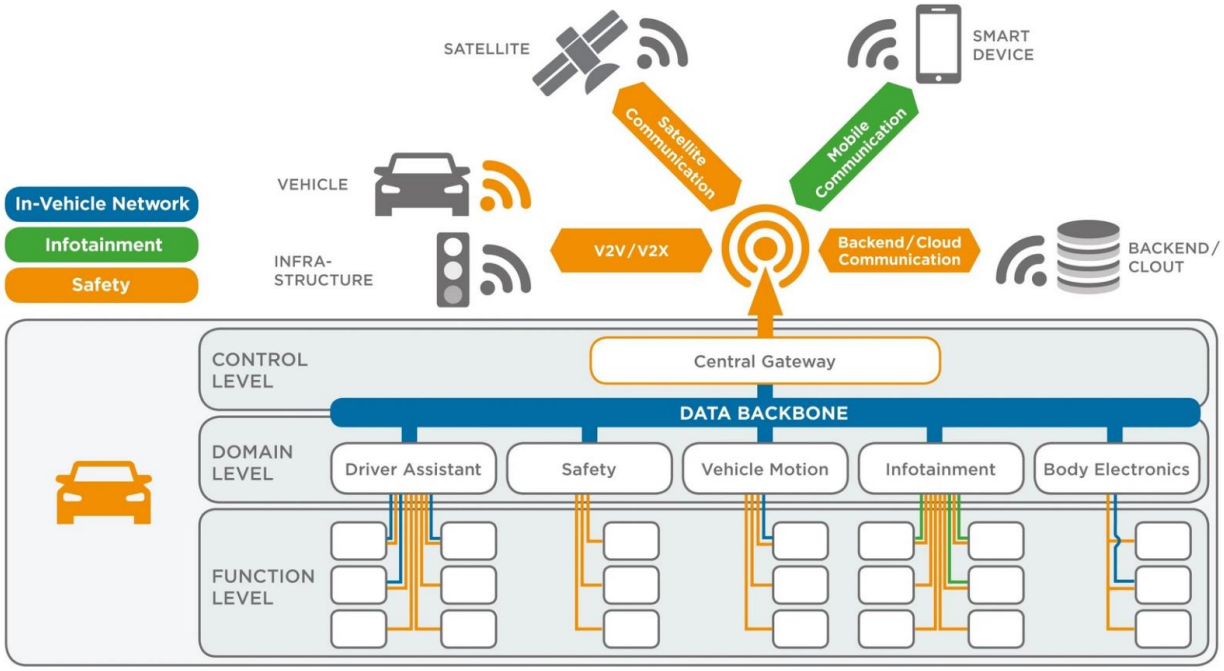


Cada uno de estos protocolos tiene características diferentes y tiene que lidiar con su propio set de vulnerabilidades. Las pasarelas que interconectan las subredes suelen utilizar buses CAN de alta velocidad.

En los últimos tiempos se han ido añadiendo interfaces de entrada y salida a las redes vehiculares como puertos USB, bluetooth o Wi-Fi que ofrecen más conectividad a los ocupantes y mejoran la experiencia de viajar en automóvil, pero también complican el diseño de la red interna del vehículo y lo vuelven más *hackeable*.

El desarrollo de las tecnologías de vehículos CAV va a contribuir al incremento del número de unidades ECU así como al aumento de los requisitos de capacidad de procesamiento y de ancho de banda. Las estimaciones son que un vehículo autónomo podrá llegar a generar 40 TB de datos en un día y a necesitar un ancho de banda de 50 Mbit/s [9] [10].

Imagen 8. Interconexión de redes internas vehiculares



Fuente: TE Automotive

2.5. Comunicaciones vehiculares

2.5.1. Las comunicaciones V2X

Hemos visto que los CAV necesitan un flujo de datos constante con información sobre el entorno. Las comunicaciones externas que el vehículo establece con otros vehículos y la infraestructura constituyen una fuente adicional de valiosa información "más allá del horizonte" que no puede ser suministrada por la red de sensores del vehículo.

Dependiendo del tipo de enlace, nos podemos encontrar con varios tipos de comunicaciones vehiculares:

- **Vehículo a vehículo (V2V)**. Intercambio de información en tiempo real entre vehículos que se encuentren próximos. Generalmente, se trasmite y recibe información relativa a la velocidad del vehículo, su rumbo o intención. La comunicación es descentralizada; cada vehículo constituye un nodo de la red que puede recibir información y retransmitirla.

- **Vehículo a infraestructura (V2I)**. Intercambio de información entre los vehículos y la infraestructura de la vía. Los vehículos pueden recibir información de sensores instalados en la vía sobre el estado de los semáforos, accidentes, aparcamientos libres, etc. A su vez, el vehículo

también envía información propia, o reenvía la recibida de otros vehículos, a la infraestructura con el objetivo de mejorar la circulación y disminuir el número de accidentes.

- **Vehículo a peatón (V2P)**. Los peatones también pueden estar preparados para comunicarse con el ecosistema. Algunas finalidades pueden ser informar por medio de aplicaciones móviles de la presencia de bicicletas, sillas de ruedas o niños en las proximidades.

- **Vehículo a red (V2N)**. Originalmente, el término V2N se refería al intercambio de mensajes con la infraestructura pero, con la aparición de comunicación vehicular basada en redes celulares, el término V2N ha pasado a referirse a la recepción de información proveniente de las redes de operadores móviles LTE o 5G. El tipo de información recibida puede ser de variados tipos, desde información meteorológica hasta información sobre el estado del tráfico, rutas alternativas o *infotainment*.

El término V2X (*Vehicle-to-Everything*) se usa para aglutinar todas las comunicaciones mencionadas anteriormente; por tanto, V2X es un término genérico que representa cualquier comunicación originada desde el vehículo.

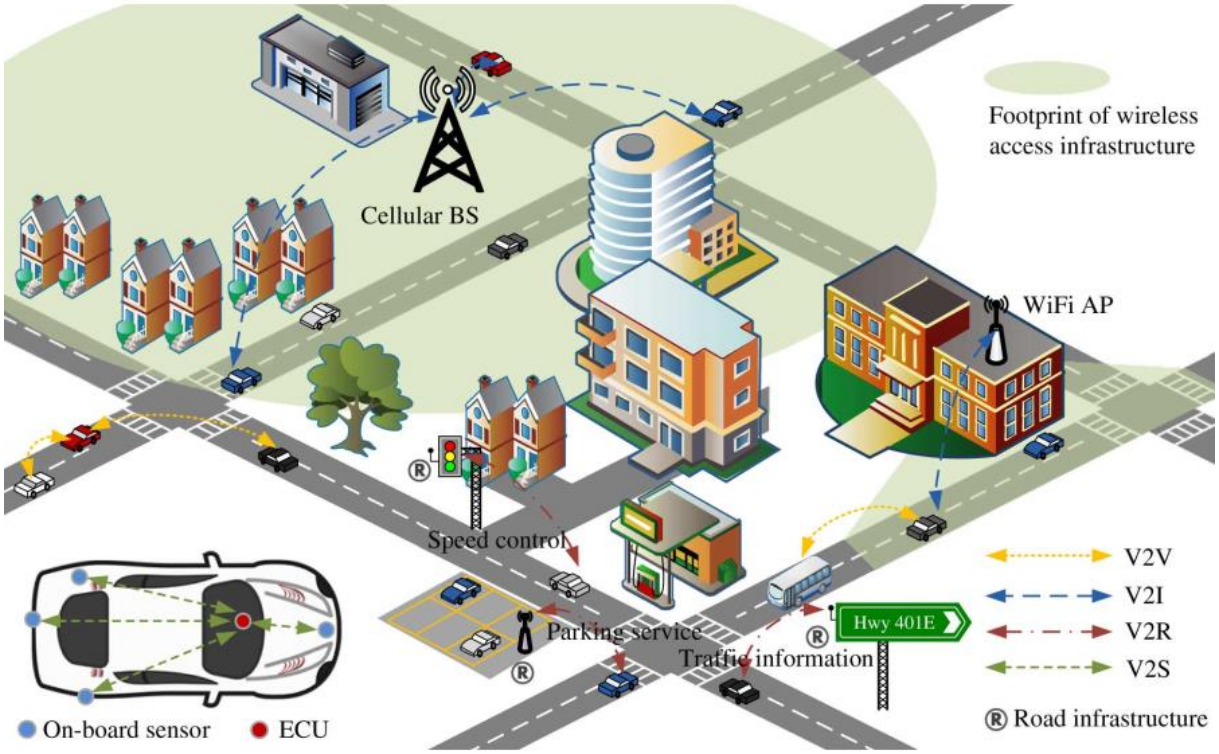
En este entorno, los requisitos cruciales para las comunicaciones vehiculares son la baja latencia (retraso o tiempo transcurrido entre que un emisor emite un mensaje y es recibido y procesado por el receptor) y la adaptación a un medio altamente cambiante. Adicionalmente y dependiendo de la aplicación, también se puede requerir buena fiabilidad en las conexiones y alta velocidad de transmisión de datos.

Dos vehículos viajando a 100 km/h en sentido contrario (con velocidad relativa de 200 km/h) interactúan durante breves segundos, por lo que la baja latencia es indispensable para que el intercambio de datos se haga de forma rápida y segura.

Normalmente, se estima que para aplicaciones típicas V2X (p. ej. *collision warning*) la latencia no puede superar los 100 ms. Sin embargo, en aplicaciones relacionadas con la conducción autónoma los requisitos de latencia pueden llegar a bajar hasta los 5 – 10 ms [11].

Por otra parte, también es fundamental que las comunicaciones sean capaces de adaptarse a los cambios en las condiciones de la vía (meteorología, tráfico, etc.).

Imagen 9. Ejemplo de ecosistema de comunicaciones V2X



Fuente: Lu et al. [12]

2.5.2. Redes VANET

A nivel de red, los vehículos intercambian datos estableciendo redes inalámbricas *ad-hoc* conocidas como redes VANET (*Vehicular Ad-hoc NETwork*). De manera característica, estas redes son:

- descentralizadas, cada elemento puede actuar de enrutador de paquetes de manera dinámica de acuerdo a los algoritmos de encaminamiento, y
- espontáneas; es decir, se establecen, organizan y gestionan de manera autónoma sin necesidad una infraestructura fija subyacente, como *routers* o equipos de red.

Las redes VANET se derivan de las redes *ad-hoc* móviles MANET (*Mobile Ad-hoc NETwork*) a las que se les añaden modificaciones destinadas a mejorar requisitos adicionales de ancho de banda, fiabilidad y alcance [13].

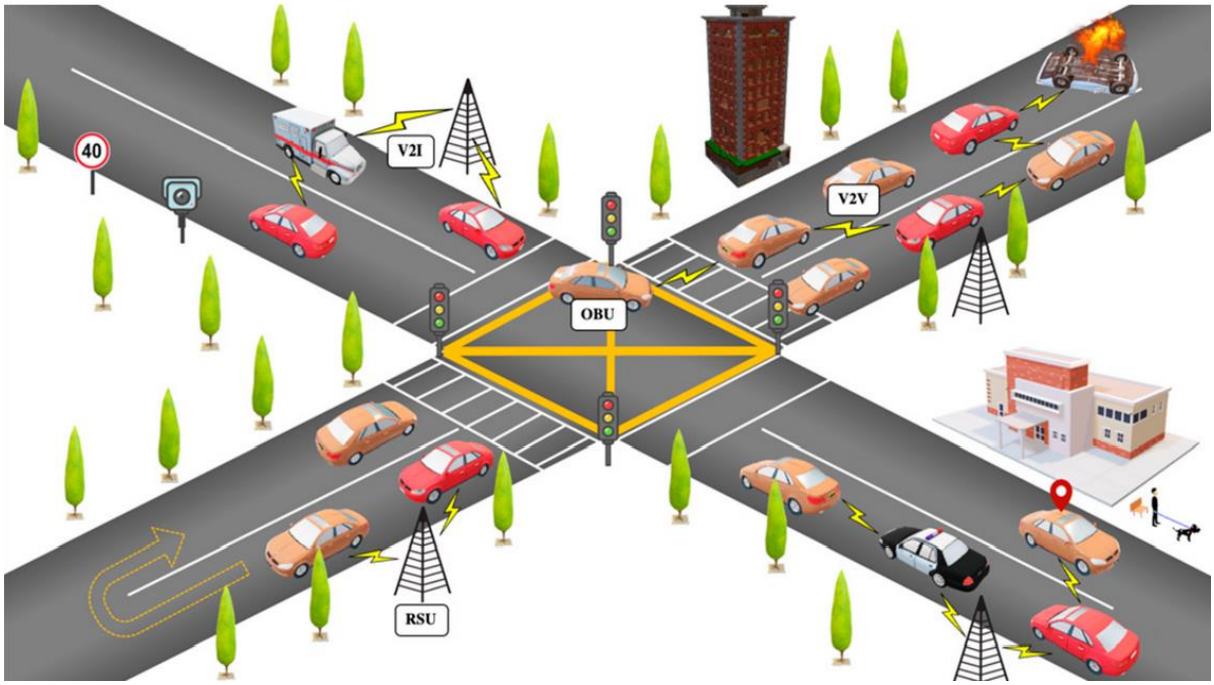
Normalmente, las VANETs se establecen entre las OBU (en el caso de V2V) o entre una OBU y una RSU (en V2I).

Como ya hemos mencionado, las OBU son las unidades de comunicación inalámbricas embarcadas en los vehículos, mientras que las RSU (*Road Side Unit*)

son unidades fijas de comunicaciones instaladas en la infraestructura de la vía, que también actúan de *gateway* para comunicaciones con otros servidores o internet.

Las RSU transmiten información sobre el estado de la vía, alertas de tráfico o incidencias en los alrededores. Por su parte, las OBU transmiten información sobre la localización del vehículo, velocidad y rumbo.

Imagen 10. Vehicular *ad-hoc* network (VANET)



Fuente: Khan et al.

En cuanto a las aplicaciones que soportan las VANET, se pueden dividir en dos grupos: las relacionadas con la seguridad y las relacionadas con aspectos de comodidad de los ocupantes [14].

En cuanto al primer tipo, las aplicaciones de seguridad, éstas pueden ser:

- IM (*information messages*), peajes y límites de velocidad;
- AM (*assistance messages*), asistencia a la conducción, navegación o evasión de accidentes, y
- WM (*warning messages*), información sobre condiciones de la vía o accidentes en las proximidades.

Tabla 4. Aplicaciones de seguridad en redes VANET

APLICACIÓN		DESCRIPCIÓN
Information messages	Curve speed	Informa sobre los límites de velocidad en curvas
	Work zone	Informa sobre la presencia de obras en la vía
	Pedestrian crossing information	Informa sobre la proximidad de un paso de cebra
Assistance messages	Turn assistance	Proporciona ayuda en giros
	Lane change assistance	Asistencia en cambios de carril seguros
	Blind spot warning	Indica al conductor de otro vehículo en el punto ciego
Warning messages	Post-crash	Alerta sobre un accidente en las proximidades
	Forward collision warning	Alerta de colisión con el vehículo precedente
	Emergency service vehicle	Alerta sobre la presencia de un vehículo de emergencias

Fuente: Ghori et al.

En cuanto al segundo tipo, las relacionadas con el confort de los ocupantes, son aplicaciones que pueden estar relacionadas con servicios de valor añadido para las personas que viajan en el interior del vehículo.

Ejemplos de dichas aplicaciones son: telepeaje, información sobre restaurantes y servicios en las proximidades o *infotainment*.

Tabla 5. Aplicaciones de comodidad en redes VANET

APLICACIÓN	DESCRIPCIÓN
Service announcement	Proporciona información sobre servicios en las inmediaciones (p. ej. gasolineras, hoteles…)
Remote diagnostic	Diagnóstico remoto en caso de avería o solicitud de asistencia en carretera
Entertainment	Proporciona contenido multimedia bajo demanda a los ocupantes del vehículo
Passenger health report	Permite solicitar una ambulancia o asistencia médica remota a los ocupantes del vehículo
Map download	Descarga de mapas
Navigation	Servicios de navegación y descubrimiento de rutas alternativas en caso de congestión
Parking availability	Información sobre parkings cercanos y disponibilidad de plazas de aparcamiento

Fuente: Ghori et al.

2.5.3. Arquitecturas V2X basadas en Wi-Fi

La primera tecnología propuesta para la implementación de las redes VANET ha sido desarrollada por IEEE y SAE en EE.UU. y se conoce como DSRC/WAVE (*Dedicated Short-Range Communications / Wireless Access in Vehicular Environments*).

El punto de partida de la investigación se sitúa en el año 1999, momento en el que la FCC reserva un ancho de banda de 75 MHz en la banda de los 5.9 GHz para fomentar la investigación de una nueva tecnología inalámbrica de corto alcance. Este ancho de banda inicialmente se dividió en 7 canales de 10 MHz, y un canal de guarda de 5 MHz.

Se preveía una arquitectura basada en equipos OBU embarcados que se comunicaran con la infraestructura, RSU, e intercambiaran información

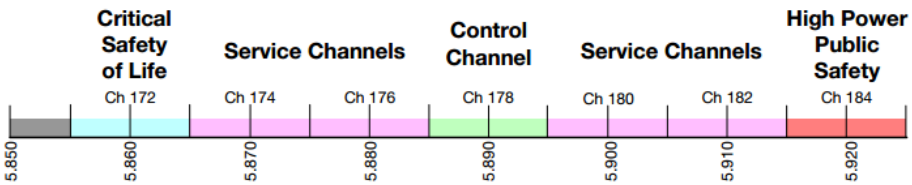
principalmente relacionada con la seguridad vial. El alcance de las comunicaciones era de un centenar de metros aproximadamente.

La asignación del ancho de banda inició un periodo de experimentación que culminó en 2010, año en el que el IEEE publicó una especificación de protocolos de capa física y capa MAC para la implementación de DSRC. Esta especificación forma parte de la familia de estándares WLAN IEEE 802.11, y pasó a denominarse IEEE 802.11p.

El nuevo estándar se creó a partir de IEEE 802.11a (estándar Wi-Fi), al cual se le añadían algunas modificaciones para adaptarlo a los requisitos de las redes vehiculares. Los principales cambios son la disminución del canal de 20 MHz a 10 MHz, más adecuado para las comunicaciones vehiculares por la reducción del efecto Doppler y el retardo asociado, y el acortamiento máximo posible del tamaño de los paquetes a enviar [15]. El objetivo estaba dirigido a reducir la latencia que, como hemos visto, es el parámetro esencial para las comunicaciones V2X.

No obstante, dado que 802.11p es un estándar heredado de 802.11a, también conserva muchas de sus características de capa física, como el uso de multiplexación OFDM y modulación 64-QAM. Igualmente, hereda en la capa MAC de acceso al medio el esquema CSMA/CA de acceso al medio, algo que limita al protocolo en casos de alta congestión como veremos más adelante.

Imagen 11. Asignación de canales en DSRC



Fuente: Arena et al.

Para las capas superiores, IEEE desarrolló el conjunto de normas 1609, que cubren:

- IEEE 1609.1, la capa de aplicación;
- IEEE 1609.2, la capa de seguridad;
- IEEE 1609.3, la capa de red, e
- IEEE 1609.4 la parte superior de la capa de acceso al medio

Dependiendo de la aplicación, en la capa de red puede usarse IPv6/TCP/UDP o un formato propio de mensajes definido en IEEE 1609.3 conocido como WSM (*WAVE Short Message*) que, como su nombre indica, se basa en mensajes cortos optimizados para que su transmisión sea lo más rápida posible. El protocolo encargado de la transmisión y recepción en la capa de red es WSMP (*WAVE Short Message Protocol*). Un tipo de mensajes WSM son los mensajes WSA (*WAVE Service Agreement*), que son emitidos por las RSU y contienen información de los

servicios provistos por la infraestructura y los canales de trasmisión y recepción usados por cada uno de ellos.

En cuanto a la capa de seguridad, IEEE 1609.2 provee varios servicios de autenticación y cifrado de paquetes que, en principio, son opcionales, de forma que en la arquitectura pueden darse tanto paquetes no seguros como paquetes cifrados y autenticados (firmados). La decisión de cifrar la información o no dependerá de los requisitos de latencia de cada aplicación. La autenticación tiene dos finalidades: permitir el acceso a la red de usuarios autorizados y legitimar la autoría del emisor del paquete; no obstante, no exime a los participantes de la red de tener un comportamiento malicioso. Los algoritmos de *hash* soportados son SHA-256 y SHA-384. Para para firmar los mensajes y garantizar la autenticidad e integridad de los paquetes se proponen dos algoritmos, ECDSA y ECQV, basados en el esquema de clave pública ECC. No obstante, el *overhead* añadido por los protocolos criptográficos incrementa la capacidad de procesamiento necesaria para comprobar la autenticidad de las firmas o cifrar los paquetes, afectando al rendimiento del sistema [16].

La arquitectura se completa con la norma SAE J2735 (2006) que define la sintaxis y estructura de los mensajes V2X. Entre ellos, el mensaje más importante relacionado con la seguridad es el BSM *(Basic Safety Message*), transmitido por el vehículo al resto de la red (*broadcasting*), normalmente cada 100 ms, con información sobre rumbo, velocidad, posición y estado de los frenos y acelerador.

Imagen 12. Mensaje BSM

```
BasicSafetyMessageVerbose ::= SEQUENCE {
   msgID       DSRCmsgID,              -- App ID value, 1 byte

-- Part I, sent at all times
   msgCnt      MsgCount,               -- 1 byte
   id          TemporaryID,            -- 4 bytes
   secMark     DSecond,                -- 2 bytes
   -- pos      PositionLocal3D,
   lat         Latitude,               -- 4 bytes
   long        Longitude,              -- 4 bytes
   elev        Elevation,              -- 2 bytes
   accuracy    PositionalAccuracy,     -- 4 bytes

   -- motion   Motion,
   speed       Speed,                  -- 2 bytes
   heading     Heading,                -- 2 bytes
   accelSet    AccelerationSet4Way,    -- 7 bytes

   -- control  Control,
   brakes      BrakeSystemStatus,      -- 2 bytes

   -- basic    VehicleBasic,
   size        VehicleSize,            -- 3 bytes

   -- Part II, sent as required
```

Fuente: SAE International

Además de los mensajes BSM, la SAE J2735 define otros 14 mensajes que, funcionando de manera combinada y coordinada, habilitan las aplicaciones VANET de seguridad y confort.

Imagen 13. Mensajes DSRC/WAVE definidos en la SAE J2735

Mensaje	Descripción	Origen
Basic Safety Message	Información de seguridad sobre el vehículo	OBU
Common Safety Request	Interroga a un vehículo determinado sobre información de seguridad, la respuesta se envía en forma de BSM	OBU
Emergency Vehicle Alert	Vehículo de emergencias en las proximidades	RSU
Intersection Collision Avoidance	Información sobre el riesgo de colisión en la siguiente intersección	RSU
Map Data	Descripción de áreas geográficas	RSU
Personal Safety Message	Información se seguridad sobre peatones o ciclistas	
Probe Data Management	Intercambio de información para definir patrones de cobertura de señal	RSU
Probe Vehicle Data	Intercambio de información sobre presencia de vehículos en una determinada zona	OBU
Roadside Alert	Alerta de peligros en las proximidades	RSU
Signal Phase and Timing Message	Enviados por la RSU en intersecciones señalizadas con información sobre los tiempos de activación y sincronización de la señalización	RSU
Signal Request Message	El vehículo solicita a la infraestructura el estado de la señalización en la próxima intersección. Se envían datos del vehículo y tiempo estimado de llegada a la intersección	OBU
Signal Status Message	La RSU envía al vehículo estado de la señalización en la próxima intersección	RSU
Traveler Information Message	Información y advertencias sobre el estado del tráfico	RSU
NMEA corrections	Corrección de posición en formato NMEA (GPS)	RSU
RTCM corrections	Corrección de posición diferencial RTCM (GPS)	RSU

Fuente: SAE International

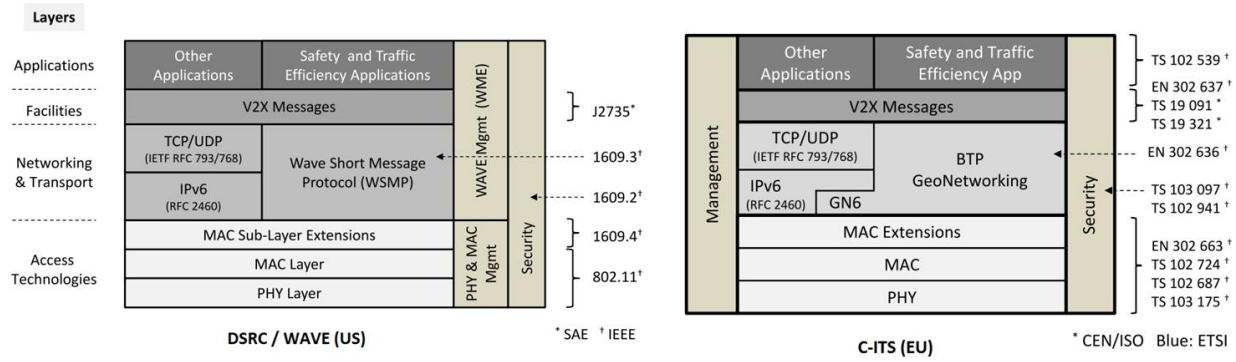
El término DSRC/WAVE especifica la arquitectura formada por los tres protocolos: IEEE 802.11p (capa física y MAC), IEEE 1609 (protocolos WAVE) y SAE J2735 (mensajes V2X).

A la versión europea de DSRC/WAVE se le conoce como C-ITS (*Cooperative Intellingent Transport System*) y ha sido desarrollada por el Instituto Europeo de Estándares de Telecomunicación (ETSI), bajo mandato de la Comisión Europea, desde finales de la década de los años 2000.

La capa física y de acceso al medio de C-ITS se denomina ITS-G5[3] y está definida en la norma ETSI EN 302 663[4]. ITS-G5 también está basado en el protocolo IEEE 802.11p, por lo que comparte bastantes similitudes con DSRC/WAVE, como el uso de la banda de los 5.9 GHz, la multiplexación OFDM, modulación 64-QAM y el esquema de acceso al medio CSMA/CA.

[3] El 5 indica que se usa la banda de los 5,9 GHz.
[4] Todos los estándares del ETSI son de libre acceso y se pueden descargar desde el sitio web: https://www.etsi.org/standards

Imagen 14. Pilas de protocolos DSRC/WAVE y C-ITS



Fuente: Festag [17]

Adicionalmente, se han aplicado modificaciones para cumplir con los requisitos de interoperabilidad impuestos por la Comisión Europea. Ente ellas, la más importante es la división del espectro en 4 bandas.

- ITS-G5A, con un ancho de banda de 30 MHz compuesto por 3 canales de 10 MHz dedicados a aplicaciones de seguridad;
- ITS-G5B, con 2 canales de 10 MHz dedicados a aplicaciones no relacionadas con la seguridad;
- ITS-G5C, con un ancho de banda de 255 MHz compartido con la banda RLAN (*Radio Local Area Network*), e
- ITS-G5D, reservado para futuras aplicaciones.

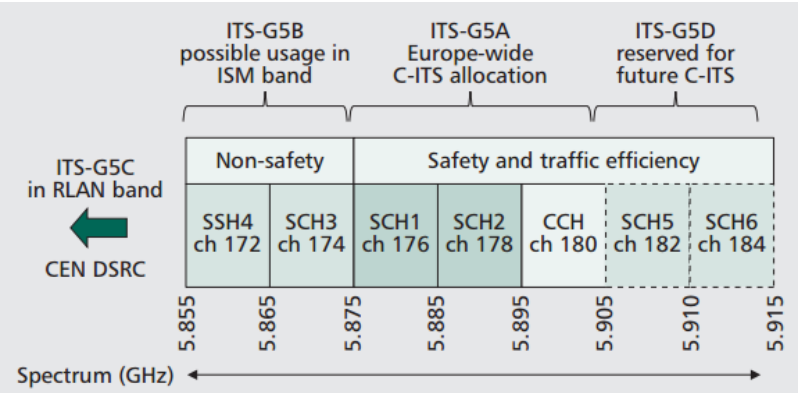
Desde el punto de vista de la seguridad, es importante destacar que la banda ITS-GC soporta DFS (*Dinamic Frequecy Selection*) un esquema de asignación dinámica de frecuencias útil para contrarrestar interferencias intencionadas.

C-ITS define dos tipos de mensajes para el intercambio de información, CAM (*Cooperative Awareness Message*) y DENM (*Decentralized Environmental Notification Message*), cuya estructura y sintaxis se especifica en las normas ETSI TS 102 637-2 y ETSI TS 102 637-2 respectivamente.

Los mensajes CAM son el equivalente a los BSM de SAE J2735. Son mensajes de *broadcasting* transmitidos con un periodo mínimo de 100 ms y máximo de 1 s que informan a las estaciones cercanas sobre la posición y rumbo del vehículo emisor.

Por otra parte, los mensajes DENM se envían únicamente en caso de determinados eventos y en un área determinada. No son mensajes periódicos sino que es una aplicación ITS la que, en presencia de dichos eventos, decide enviar la notificación DENM a los vehículos en las inmediaciones con información y detalles sobre el tipo de evento y la localización del mismo.

Imagen 15. Asignación de canales en ITS-G5



Fuente: ETSI EN 302 571

La arquitectura de gestión de la seguridad y privacidad del sistema se especifica en las normas ETSI 102 940 y ETSI 102 941 respectivamente.

Las aplicaciones se han dividido en 4 grupos: seguridad vial, servicios cooperativos locales, servicios cooperativos de eficiencia del tráfico y servicios globales de internet. La norma ETSI 102 941 especifica que todos los servicios relacionados con la seguridad de la vía, incluyendo el *broadcasting* de mensajes CAM y DENM, requieren autenticación y autorización para garantizar su integridad.

En cuanto a la confidencialidad y la privacidad, el sistema provee pseudonimización y no se contempla el uso de cifrado de mensajes por defecto. Los mensajes se envían empleando pseudónimos y, en cualquier caso, el identificador canónico de la estación nunca se envía.

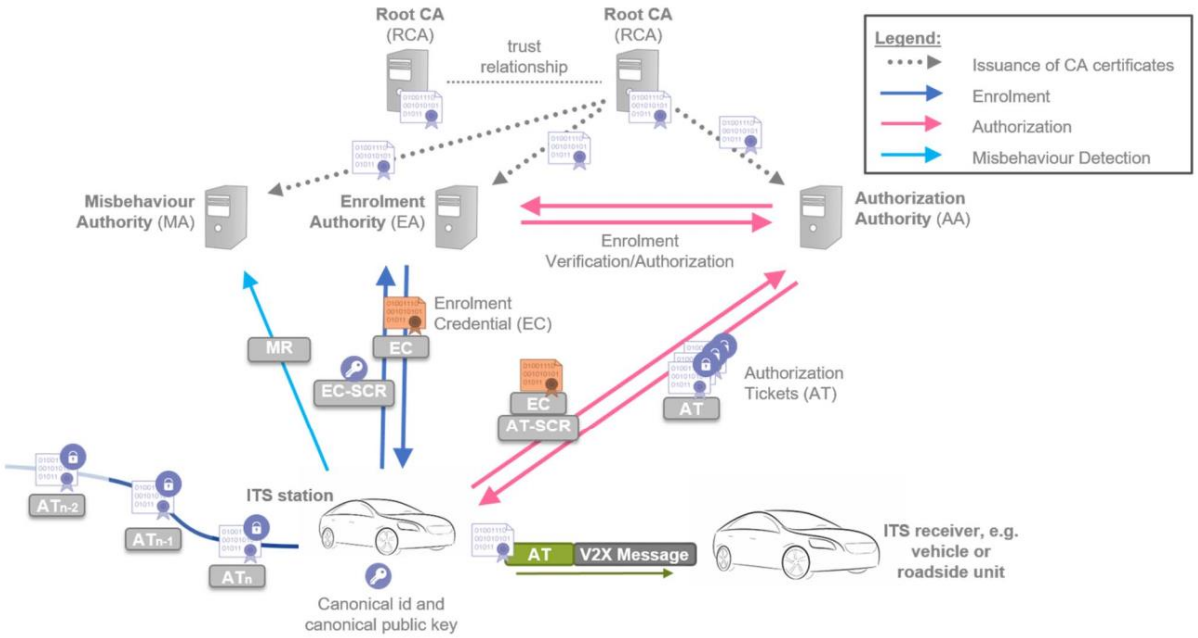
No obstante, un atacante que escanee un sector suficientemente amplio de la red podría llegar a re-identificar a un usuario asociando vehículos con trayectorias y llegar a deducir datos como rutas o hábitos de los ocupantes. Para dificultar este tipo de acción, cada estación ITS recibe múltiples certificados pseudonimizados que han de ser usados de manera alternativa, cambiando el certificado activo en cada momento con una determinada frecuencia.

Asimismo, la norma entiende que los mensajes de seguridad necesitan suficiente difusión por lo que el cifrado no es necesario. En el caso de los mensajes DENM emitidos por una RSU con información sobre, por ejemplo, un accidente en las proximidades, no se contemplan riesgos de privacidad; es más, se entiende que el objetivo es diseminar y difundir la información lo máximo posible.

El proceso de autenticación y autorización comprende 5 pasos: inicialización, inscripción (*enrollment*), autorización, operación y finalización. Para la gestión de los certificados se requiere una PKI que en el entorno C-ITS se conoce como C-ITS

SCMS (*Security Certificate Management System*) o simplemente C-ITS Trust Model. La norma donde se define la estructura de los certificados es la ETSI TS 103 097.

Imagen 16. Arquitectura de una PKI C-ITS Trust Model



Fuente: ETSI EN 102 940

El último de los estándares V2X basados en redes Wi-Fi existentes en la actualidad es el ARIB STD-T109[5], desarrollado en Japón, el cual presenta diferencias respecto a DSRC/WAVE y C-ITS. La capa física es similar a IEEE 802.11p pero opera en la banda de los 700 MHz. Además, el acceso al medio se realiza mediante un esquema TDMA.

Los principales fabricantes de automóviles involucrados en el desarrollo de comunicaciones V2X basadas en IEEE 802.11p son Volkswagen, Toyota y Renault. El grupo alemán anunció en 2019 el Volkswagen Golf 8, su primer modelo compatible [18]. Por otra parte, Car-2-Car[6] es un consorcio europeo dedicado a la estandarización y promoción de C-ITS que agrupa a 73 miembros entre los que se encuentran fabricantes, suministradores e investigadores.

En cuanto al grado de despliegue de la tecnología, actualmente se encuentra en funcionamiento en autopistas de Austria y en el puerto de Hamburgo, donde controla el tráfico de camiones [19].

[5] Disponible en: https://www.arib.or.jp/english/std_tr/telecommunications/std-t109.html
[6] https://www.car-2-car.org/about-c-its/

2.5.4. Arquitecturas V2X basadas en redes celulares

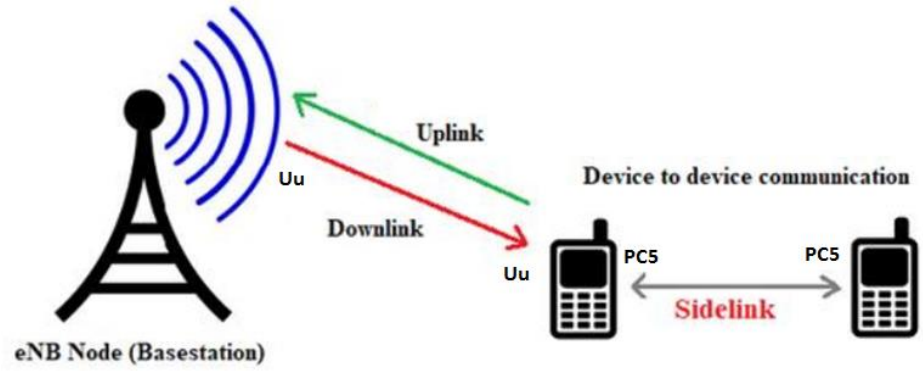
Desde mediados de los años 2010, el consorcio 3GPP viene trabajando en una nueva forma de implementación de redes VANET basada en redes celulares conocida como C-V2X (*Cellular Vehicle-to-Everything*).

Básicamente, las redes celulares son redes inalámbricas cuya zona de cobertura se divide en celdas (o "células") asignadas a una estaciones base, que son instalaciones fijas donde se ubican los transceptores y los equipos de acceso a la red que actúan de nodo controlador de la celda.

Los equipos de usuario (UE) pueden moverse e interactuar con la red libremente dentro de la zona de cobertura de la celda. La forma de hacerlo es mediante la interfaz Uu de los UE, que es la encargada de establecer los canales *uplink* y *downlink* con la estación base.

El funcionamiento de las comunicaciones C-V2X se basa en reservar una parte de las tramas *uplink* para el intercambio de datos punto a punto entre dispositivos celulares D2D (*device-to-device*) [20]. A esta comunicación se le conoce como *sidelink*, y es posible gracias a otra interfaz PC5 que no interactúa con la red celular, sino que establece conexiones directas con otros dispositivos. Por consiguiente, el *sidelink* no necesita cobertura de la red celular para funcionar.

Imagen 17. Sidelink LTE



Como ocurre habitualmente en el mundo tecnológico, el *sidelink* fue concebido con una intención diferente a la de ser usado en comunicaciones V2X. En 2015, el consorcio 3GPP publicó la Release 12, dedicada a la especificación de LTE (precursor del 4G), en la que se introducía el *sidelink* como un nuevo modo de comunicación directo entre dispositivos en situaciones de emergencia.

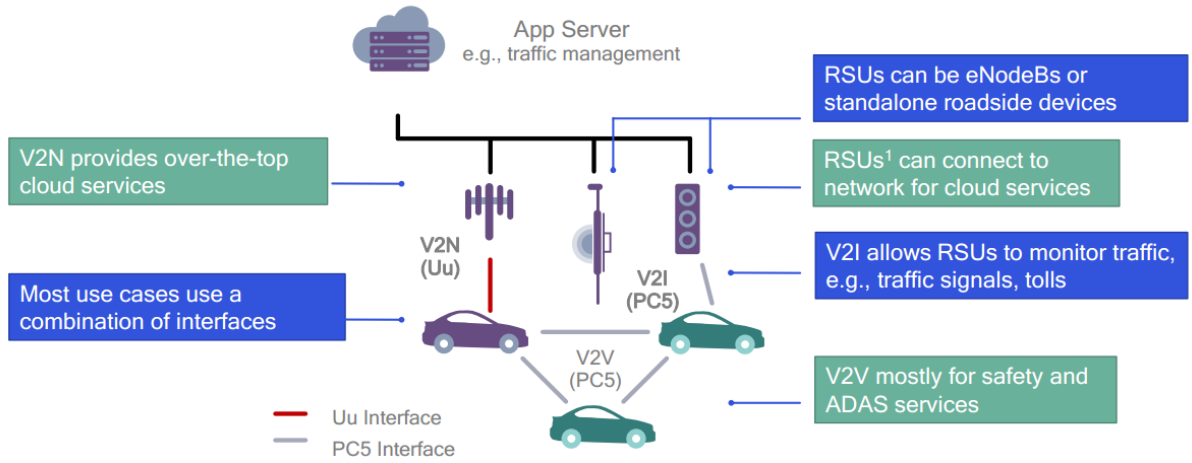
El *sidelink* LTE incluía 2 modos de funcionamiento, modo 1 y modo 2, y permitía las comunicaciones entre dispositivos, empleando las modulaciones y señales LTE, con la particularidad de que no era necesario que los dispositivos tuvieran que estar conectados a la red celular [21].

De esta forma, se conseguía comunicar con dispositivos en situaciones de emergencia donde no existiera cobertura de red. Sin embargo, la funcionalidad fue diseñada con la prioridad de prolongar la batería del dispositivo y a costa de sacrificar la latencia, por lo que esta primera implementación de *sidelink* no fue válida para aplicaciones vehiculares.

En la Release 14 (2016) el 3GPP introdujeron dos nuevos modos para el *sidelink* LTE, el modo 3 y el modo 4, que incluían mejoras para disminuir sustancialmente la latencia [22] y hacerlos aptos para V2X. A la nueva tecnología se le bautizó como LTE-V o LTE-V2X, esto es, comunicaciones vehiculares basadas en redes celulares LTE.

LTE-V2X se aprovecha las interfaces Uu y PC5 para comunicar a los vehículos con el exterior. Por una parte, Uu habilita las comunicaciones V2N con la red LTE y los servicios en la nube; y por otra, la interfaz PC5 habilita las comunicaciones V2V y V2I con otros vehículos y las RSU mediante el *sidelink*.

Imagen 18. Interfaces C-V2X



Fuente: Qualcomm

El 3GPP ha continuado mejorando el estándar y en la Release 16 (2019) publicó una nueva versión denominada New Radio V2X (NR-V2X) basada en 5G. A partir de este momento, el término C-V2X pasó a aglutinar a todas las comunicaciones V2X basadas en redes celulares, tanto LTE-V2X (basada en LTE) como a la nueva NR-V2X (basada en 5G).

Aprovechando las mejoras introducidas por 5G, NR-V2X ofrece un rendimiento muy superior a DSRC/WAVE, con latencias que pueden llegar a 1 ms y muy alta fiabilidad que, potencialmente, pueden habilitar cualquier aplicación V2X disponible en este momento [23] [24].

Sin embargo, un dato negativo a tener en cuenta es que el *sidelink* 5G NR-V2X no es compatible hacia atrás con el *sidelink* de LTE-V2X.

Tabla 6. Requisitos y casos de uso para comunicaciones C-V2X

Use case area	Use cases	QoS requirements			Technical enablers
		Latency [ms]	Reliability [%]	Data rate [Mb/s]	
Platooning	Information sharing within or outside platoon	10	99.99	65	LTE or NR broadcast (for limited cases) NR groupcast or unicast
Advanced driving	Cooperative collision avoidance Information sharing Emergency trajectory alignment Vulnerable road user detection	3	99.999	53	NR broadcast/groupcast/unicast
Extended sensor	Collective perception of environment See-through	3	99.999	1000	LTE broadcast (for limited cases) NR broadcast
Remote driving	Server or operator remotely controls a vehicle	5	99.999	Uplink: 25 Downlink: 1	LTE or NR unicast via cellular interface

Fuente: Ashraf et al.

C-V2X ha sido desarrollado con posterioridad a DSRC/WAVE pero tiene a su favor un mayor rendimiento, sobre todo en el caso de NR-V2X, y el hecho de que la infraestructura de red celular ya está desplegada, con lo que la inversión y el coste se reducen significativamente. La implantación de C-V2X está apoyada por 5GAA (5G Automotive Association), un consorcio de fabricantes de telecomunicaciones y de automóviles entre los que se encuentran BMW, Daimler, Ford, PSA, Ericsson, Vodafone, Huawei, Intel, Qualcomm y Samsung [25]. EE.UU. y China están apostando por el desarrollo del 5G para V2X. Actualmente no existe ninguna vía donde las comunicaciones C-V2X estén desplegadas, pero existen proyectos de investigación liderados por empresas de telefonía móvil [26].

2.5.5. Rendimiento de los estándares: limitaciones y evolución

En el momento de la aparición de LTE-V2X comenzó la carrera por determinar cuál de las dos tecnologías era las más adecuada para los requerimientos de V2X, las basadas en IEEE 802.11p (DSRC/WAVE y C-ITS) o las basadas en redes celulares (C-V2X). En un principio, los estudios determinaron que, en condiciones de baja congestión de red, IEEE 802.11p era superior en latencia mientras que LTE-V2X lo era en términos de PDR (*Packet Delivery Ratio*) [27]. Sin embargo, uno de los principales puntos fuertes de LTE-V2X era su apoyo en redes LTE ya desplegadas, lo que le permitía beneficiarse de las economías de escala [28].

Originalmente, IEEE 802.11p fue diseñado para proporcionar una latencia máxima de 100 ms y un alcance de 1000 m para soportar aplicaciones básicas de seguridad. El problema con IEEE 802.11p es que la latencia es muy dependiente de la congestión de la red. Se ha observado que el esquema de acceso al medio basado en CSMA/CA limita la escalabilidad del sistema. El rendimiento decrece de manera importante a medida que aumenta la congestión de la vía debido al aumento de las colisiones y al problema del nodo oculto (*hidden node*), característico de las redes

Wi-Fi, que degradan su rendimiento y su latencia [29]. Otras limitaciones vienen derivadas de los problemas de cobertura, zonas de sombra de señal y pérdidas de comunicaciones fuera de la "línea de vista" (LOS), habituales en las redes *wireless*. El coste asociado al despliegue de la red (RSU) también ha de tenerse en cuenta.

Por su parte, LTE-V2X ha demostrado ser adecuado para aplicaciones de seguridad pero su latencia también aumenta con la congestión de vehículos. No obstante, requiere mucha menos inversión en infraestructura de red a desplegar puesto que la interfaz Uu emplea la red LTE existente, y para la comunicación vía *sidelink* no se necesita infraestructura subyacente ni tampoco cobertura de red celular.

En 2018 se creó un grupo de estudio con el objeto de mejorar las prestaciones de IEEE 802.11p. El estándar Wi-Fi original, IEEE 802.11a, había sido objeto de varias actualizaciones (802.11n/ac/ax) desde su publicación y, tomándolas como base, se desarrolló una evolución de 802.11p denominada 802.11bd. Entre las modificaciones aplicadas se encuentra el soporte a las bandas de frecuencia de 59 GHz y 60 GHz y una mejora de la latencia y *throughput* gracias a un método de acceso al medio mejorado [30]. Sin embargo, aunque IEEE 802.11bd consiga mejorar a IEEE 802.11p, no parece que vaya a superar a NR-V2X en latencia y velocidad [31].

Tabla 7. Comparación 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 (*sidelink*)	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

Fuente: Autor

La investigación en redes celulares continúa y ya se está empezando a desarrollar el estándar 6G, del que se espera que dedique un capítulo a avances en el campo de la comunicación vehicular. Fundamentalmente, 6G supone el salto a las velocidades de procesamiento del orden de los THz, y a las velocidades de transmisión de varios cientos de Gbit/s o incluso Tbit/s. En cualquier caso, 6G está todavía en fases tempranas de estudio y desarrollo, se estima que la primera Release que introduzca el estándar sea la 20 (2027) y que no será antes de 2030 cuando se puedan empezar a desplegar redes de este tipo.

Por consiguiente, es muy temprano para hacer predicciones; no obstante, ya existen estudios que se aventuran a sugerir aplicaciones futuristas en el campo de los CAV que podrían ser habilitadas por el 6G, como V2X basada en computación cuántica, interfaces cerebro-vehículo o comunicaciones táctiles para conducción y formación de conductores [32].

2.6. Guerra comercial

En este capítulo hemos descrito a nivel técnico las dos principales tecnologías V2X disponibles. Como hemos mencionado, actualmente la industria y los países se encuentran divididos en su apoyo a la tecnología que debe dominar V2X en los próximos años debido a intereses económicos y geopolíticos.

DSRC/WAVE nació en EE.UU., pero parece que poco a poco la preferencia de este país va orientándose hacia el 5G, al igual que China. Ambos países se encuentran enfrentados en una guerra comercial por el liderazgo del 5G que está afectando al despliegue de V2X basado en Wi-Fi [33]. El trasfondo son los beneficios que se espera que el 5G genere en los próximos años y el liderazgo tecnológico mundial.

IEEE 802.11p está siendo apoyado por Japón y por la Comisión Europea, aludiendo al hecho de que es un estándar probado y listo para ser desplegado que podría salvar muchas vidas. También se apunta a que Europa prefiere favorecer estándares que la mantengan tecnológicamente independiente de EE.UU. y China [34].

Sea como fuere, lo cierto es que en Europa se han ido sucediendo las pérdidas de apoyos a IEEE 802.11p durante los últimos años. En 2019 el Consejo Europeo rechazó la propuesta de la Comisión sobre la adopción de Wi-Fi como estándar V2X de referencia en Europa [35] [36]. Asimismo, recientemente algunos fabricantes europeos, aliados con operadores de telecomunicaciones, están alineándose con el 5G y han pedido a la Comisión que dé marcha atrás en su apoyo a IEE 802.11p [37].

En EE.UU., el mayor jarro de agua fría se lo llevó DSRC/WAVE en 2020, momento en el que la FCC retiró la mitad del espectro asignado a DSRC en la banda de los 5,9 GHz en favor del Wi-Fi doméstico debido a que “no se han producido avances

significativos en los últimos 20 años y el ancho de banda no se está usando apropiadamente” [38].

En el caso de que hubiera un perdedor, las pérdidas serían cuantiosas en términos de tiempo y dinero invertidos en investigación y desarrollo. La Comisión Europea ha llegado a sugerir un reparto equitativo: 5G para los vehículos autónomos y Wi-Fi para los conectados [39], probablemente con la intención de salvar los años invertidos en el desarrollo de C-ITS en Europa. Sin embargo, está por ver si una fragmentación del mercado sería aceptable por parte de los fabricantes ya que doblaría el tamaño de las cadenas de suministro y los costes de producción.

En conclusión, no parece que se vaya a llegar a un acuerdo en el corto plazo y, en todo caso, las motivaciones finales no parece que vayan a ser, por lo menos en su mayoría, estrictamente técnicas.

3. CIBERSEGURIDAD EN COMUNICACIONES V2X

3.1. Introducción y metodología

La información intercambiada por medio de las comunicaciones V2X condiciona en gran medida las decisiones y maniobras ejecutadas por los sistemas de conducción automatizada. A ojos de estos sistemas, V2X representa un flujo de datos de entrada equiparable al de cualquier otro sensor, pero uno muy importante, puesto que por este canal va a suministrarse información “más allá de la línea de vista” que la red de sensores del vehículo no puede detectar.

Es fácil imaginar que la manipulación no autorizada de los datos recibidos por estos canales puede acarrear graves consecuencias; por consiguiente, las comunicaciones deben ser protegidas adecuadamente. Es de vital importancia tener claros los riesgos de seguridad asociados a las comunicaciones V2X y las contramedidas que pueden aplicarse.

En este capítulo se realiza un análisis cualitativo de los riesgos que afectan a las comunicaciones V2X desde el punto de vista de la ciberseguridad. El método empleado está basado en la identificación de vulnerabilidades y amenazas, ponderación de los riesgos y proposición de contramedidas que mitiguen o eliminen dichos riesgos.

Este tipo de análisis puede usarse como punto de partida para procesos de gestión de riesgos y toma de decisiones: si los riesgos se van a asumir, a mitigar o a eliminar.

Antes de continuar con el análisis, realizaremos un repaso de términos relacionados con la ciberseguridad que se van a usar en el documento.

Activo. Elementos del sistema que soportan una función que es necesario proteger; por ejemplo, la infraestructura de la red o la información. En el caso de los CAV, también es necesario proteger la integridad de los vehículos y de sus ocupantes.

Seguridad. Proceso continuado de protección de activos valiosos frente a ataques externos o accesos no autorizados. Cuando los activos a proteger son elementos relacionados con sistemas informáticos (como redes, programas y datos), se habla de ciberseguridad.

Vulnerabilidad. Punto débil de un activo que puede permitir a un atacante eludir la seguridad y dañar o apoderarse de los activos. Las vulnerabilidades pueden ser ocasionales (un fallo de diseño o de configuración) o inherentes al sistema. Por

ejemplo, por el mero hecho de utilizar como canal un medio abierto y accesible por todos como es el medio aéreo, las comunicaciones inalámbricas ya presentan ciertos puntos débiles que hay que proteger. Esto es inseparable de la tecnología y no se puede cambiar; no obstante, se pueden moderar sus inconvenientes.

Atacante o adversario. Entidad externa que actúa negativamente sobre un activo.

Explotación o *exploit*. El proceso por el cual un atacante se aprovecha de un punto débil o vulnerabilidad y, abusando de ella, accede a un activo con la intención de obtener algún beneficio, ganancia o, simplemente, dañarlo.

Amenaza. Evento potencial (tiene una determinada probabilidad de ocurrir) por el cual un atacante abusa o explota una vulnerabilidad. Dicha probabilidad de ocurrencia de la amenaza aumenta cuando el atacante posee 3 cualidades fundamentales: intención, capacidad y oportunidad.

Impacto o daño. Degradación o perjuicio causado en los activos tras la materialización de una amenaza. En otras palabras, el impacto son las consecuencias negativas para el sistema que conlleva el que un atacante ejecute su potencial de explotar alguna vulnerabilidad. Normalmente, cuando los activos afectados están relacionados con la información o los datos, suelen degradarse la integridad, confidencialidad o la disponibilidad.

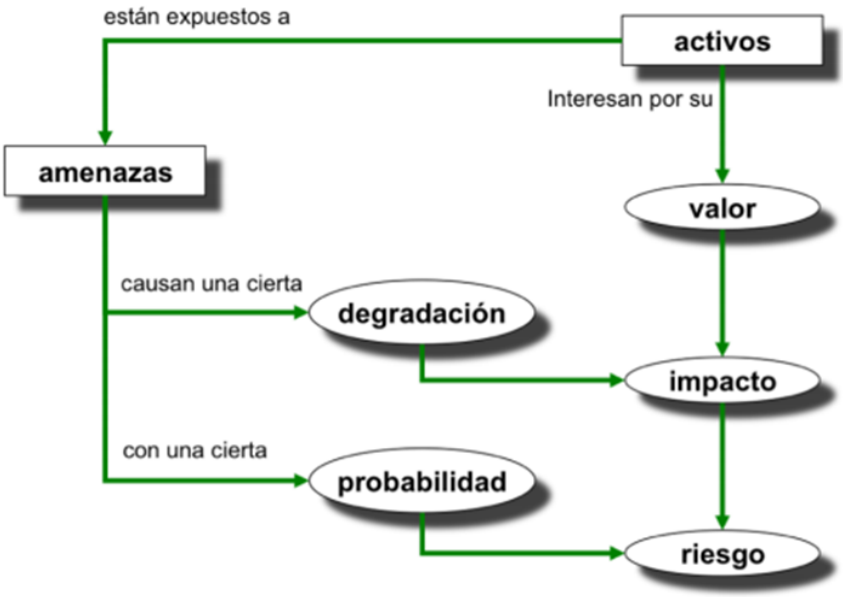
Riesgo. Relación ponderada entre la probabilidad de materialización de una amenaza y el daño asociado a ella. Los riesgos se deben identificar y, posteriormente, gestionar, ya sea mitigándolos, reduciendo su probabilidad de ocurrencia o, simplemente, asumiéndolos.

Por ejemplo, un terremoto o un ataque terrorista producirían daños catastróficos pero, normalmente, tienen asociada una probabilidad muy baja, por lo que probablemente el riesgo se asuma.

Sin embargo, en el caso de un ataque de *malware*, el daño probablemente sea menor que en el caso de una catástrofe, pero su probabilidad es bastante más alta, por lo que habrá que gestionarlo de alguna forma, ya sea protegiéndose activamente o mitigando sus consecuencias.

El proceso de gestión de riesgos está relacionado con la toma de las decisiones basadas en dos aspectos fundamentales: la información y el presupuesto disponibles. Un análisis de riesgos realista determina en gran medida la calidad de la información disponible que se puede emplear posteriormente en el proceso de toma de decisiones.

Imagen 19. Elementos del análisis de riesgos



Fuente: MAGERIT

La metodología de análisis de riesgos que se va a seguir en este capítulo es la siguiente:

1. Identificación de los activos presentes en los sistemas de transporte inteligente.

2. Estudio de las vulnerabilidades del sistema.

3. Identificación de las amenazas que pueden explotar las vulnerabilidades.

    a. Cada amenaza será presentada como un tipo de ataque que genera un daño en el sistema.

    b. Para cada amenaza se cuantifica una probabilidad que se determinará en base a diferentes factores: facilidad de implementación del ataque, el nivel de conocimiento, equipamiento y tiempo necesarios para montar el ataque.

4. Cuantificación del riesgo asignado a cada amenaza en base a la probabilidad y el índice de daño.

5. Proposición de contramedidas de protección para cada amenaza.

3.2. Identificación de los activos

En los entornos de los sistemas de información los activos se suelen dividir en físicos (hardware) y lógico (software e información). En el entorno vehicular la división sigue siendo aplicable pero hay que añadir una dimensión más, la correspondiente a la integridad de las personas ocupantes de los vehículos y de la vía pública.

Imagen 20. Activos de los sistemas V2X

Fuente: Autor

La información es un activo que hay que proteger y, habitualmente, las dimensiones de la información se clasifican en cinco categorías.

- **Confidencialidad**. La información sólo debe ser accesible a los destinatarios autorizados. Ejemplos de información confidencial pueden ser datos personales de los usuarios, credenciales de acceso, etc.

- **Integridad**. La información no debe cambiar desde el momento en que se emite hasta que es recibida. Esta cualidad en fundamental en V2X, los datos de navegación o sobre el estado de la vía deben ser precisos y no manipulados.

- **Disponibilidad**. Los usuarios autorizados deben poder acceder al sistema siempre que lo soliciten. Los ataques de denegación de servicio o las pérdidas de señal son degradaciones de la disponibilidad de la información.

- **Autenticación**. Debe ser posible verificar la identidad de los emisores o receptores de información para verificar que proviene de emisores confiables.

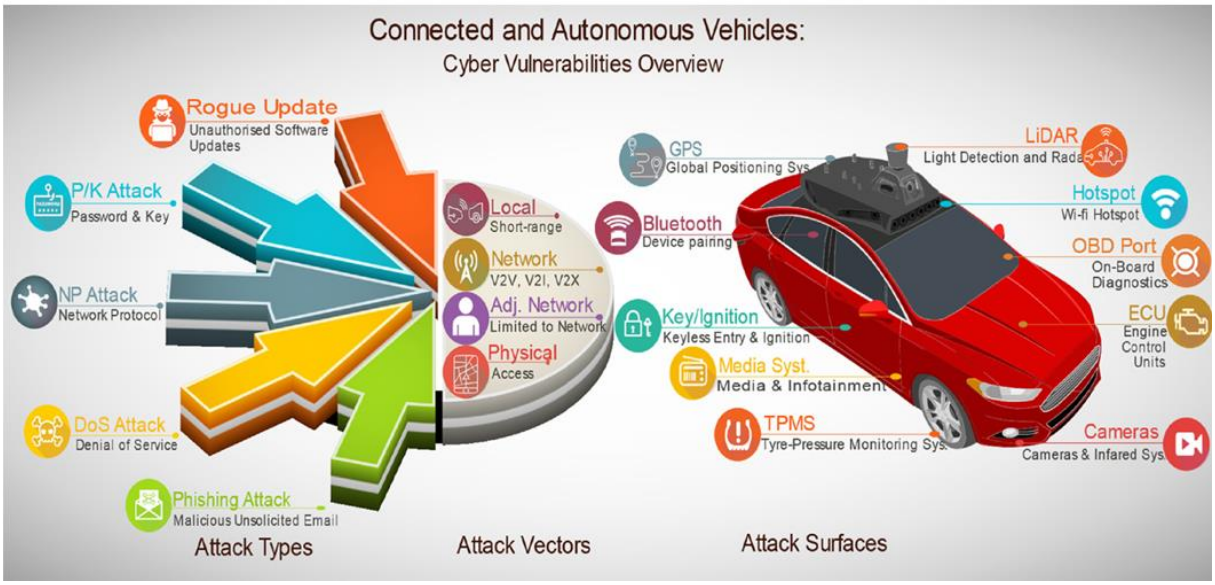
- **No repudio**. Debe ser posible verificar la autoría de un mensaje o acción. Por ejemplo, en caso de accidente es importante mantener la cualidad del no repudio.

3.3. Vulnerabilidades

A continuación veremos una lista vulnerabilidades, puntos débiles y limitaciones del sistema V2X que pueden explotarse por parte de un adversario.

Muchas de ellas tienen que ver con las limitaciones y la exposición de las superficies de ataque propias de las comunicaciones inalámbricas. También hay vulnerabilidades heredadas de los protocolos en los que están basadas las arquitecturas DSRC/C-ITS y C-V2X. Finalmente, otra categoría son las vulnerabilidades derivadas de los requisitos impuestos por las necesidades de los CAV (p. ej. baja latencia).

Imagen 21. Superficies y vectores de ataque en CAV



Fuente: Sheehan et al. [40]

3.3.1. Vulnerabilidades asociadas al diseño del sistema

Los vehículos CAV y las comunicaciones V2X han sido diseñados con requisitos muy estrictos en ciertos aspectos que pueden atraer la atención de los atacantes.

- Baja latencia. Es el parámetro esencial a mantener durante la transmisión. Los sistemas han de procesar y transmitir paquetes a alta velocidad puesto

que la alta variabilidad del medio puede hacer que la información se vuelva obsoleta rápidamente. Esta dependencia de la latencia los hace objetivo de ataques de *timing* y *spamming* que aumentan la latencia y degradan su rendimiento.

- Limitada capacidad de procesamiento. La capacidad de los sistemas de comunicaciones embarcados depende de cada modelo pero, normalmente, los requisitos se centran en la necesidades de tamaño, peso y coste para hacerlos atractivos y económicamente viables para el fabricante. Por esta razón, la capacidad de procesamiento de paquetes es limitada y el soporte a protocolos criptográficos puede no ser factible sin un retraso considerable en las operaciones. Hay que estudiar con cuidado la sobrecarga que supone añadir esquemas de autenticación y cifrado para verificar la integridad de los paquetes. Igualmente, la generación archivos de *log* de eventos añade trabajo de lectura y escritura de ficheros y, en cualquier caso, el alto número de paquetes recibido podría llegar a colapsar el espacio de almacenamiento en poco tiempo. Estas limitaciones pueden hacen que los fabricantes opten por no implementar funciones de seguridad en sus sistemas, lo que los volvería vulnerables a multitud de ataques.

3.3.2. Vulnerabilidades asociadas al medio inalámbrico

El hecho de que las comunicaciones inalámbricas empleen el aire como canal condiciona varios aspectos que pueden ser aprovechables para atacar el sistema:

- El canal es expuesto y abierto por lo que la información puede ser interceptada fácilmente por usuarios no autorizados. Esto las hace vulnerables a ataques contra la confidencialidad de las comunicaciones.

- El medio es cambiante y está sujeto a pérdidas de señal, atenuaciones aleatorias, zonas de baja cobertura e interferencias. Esto puede ser aprovechado para lanzar ataques de denegación de servicio. Igualmente, las limitaciones en la conectividad pueden suponer pérdida de acceso a actualizaciones de software

3.3.3. Vulnerabilidades asociadas a los protocolos

DSRC/WAVE y C-ITS heredan varias vulnerabilidades de IEEE 802.11a. Igualmente, las comunicaciones C-V2X comparten con LTE y 5G varias vulnerabilidades conocidas relacionadas con el proceso de autenticación.

- DSRC/WAVE y C-ITS. Las vulnerabilidades propias del carácter inalámbrico del estándar Wi-Fi son aplicables a DSRC/WAVE y C-ITS, abriendo la puerta a ataques de denegación de servicio, MITM (*Man-In-The-Middle*) o puntos de acceso no autorizados (*rogue AP*) [41]. Igualmente, el esquema de acceso al medio CSMA/CA hace al protocolo sensible a la congestión de la red, por lo que un ataque de envío masivo de paquetes (*spamming*) degradaría el rendimiento. La exposición del canal de transmisión lo hace vulnerable a la saturación de mensajes de *broadcasting*, a ataques de suplantación (*impersonation attack*) o falsificación de paquetes (*spoofing*). Finalmente, hay que destacar que, aunque tanto DSRC/WAVE como C-ITS proponen esquemas de cifrado basado en clave pública, su uso no es obligatorio debido al aumento de tiempo de procesamiento y latencia que supone. En cuanto a la autenticación, las últimas versiones de C-ITS obligan a que los paquetes relacionados con la seguridad (CAM y DENM) sean autenticados. Sin embargo, no era obligatoria en las primeras versiones de las normas, por lo que implementaciones de red antiguas han podido no adoptar esquemas de autenticación para reducir el *overhead*, lo cual abriría las puertas a multitud de ataques.

- LTE y 5G. En la especificación original de 3GPP se reconoce que la autenticación es necesaria, pero no se indica cómo hacerla [42]. Se ha desarrollado un esquema de autenticación en LTE denominado LTE-AKA, que presenta vulnerabilidades conocidas como exceso de *overhead*, alto consumo de ancho de banda y ausencia de re-autenticación rápida [43]. Este aspecto de las redes celulares constituye uno de los puntos de mejora abiertos de C-V2X. Se han propuesto soluciones de autenticación en redes LTE y 5G basadas en sistemas de clave pública y simétrica y mejoras de la capa física, aunque no está claro cómo funcionarían en una VANET real.

- GPS. Las señales GNSS son usadas por los vehículos para servicios de localización. Sin embargo, estas señales son vulnerables debido al hecho de que no son autenticadas y, además, al provenir de satélites situados a 19.300 km de la Tierra, llegan a la superficie suficientemente atenuadas como para ser vulnerables a los ataques de interferencia intencionada.

3.4. Modelado de atacantes

Para modelar el tipo de atacantes que pueden aparecer en los entornos vehiculares seguiremos una clasificación basada en la propuesta por Monteuuis et al. en 2018 [44].

- **Interno o externo**. En función de si son participantes de la red o no. Si los atacantes están autenticados en la red pueden en principio comunicarse con

otros pares y con la infraestructura. La autenticación asegura que el acceso sólo se permitirá a usuarios autorizados pero no garantiza que éstos no se comporten de manera maliciosa.

- **Malicioso o racional**. En función de la motivación del atacante y del beneficio u objetivo que persiga. Un atacante racional persigue un beneficio propio (por ejemplo, un usuario puede enviar mensajes falsos al resto de la red para que se desvíen de su trayectoria y dejen la vía libre) mientras que un atacante malicioso no tiene objetivo definido o conocido más allá de dañar al sistema. La conducta de un usuario racional es hasta cierto punto predecible mientras que la del usuario malicioso no lo es.

- **Activo o pasivo**. El atacante activo interacciona con la red; por ejemplo, enviando paquetes maliciosos o interfiriendo intencionadamente los canales. Por esta razón es más fácil de detectar. Por otra parte, el atacante pasivo se limita a escuchar las comunicaciones y analizar los datos y es más difícil de detectar.

- **Local o universal**. El atacante local sólo ataca a una zona determinada de la red (por ejemplo, en un ataque de tipo *black hole*). Cuando el ataque se dirige a toda la red se dice que es universal.

- **Intencionado o involuntario**. El ataque intencionado se ejecuta con dolo, esto es, de manera voluntaria y conociendo sus consecuencias. Por el contrario, un ataque involuntario es aquél que ocurre de manera fortuita o accidental. En este TFM no trataremos los ataques involuntarios.

3.5. Amenazas y ataques

A continuación haremos una descripción de las amenazas más probables en un medio vehicular en forma de ciberataques que explotan alguna de las vulnerabilidades presentadas anteriormente.

En este trabajo cubrimos las amenazas que usen como vector de ataque las comunicaciones V2X. Por tanto, quedan fuera del alcance los ataques cuya superficie sean dispositivos localizados en el interior del vehículo como el abuso del bus CAN o la manipulación de sensores y puertos USB u OBD. A este respecto, hay abundante bibliografía disponible sobre la explotación de vulnerabilidades del bus CAN [45], inyección de paquetes [46] y otros tipos de abusos de vulnerabilidades de la red interna del vehículo [47], derivados principalmente del hecho de que no existe autenticación ni cifrado de paquetes en el protocolo CAN.

Tampoco se va a entrar en el *hackeo* de llaves inalámbricas o RKE (*Remote Key Entry*), de los cuales también hay varios ejemplos en internet [48] [49].

3.5.1. Denegación de servicio (DoS)

Un ataque de DoS está destinado a dañar la disponibilidad del sistema impidiendo a los usuarios hacer uso de él. Normalmente, se consigue saturando la capacidad de procesamiento o el ancho de banda. Este ataque provoca una disrupción de la comunicación que tiene potencial de generar graves consecuencias en la circulación. Saturar la capacidad de procesamiento de las OBU puede ser relativamente sencillo. Una forma de realizarlo es reenviando masivamente (*spamming*) paquetes de *broadcasting* que se acaben descartando por la imposibilidad de procesarlos, produciendo pérdida de paquetes o de sincronización de los mismos. La naturaleza de las redes VANET, donde multitud de usuarios pueden entrar y salir al mismo tiempo, habilita los ataques DoS distribuidos (DDoS) por parte de varios usuarios maliciosos; por ejemplo, aumentando artificialmente el tamaño de los paquetes transmitidos para generar *buffer overflow* y pérdida de paquetes [50].

La armamentización de este ataque puede consistir en un *malware* que ralentice el procesamiento o que genere un envío masivo de paquetes. El atacante es activo y puede ser interno o externo. Consideramos que la probabilidad es alta, por la relativa facilidad de montar ataques de este tipo.

3.5.2. Interferencia intencionada (*jamming*)

Una variante del ataque DoS es la interferencia intencionada (*jamming*) de señales de RF. El ataque consiste en situar transmisores de señal más potentes que el emisor de la RSU con el objeto de hacer imposible la recepción de la señal original (GPS, IEEE 802.11p, etc.) por el ruido de fondo.

Este ataque se aprovecha de la accesibilidad del medio inalámbrico y es relativamente fácil de ejecutar puesto que el atacante puede ser externo.

3.5.3. Aislamiento (*black hole*)

Un ataque de aislamiento o *black hole* es un ataque contra la disponibilidad que consiste en la incomunicación selectiva de zonas de cobertura de señal donde los mensajes no se propaguen. Se puede conseguir de varias formas: inutilizando determinadas RSU con *malware* o boicoteando el funcionamiento de la red; por ejemplo, dejando de retransmitir paquetes o no contestando a peticiones. También se puede interferir la señal intencionadamente en una determinada zona. Si se

consiguen aislar varios nodos la red puede llegar a particionarse, evitando la sincronización interna, lo cual aumenta la gravedad del ataque.

Son ataques que pueden tener un grave impacto en la red pero, dada la complejidad de los mismos, consideraremos que tienen una probabilidad baja de ocurrencia.

3.5.4. Malware

Como todo sistema de información, las redes V2X están expuestas a ataques de *malware* de todo tipo: virus, troyanos, *ransomware*, etc. [51]. Además, el nivel de interconexión entre los usuarios favorece la diseminación del software malicioso. Las limitaciones de conectividad o pérdidas de señal inalámbricas limitan el acceso de los vehículos a las actualizaciones de software y firmware. La probabilidad de ocurrencia de un ataque de este tipo es alta, pues constantemente se publican vulnerabilidades que afectan a los últimos modelos de automóvil [52]. Incluso existen casos de acceso a vehículos mediante Wi-Fi con herramientas como metasploit y nmap en entornos controlados [53], por lo que la implicación de los fabricantes en el desarrollo de software seguro es fundamental. Un ataque de este tipo tiene consecuencias imprevisibles, un troyano puede afectar a un solo vehículo pero un ataque de *ransomware* podría tumbar la red entera, por lo que la protección contra el software malicioso es crítica.

Consideramos que este tipo de ataques son graves, ya que pueden inutilizar la red completamente y tienen alta probabilidad de ocurrencia.

3.5.5. Escucha secreta (*eavesdropping*)

La escucha secreta es un ataque contra la confidencialidad de la información relativamente fácil de ejecutar en los medios inalámbricos. El objetivo es interceptar los paquetes para obtener información valiosa o re-identificar a los usuarios de la red. En las arquitecturas DSRC/WAVE y C-ITS no todos los paquetes son confidenciales; de hecho, interesa que algunos de ellos sean conocidos cuanto más mejor. Los mensajes de *broadcasting* BSM (SAE J2735) y CAM (ETSI TS 102 637-2) son emitidos varias veces por segundo (100 ms de periodo máximo), y además contienen datos de localización. Un atacante a la escucha en un área muy amplia puede llegar a identificar a los vehículos, asignar patrones y llegar a deducir hábitos de la vida privada del usuario a partir del origen y destino de sus rutas. Los patrones de tráfico podrían también obtenerse con mensajes autenticados.

En el caso de las redes LTE, se puede re-identificar a los usuarios a partir de las conexiones a los proveedores de servicios [54], y de los identificadores IMEI o UICC. Especial atención ha de prestarse a los ataques de escucha secreta de

comunicaciones de vehículos que se aproximan a zonas donde se pueden intercambiar datos relacionados con tarjetas de crédito o medios de pago, como los peajes automáticos.

El atacante es externo y racional, y la probabilidad del ataque es alta debido a la facilidad con la que puede llevarse a cabo. El daño que se le puede causar al sistema es variable, puede ir desde una puntual pérdida de privacidad de un usuario a una interceptación de datos bancarios o de medios de pago.

3.5.6. Repudio

En las arquitecturas V2X no hay obligación de mantener un *log* de paquetes recibidos. Además, en el caso de redes donde por alguna razón no se haya implementado un mecanismo de autenticación, los atacantes pueden repudiar la recepción o envío de mensajes.

El repudio es relevante en el caso de accidentes. Un usuario puede negar haber recibido una instrucción que el obligaba a girar o haber enviado un paquete malicioso que ha ocasionado una colisión.

3.5.7. Falsificación o envenenamiento de paquetes (*spoofing*)

Se trata de un ataque contra la integridad de la información consistente en la creación o fabricación de mensajes falsos que imiten a los auténticos y se hagan pasar por ellos. Es particularmente dañino en entornos donde no exista autenticación o pueda abusarse de las vulnerabilidades de los protocolos de cifrado. Un ejemplo de este tipo de ataque es el GPS *spoofing,* donde el atacante se aprovecha de dos vulnerabilidades del sistema GPS civil: las señales no están autenticados ni cifradas, y los receptores siempre suelen estar programados para priorizar la señal recibida más potente. El atacante comienza sincronizándose con la señal GPS real y la simula. Acto seguida va aumentando progresivamente la potencia e introduciendo derivas en la posición actual de la víctima. Aunque el proceso no es trivial y requiere conocimientos y equipos relativamente costosos [55], en caso de éxito puede tener graves consecuencias en sistemas V2X y CAV.

La falsificación de señales GPS se denomina:

- *spoofing*, cuando se simula la señal original con el objeto de confundir al receptor y enviarle información manipulada;
- *meaconing*, cuando se interceptan las señales y se reenvían con un determinado retraso, y

- *tunelling*, cuando se aprovecha la pérdida local de señal de GPS (p. ej. en un túnel) para inyectar la señal envenenada.

También dentro de esta categoría se encuentra la falsificación de paquetes aprovechando la carencia de métodos del sistema para comprobar la verosimilitud o credibilidad de la información que se intercambia. Por ejemplo, un atacante con acceso físico a los sensores de un vehículo puede manipularlos con el fin de que generen información falsa sobre el entorno. Estos ataques (*illusion attacks*) inducen una visión irreal del entorno en los demás usuarios y son muy difíciles de detectar puesto que, desde el exterior, no se puede saber que los sensores del vehículo de un miembro autenticado en la red han sido manipulados. En otras palabras, en la red existen medios para verificar que los datos se envían correctamente, pero no para verificar que los datos que se envían sean los correctos (*do things right vs do the right things*).

El envío de información falsa también puede emplearse en beneficio propio. Un ejemplo sería el envío datos falsos sobre el estado del tráfico con el objeto de que los vehículos circundantes cambien de trayectoria y dejen paso libre al atacante (*bogus attack*).

Los ataques de falsificación de paquetes pueden ser muy dañinos pero también son difíciles de implementar pues requieren un atacante sofisticado con conocimientos avanzados de redes y manipulación de sensores, por lo que consideraremos que la probabilidad de ocurrencia es baja. El modelo de atacante es interno y racional

3.5.8. Ataques de suplantación y enmascaramiento

En los ataques de suplantación y enmascaramiento el atacante finge ser un nodo de la infraestructura (*impersonation*), una RSU (DSRC/WAVE y C-ITS) o una estación *femtocell* (LTE), o se presenta a los demás nodos con una identidad falsa o "máscara" (*masquerading*).

Un atacante puede interceptar mensajes, como BSM u otros mensajes no cifrados, para retransmitirlos haciéndose pasar por una RSU, lo que constituye un ataque contra la integridad de la información. También se pueden crear mensajes falsos a partir de otros mensajes válidos capturados anteriormente.

Otra forma de suplantar un nodo consiste en robar las credenciales y acceder a él de manera no autorizada, en estos casos los ataques constituyen, además de un riesgo para la integridad, un riesgo para la confidencialidad de la información ya que un atacante que ha suplantado un nodo puede tener acceso a información sensible.

Un atacante enmascarado como un nodo puede causar estragos en la circulación u otros comportamientos deshonestos (por ejemplo, vehículo que se hace pasar por un vehículo de emergencia para tener la vía libre).

3.5.9. *Man-in-the-middle*

La suplantación de un nodo sirve como como punto de partida para escalar a otros tipos de ataques, como MITM, donde el atacante intercepta la comunicación y la reenvía de nuevo al destinatario tras ejecutar sobre ella alguna acción.

Los ataques MITM son ataques contra la integridad de la información propios de las redes Wi-Fi y también aplicables a V2X. El entorno inalámbrico facilita la interceptación de paquetes pero exige que el atacante engañe de alguna forma al destinatario para hacerle creer que él es el originador de la información. Dependiendo de la acción ejecutada sobre el paquete interceptado, los ataques MITM tienen diferentes variantes:

- *Timing attack*. El atacante se limita a retener el paquete y reenviarlo con un determinado retraso. En un entorno V2X puede ser devastador por los exigentes requisitos de latencia requeridos. El reenvío de paquetes aprovecha debilidades del sistema: los paquetes no poseen un *timestamp* para verificar cuándo fueron generados y, por otra parte, la latencia puede aumentar debido a condiciones del canal inalámbrico e impide al receptor evaluar si la información que contiene ha expirado o no.

- *Replay attack*. El atacante reenvía el mismo paquete una y otra vez con el objeto de confundir al destinatario. En este caso, se pueden adoptar contramedidas en el receptor como comparación con paquetes recibidos previamente, pero está limitado por la capacidad de procesamiento del vehículo y por la capacidad del *log*.

- *Wormhole attack*. Un caso particular son los ataques de agujero de gusano en los que un atacante se sitúa en una zona estratégica de la red, donde la distancia entre nodos es más corta, o donde puede interceptar el tráfico de una parte de la red y reenviarlo a otras zonas. En su situación, puede anunciarse al resto de la red como un enrutador de paquetes y crear un túnel entre diferentes segmentos de la red, recibiendo paquetes por un lado y reenviándolos hacia otro con cierto retraso. La dificultad del ataque lo hace menos probable que los demás.

El modelo de atacante MITM es interno, local y activo. Dependiendo de la cantidad de información que ha de procesarse, pueden ser ataques difíciles de implementar debido a que en cortos intervalos de tiempo debería interceptarse la transmisión,

modificarse y reenviarse a las víctimas. Esto aumenta la dificultad del ataque y reduce su probabilidad [56].

En el caso de los ataques de *timing* y *replay*, el procesado de información que se realiza es mínimo; lo cual, unido a la peligrosidad de las consecuencias, hace que haya que prestarles especial atención.

3.5.10. Ataque Sybil

Un ataque de tipo Sybil es un ataque dirigido contra la autenticidad de la información en el cual el atacante crea varias identidades falsas con el objeto de confundir a los demás vehículos. De esta manera, una víctima que circule sola por la carretera puede llegar a creerse erróneamente rodeada de vehículos. El ataque puede dirigirse directamente a las víctimas, enviándoles diferentes mensajes para confundirlas, o contra la infraestructura, aprovechando alguna vulnerabilidad que permita al atacante poseer más de una firma digital válida u obtener varios certificados de la CA. Implementaciones de redes VANET que no posean certificados digitales u otros sistemas de autenticación están expuestas a este tipo de ataques.

El tipo de atacante es interno y racional. Las consecuencias podrían ser importantes y causar pérdida de confianza en el sistema por parte de la víctima; no obstante, la dificultad que entraña su ejecución rebaja la probabilidad de ocurrencia.

3.6. Análisis de riesgos

Una vez identificadas las vulnerabilidades y las amenazas que pueden explotarlas, hay que determinar el riesgo asociado a cada una de ellas. Para ello, ponderamos la probabilidad de ocurrencia de cada amenaza con el impacto o daño que recibiría el sistema en caso de materializarse.

El daño se cuantificará en base a 3 niveles:

- **Bajo**, cuando los activos no son dañados o generan molestias puntuales.
- **Medio**, cuando se produce un daño importante a los activos.
- **Crítico**, cuando se produce un impacto severo o el ataque puede implicar un riesgo para la vida de los usuarios

Tabla 8. **Cuantificación de daños**

Impacto	Puntuación
Bajo	1
Medio	2
Crítico	3

En cuanto a la probabilidad, ésta se evalúa en base a tres cualidades que el atacante debe poseer:

- intención o motivación derivada del valor del beneficio conseguido;
- capacidad de obtención de medios y conocimientos requeridos para el ataque, y
- oportunidad o exposición de las superficies de ataque y duración de las ventanas de oportunidad.

Añadiremos un punto hasta un máximo de 3 por cada cualidad que se cumpla.

Tabla 9. **Estimación de intención, capacidad y oportunidad**

Intención	Motivación del atacante para ejecutar el ataque. Será alta si el beneficio que puede obtener es alto	0: poco o ningún valor para el atacante 1: beneficio comprobable para el atacante
Capacidad	Disponibilidad de medios y conocimiento necesarios para ejecutar el ataque	0: no existen medios o es muy difícil conseguirlos 1: medios y conocimientos fácilmente obtenibles
Oportunidad	Nivel de exposición del activo y facilidad de acceso a él	0: ventana limitada de acceso al activo 1: fácil acceso (p. ej. *always-on*)

La probabilidad final será la suma:

Pr = intención (I) + capacidad (C) + oportunidad (O)

El cálculo anterior resulta en un conjunto de 4 posibles valores obtenibles. Si un atacante posee intención, capacidad y oportunidad, el ataque tiene altas probabilidades de producirse, mientras que si no tiene ninguna de ellas la probabilidad de que ocurra es descartable.

Tabla 10. Cálculo y valoración de la probabilidad de ataque

Pr = O + C + I	Valoración
0	Descartable
1	Poco probable
2	Posible
3	Inminente

Con los resultados de evaluar la probabilidad y el impacto o daño establecemos el riesgo como el producto: impacto x probabilidad.

Dado que Probabilidad = [0,1,2,3] e Impacto=[1,2,3], los valores que puede tomar el riesgo son Riesgo=[0,1,2,3,4,6,9].

Tabla 11. Tabla de valoración de riesgos

Valor	Riesgo	Valoración
0	Descartable	No existe riesgo
1,2	Menor	No hay activos esenciales en riesgo, o la probabilidad de ataque es muy baja. Se puede decidir si se quiere asumir el riesgo o mitigarlo
3,4	Mayor	Existe una probabilidad significativa de ataque a activos importantes del sistema. Conviene gestionar el riesgo aplicando contramedidas para mitigar los riesgos o eliminarlos
6,9	Crítico	Existe una alta probabilidad de ataque con consecuencias importantes hacia activos esenciales o la vida de las personas. Es obligatorio medidas para protegerse contra el ataque

Los riesgos se pueden gestionar de diferente manera dependiendo de dos cuestiones: el coste que supondría tomar medidas y el coste que supondría no tomarlas.

En el primer caso hay que tener en cuenta el presupuesto disponible y el nivel del riesgo que se quiera tratar. En el segundo, hay que evaluar las consecuencias que tendría para la organización y la sociedad el no tomar ninguna acción.

Tabla 12. Ponderación de las amenazas V2X

Ataque (amenaza)	Probabilidad			Impacto (daño)	Riesgo
	Intención (motivación)	Capacidad (facilidad)	Oportunidad (exposición)		
DoS / DDoS	1	1	1	3	9
Malware	1	1	1	3	9
GPS spoofing	1	0	1	3	6
Jamming	1	1	1	2	6
Timing attack	1	0	1	3	6
Packet replay	1	0	1	3	6
Repudio	1	1	0	2	4
Sybil	1	0	1	2	4
Suplantación	1	0	0	3	3
Wormhole	1	0	0	3	3
Black hole	1	0	0	3	3
Eavesdropping (red)	1	1	1	1	3
Eavesdropping (vehículo)	1	1	0	1	2
Bogus attack	1	0	0	2	2
Illusion attack	1	0	0	2	2

3.7. Contramedidas

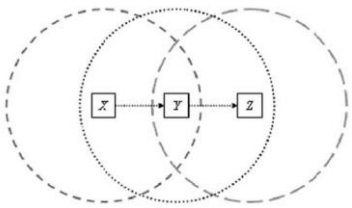
Una vez identificadas las amenazas y cuantificados sus efectos, propondremos varias contramedidas que pueden utilizarse para contrarrestarlos.

3.7.1. Diseño seguro de la red RF

Algunas de las limitaciones y vulnerabilidades de las comunicaciones inalámbricas, como las pérdidas de cobertura o los ataques de aislamiento, pueden subsanarse o mitigarse con un diseño inteligente de la topología de red. El reconocimiento pasivo entre estaciones (*pasive acknowledgement*), ya recogido en la especificación original de 800.11p, consiste en situar las estaciones de forma que cada una transmita y simultáneamente escuche lo que transmiten las estaciones cercanas. De esta forma pueden detectar anomalías como si alguna estación ha dejado de transmitir o si alguna de las direcciones MAC ha sido duplicada, en cuyo caso se iniciaría el proceso de repudio de la RSU. Esta contramedida contribuye a eliminar los ataques *black hole*, y a mitigar el *jamming*.

Otras contramedidas que se pueden implementar a nivel físico son: rutas de respaldo o de *backup*, señales *multipath* y técnicas de optimización de la propagación. Alternativamente se pueden establecer nodos que retransmitan la información enviada por los demás, aunque conlleva un incremento del coste.

Tabla 13. Reconocimiento pasivo entre estaciones



3.7.2. Estudio de señales electromagnéticas

El uso del medio inalámbrico supone ciertos riesgos pero también ofrece algunas oportunidades que se pueden aprovechar en beneficio de la seguridad. Analizar las señales electromagnéticas recibidas en las RSU permite determinar su potencia y dirección de llegada y hacer una estimación de la distancia y ubicación del emisor. Posteriormente, los datos obtenidos contrastan con las informaciones que emite el vehículo y así se verifica su verosimilitud.

Esta contramedida es útil contra ataques tipo Sybil y contra el GPS *spoofing*.

3.7.3. Detección de interferencias y ataques DoS

La amenaza de los ataques DoS y, en menor medida, de las interferencias intencionadas, es peligrosa por sus consecuencias y por la facilidad de ejecución, por lo que es necesario abordarla de alguna forma. Ya que prácticamente es imposible impedir que ocurra, es factible apoyarse en sistemas de detección temprana, que detecten que el ataque se está produciendo, y tomar las medidas adecuadas. El problema con 801.11p es que en casos de alta congestión el número de colisiones llega a ser muy alto, incluso sin que se esté produciendo un ataque DoS. El uso de sistemas de autenticación que puedan identificar a emisores haciendo *spamming* y revocar su certificado es fundamental.

También se pueden intercalar transmisiones de detección en las comunicaciones del sistema y evaluar el número medio de transmisiones correctas respecto a lo que sería un número esperable de colisiones, levantando una alerta en el caso de que éste sea anormalmente alto [57].

En el caso del *jamming* con transmisores de alta potencia, se pueden instalar detectores de RF en la infraestructura que determinen la dirección de llegada de las señales maliciosas. Una vez detectada la señal atacante, se realiza una reasignación dinámica de la frecuencia de trasmisión a un canal libre de interferencia. Éste es el fundamento de las técnicas de espectro ensanchado FHSS o el uso de bandas DFS dinámicas como ITS-G5C.

3.7.4. Protección contra el GPS *spoofing*

El sistema GPS incluye un método nativo de protección contra la falsificación de señales. La señal GPS tiene una componente civil “abierta”, de uso libre y gratuito SPS (*Standrad Positioning System*), y otra cifrada PPS (*Precise Positioning System*) que se suele emplear en aplicaciones militares (objetivo principal por el que fue diseñado el sistema). Sin embargo, no es sencillo implementar este método pues se necesita un módulo SAASM (*Selective Availability Anti-Spoofing Module*) instalado en cada dispositivo que quiera hacer uso de la señal GPS-PPS, así como el uso de claves militares.

Descartada esta posibilidad, se pueden implementar protecciones basadas en reglas de plausibilidad, que se encargan de monitorizar la señal con el objeto de detectar desviaciones improbables. No obstante, este método tiene sus limitaciones puesto que las inclemencias meteorológicas tienen precisamente esos mismos efectos en la señal GPS.

Los sistemas inerciales son métodos complementarios de localización que sirven para contrastar la información GPS recibida. También se puede usar *dead reckoning*

en zonas donde se pierde la cobertura de la señal o métodos de *differential monitoring*.

3.7.5. Actualizaciones OTA (*Over-the-Air update*)

Las actualizaciones de firmware y software recibidas por interfaces *wireless* se han desarrollado en los últimos tiempos para proteger a los teléfonos móviles. Dado que estos dispositivos raramente se conectan mediante cables a ningún sistema, ha habido que desarrollar un método para mantenerlos actualizados y protegidos contra el *malware* de manera eficiente y continuada. Las actualizaciones OTA se diseñan de forma que ocupen poco tamaño debido a las limitaciones de ancho de banda que tradicionalmente han restringido la conectividad de los teléfonos móviles.

Esta idea ha sido propuesta para ser aplicada en la actualización del software y firmware que poseen las ECU y el ADAS de los automóviles [58]. Las actualizaciones deben ser firmadas digitalmente para evitar la introducción de software malicioso o no autorizado en el automóvil.

3.7.6. Autenticación y cifrado

La autenticación de los usuarios en la red solventa muchos problemas relacionados con el enmascaramiento, la suplantación de usuarios y la falsificación de paquetes. Por otra parte, el cifrado de paquetes es útil para protegerse contra los ataques a la privacidad. Además, la utilización de múltiples certificados es útil contra ataques tipo Sybil, siempre y cuando no se permita más de un certificado activo por dispositivo.

La pseudonimización o autenticación con certificados que identifiquen a los usuarios mediante pseudónimos ayuda a proteger la privacidad de los mensajes. Para evitar la re-identificación de los usuarios por parte de un atacante universal (*eavesdropping*) los certificados deben renovarse cada pocos minutos. Éste es el método que se aplica en C-ITS. La contrapartida es se aumenta considerablemente el tiempo de procesamiento y el tamaño de los paquetes y, por consiguiente, contribuyen a aumentar la latencia de las comunicaciones. Es por esta razón que en el estándar C-ITS se recomienda cifrar únicamente los paquetes privados (no los de *broadcast*). Existen estudios que comparan el rendimiento de protocolos de cifrado aplicados a V2X donde se concluye que ECC es el mejor en transmisión, y en recepción ElGamal y ECC son equiparables. RSA es el menos indicado [59].

En cuanto a los esquemas de cifrado o firma digital, puede pensarse en dos tipos: los basados en clave simétrica y los basados en claves públicas y certificados. Cada uno de ellos presenta ventajas y desventajas relacionadas con el tiempo de procesamiento y la infraestructura necesaria para la implementación del sistema.

Tabla 14. **Comparación clave simétrica vs clave pública**

	Ventajas	Desventajas
Simétrica	Rapidez. Requiere menor capacidad de procesamiento	Requiere que la infraestructura de autenticación esté siempre conectada y disponible (*always-on*)
Pública	No requiere una infraestructura permanentemente disponible para atender a usuario que quieran autenticarse	Mucho más lento que la clave simétrica en términos de procesamiento *Overhead* adicional a la red debido al *broadcast* periódico de certificados revocados

3.7.7. Marcado temporal y resumen de paquetes

Otra forma más “ligera” de realizar un firmado de paquetes es añadiendo el resumen (*hash*) del mismo o incluyendo una marca temporal (*timestamp*). La marca temporal registra la fecha y hora en la que fue creado, y el resumen sirve para verificar que el paquete no ha sido manipulado desde el momento en el que fue generado por el emisor hasta el momento en el que fue recibido. El marcado temporal y el cálculo de resúmenes son útiles frente a ataques MITM, *packet relay* y repudio.

El marcado temporal es también una herramienta potente contra ataques tipo Sybil. Si los nodos de la red envían a la RSU mensajes con marcas temporales se pueden calcular las trayectorias que están siguiendo a medida que van pasando por las inmediaciones de cada RSU. Con esta información se realizan comprobaciones de plausibilidad de las trayectorias y ubicaciones que las OBU reportan en cada momento. La desventaja es que se aumenta la sobrecarga de la red y se añade trabajo de procesamiento a la infraestructura.

3.7.8. Pruebas de plausibilidad de mensajes recibidos

Las pruebas de plausibilidad (PVN) realizan una serie de comprobaciones predefinidas a todos los mensajes recibidos para determinar la verosimilitud de la información recibida [60]. El mensaje se valida únicamente cuando pasa todas las pruebas con éxito. Algunos ejemplos de pruebas de plausibilidad pueden ser el descarte de mensajes duplicados o la valoración de la credibilidad de la información recibida; por ejemplo, si la velocidad, la ubicación o el marcado temporal son lógicos y razonables.

Tabla 15. **Contramedidas**

Amenaza	Contramedida	Activo protegido	Coste
DoS / DDoS	Detección DoS	Disponibilidad	Puede incrementar el *overhead*
Malware	Actualizaciones OTA	Integridad	El software necesita ser firmado
GPS spoofing	GPS-PPS Plausibilidad de señales GPS Análisis de señales	Integridad	Alto coste de implementación
Jamming	FHSS / DFS	Disponibilidad	Necesita ancho de banda adicional
Timing attack	Timestamp Test de plausibilidad	Integridad	Incrementa el *overhead* y el tiempo de procesamiento de paquetes
Packet replay	Timestamp Test de plausibilidad	Integridad	Incrementa el *overhead* y el tiempo de procesamiento de paquetes
Repudio	Autenticación (clave simétrica) Autenticación (clave pública)	No repudio	*Overhead* adicional
Sybil	Análisis de señales Autenticación (clave pública)	Autenticación Integridad	*Overhead* adicional
Suplantación	Autenticación (clave simétrica) Autenticación (clave pública) Resumen de paquetes	Autenticación Integridad	*Overhead* adicional
Wormhole	Timestamp	Integridad	Incrementa el *overhead* y el tiempo de procesamiento de paquetes
Black hole	Redundancia de red	Disponibilidad	Incrementa el coste de despliegue de red
Eavesdropping (red)	Cifrado RSA/ElGamal/ECC Pseudonimización	Confidencialidad	Introduce latencia en el sistema
Eavesdropping (vehículo)	Cifrado RSA/ElGamal/ECC Pseudonimización	Confidencialidad	Introduce latencia en el sistema
Bogus attack	Test de plausibilidad	Integridad	Incrementa el tiempo de procesamiento de paquetes
Illusion attack	Test de plausibilidad	Integridad	Incrementa el tiempo de procesamiento de paquetes

3.8. Nuevas tecnologías aplicadas a la ciberseguridad CAV

3.8.1. Inteligencia artifical

Inteligencia artificial (IA) es un término genérico que agrupa varias tecnologías de computación que emulan procesos cognitivos del ser humano: razonamiento, toma de decisiones, aprendizaje, etc. Normalmente, los procesos de IA suelen seguir un modelo basado en capas de conocimiento que se van intercalando en la pila de protocolos. Analizan la información que se intercambian los protocolos entre ellos y toman decisiones en tiempo real que mejoren la eficiencia del sistema (por ejemplo, hacer una gestión de los recursos de la red en un momento dado). Dichas decisiones pueden estar también relacionadas con la seguridad: mejorar los servicios de autenticación y la privacidad u optimizar la distribución y el transporte de la información [61].

Una parte importante de la IA es el aprendizaje automático de computadores, de forma que sean ellos mismos los que, a la vista de los datos presentes y pasados, aprendan y tomen decisiones sin necesidad de intervención de un programador. El desarrollo actual del *machine learning* y el *deep learning* (ML/DL) cambia el paradigma de programación del enfoque “clásico”, centrado en la optimización del algoritmo, al basado en la disponibilidad de grandes volúmenes de datos, necesarios para entrenar a los algoritmos de aprendizaje automático.

El beneficio potencial en redes VANET viene derivado del hecho de que éstas son entornos altamente dinámicos y cambiantes. Dado que la principal cualidad del ML/DL es la capacidad de “aprender” adaptándose al entono, supondrían un avance respecto a de los métodos de evaluación tradicionales, que se basan en parámetros del sistema (por ejemplo, relación señal a ruido o señal a interferencia).

Las entradas de datos para el aprendizaje automático pueden ser los perfiles de potencia, topologías de red o parámetros dinámicos del entorno (velocidad, ubicación de vehículos cercanos, etc.). Aprendiendo de estas situaciones los algoritmos pueden adaptarse sin necesidad de ser programados, pero necesitan grandes bloques de datos.

Las 3 categorías de aprendizaje en ML/DL son:

- Supervisado. Basado en bloques de datos etiquetados. Las técnicas asociadas son clasificación y regresión. Es útil para realizar predicciones en base a una entrada de datos,

- No supervisado. Se basa en bloques de datos no etiquetados y sus técnicas principales son el *clustering* y la asociación. Es útil para realizar segmentación y categorización o descubrimiento de patrones ocultos.
- Reforzado. Basado en acciones de refuerzo.

La ventaja de los algoritmos ML/DL es que suelen estar ya desplegados en los CAV con el objeto de servir de soporte a los sistemas de decisión en materia de conducción de los vehículos.

En cuanto a las aplicaciones en materia de ciberseguridad de CAV y V2X, se pueden destacar las siguientes:

- Predicción de ataques a partir del análisis de parámetros dinámicos del entorno.
- Detección de anomalías en los sensores.
- Análisis de plausibilidad de los parámetros recibidos por otros nodos de la red.
- Clasificación de *malware*.
- Creación de nuevos algoritmos de detección de ataques basándose en la búsqueda de patrones en grandes volúmenes de datos.

Imagen 22. Aplicación del ML/DL a la ciberseguridad en CAV

Categoría	Tarea	Aplicación
Supervisado	Clasificación	Detección de intrusión. Plausibilidad
	Regresión	Predicción de parámetros. Control de rendimiento
No supervisado	*Clustering*	Control de congestión de red. Enrutamiento.
	Asociación	Agregación de datos
Reforzado	*Policy learning*	Gestión de recursos de red

Aunque el ML/DL presenta varios beneficios potenciales, también se enfrenta a limitaciones derivadas de las dificultades que supone entrenar correctamente a los algoritmos [62]. Para empezar, se necesitan grandes cantidades de datos y los tiempos de entrenamiento suelen ser grandes. Asimismo, es fundamental que los

datos que van a servir de base para el entrenamiento de los algoritmos sean de calidad, y en todo caso tampoco se descarta la aparición de falsos positivos.

Finalmente, hay que asegurarse que el hardware del CAV sea capaz de manejar los datos en términos de volumen y tiempo de procesamiento, lo cual puede representar un coste adicional.

3.8.2. Blockchain

Las cadenas de bloques son estructuras de datos (bloques) cifrados que se van uniendo secuencialmente de manera cronológica. Para asegurar la consistencia de los datos, las cadenas de bloques se basan en patrones de consenso, por lo que es imposible que un nodo malicioso o atacante altere la estructura de la cadena por su cuenta (haría falta la intervención del 51% de los miembros). Los mecanismos de consenso más importantes son PoW (*proof of work*) y PoS (*proof of stake*). Una aplicación práctica de las cadenas de bloques son los contratos inteligentes (*smart contracts*), que son pequeñas porciones de código que se ejecutan al cumplirse determinadas condiciones.

Por tanto, estas cuatro características definen a las *blockchain*: distribución, cifrado, consenso y contratos inteligentes.

En el entorno V2X estas propiedades pueden resultar bastante útiles, las cadenas de bloques suministran seguridad y privacidad adicional como complemento a la infraestructura PKI, proporcionando a los nodos una forma alternativa de comprobar la integridad de los mensajes. Éstos, en el momento de ser creados, pasarían a formar parte de los bloques de la *blockchain* y, puesto que ésta es distribuida y todos los nodos guardan una copia de ella, se puede comprobar la autenticidad del mensaje sin tener que depender de certificados de la PKI [63] [64].

4. NORMAS DE SEGURIDAD Y ORGANIZACIONES DE ESTANDARIZACIÓN

4.1. SAE

La SAE[7] es una asociación de fabricantes de automóviles fundada a comienzos del siglo XX en Estado Unidos con el objetivo de crear un foro donde los participantes de la industria pudieran discutir problemas comunes y proponer estándares de ingeniería. Durante su historia ha propuesto varios estándares en el campo de la mecánica y la seguridad que han sido reconocidos en todo el mundo. Su contribución más reciente al mundo de los CAV ha sido la norma SAE J3016. Ésta contiene una clasificación de niveles de conducción autónoma que ha sido rápidamente adoptada por casi todos los actores implicados. La edición más reciente de esta norma es la J3016_202104, publicada el 30 de abril de 2021 [65].

Otra norma importante en materia de ciberseguridad publicada por la SAE es la J3061, cuya edición más reciente data del 15 de diciembre de 2021 [66]. Este documento pretende servir de guía a las organizaciones de diseño de automóviles que quieran tener en cuenta a la ciberseguridad durante todo el ciclo de vida del producto.

- Concepto y diseño. Desarrollo de un plan de ciberseguridad que aplicará en todas las fases del ciclo de vida del producto. En esta fase se diseñan y proponen el plan de ciberseguridad del producto y las herramientas necesarias para llevarlo a cabo.
- Desarrollo y validación. En esta fase se incluyen las pruebas de vulnerabilidad y *pentesting* del producto que han de desarrollarse en paralelo al ciclo de diseño y V&V de la ingeniería de sistemas del producto.
- *Aftermarket*, soporte post-venta y respuesta a incidentes. Han de crearse procedimientos de respuesta y reporte de incidentes, así como planes de contingencia para prevenir problemas futuros.

4.2. ISO

La ISO[8] es una organización formada por varios organismos de estandarización de todo el mundo fundada a mediados del siglo XX. Hoy en día está basada en Ginebra

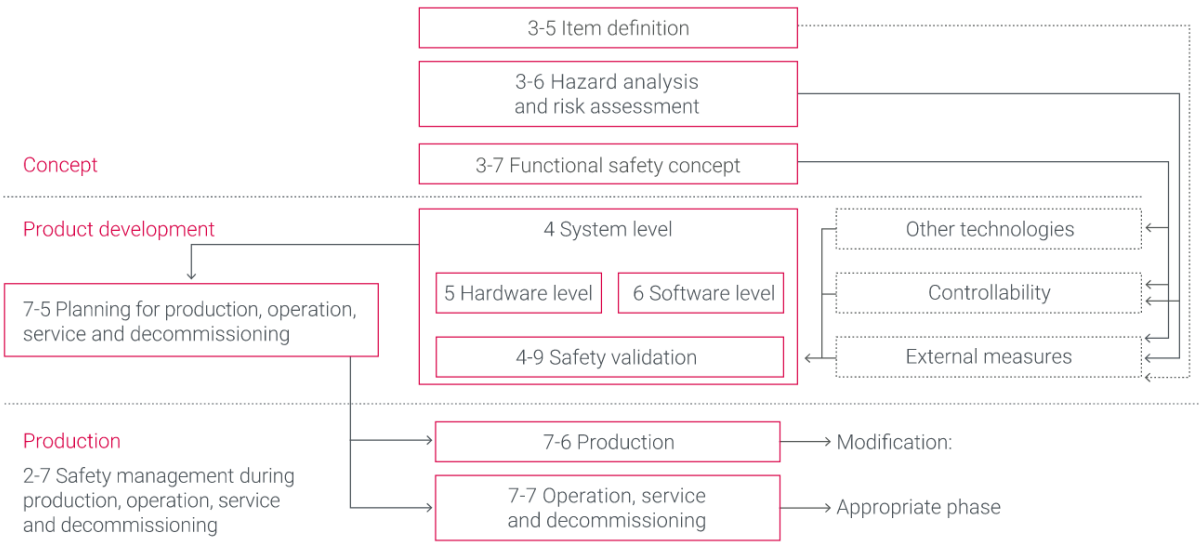
[7] https://www.sae.org/
[8] https://www.iso.org/home.html

y su principal activo es que prácticamente todos los países del mundo forman parte de ella, dedicándose a la creación de estándares internacionales.

La primera de las normas publicada por la ISO relacionada con la seguridad de los automóviles es la ISO 26262, centrada en la identificación de posibles riesgos derivados del mal funcionamiento de dispositivos eléctricos y electrónicos del vehículo. Si bien en su primera edición del 2011 no recogía aspectos relacionados con la ciberseguridad, en su última revisión [67] de 2018 se recoge una sección dedicada al análisis de riesgos en las fases de desarrollo de software.

Las dos ideas a destacar introducidas por la ISO 26262 son el concepto de seguridad funcional y los niveles ASIL (*Automotive Safety Integrity Level*). Con la seguridad funcional se asegura que para todos los componentes electrónicos (incluyendo el software) del vehículo se tiene en cuenta la seguridad en todo el ciclo de vida del producto. El ASIL es un esquema de clasificación de riesgos en 4 niveles: ASIL A, ASIL B, ASIL C y ASILD, siendo éste último el más severo (riesgos para la vida).

Imagen 23. Seguridad funcional en ISO 26262



Fuente: https://www.kuglermaag.com/functional-safety/

Como continuación del trabajo de la ISO 26262 y de la SAE J3061, ambas organizaciones publicaron conjuntamente en 2021 el estándar ISO/SAE 21434 [68], el cual se centra en el análisis de riesgos de ciberseguridad en el diseño y desarrollo de los sistemas del vehículo.

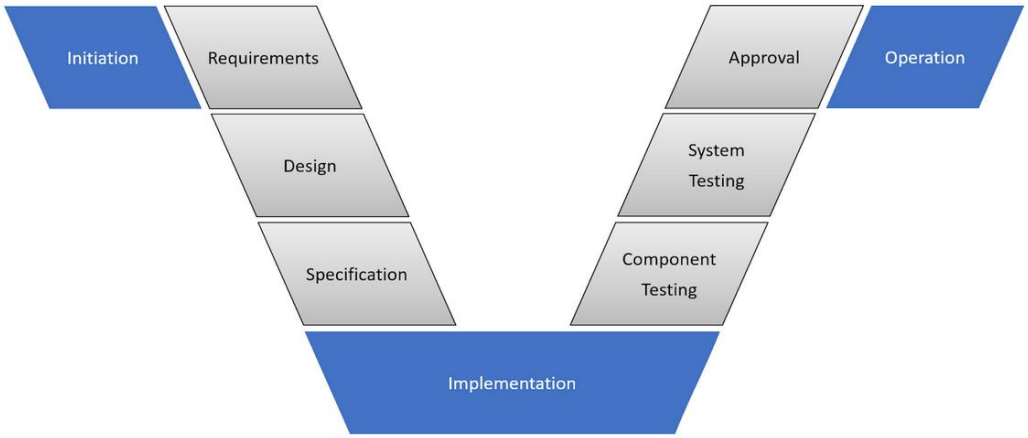
La creación de una nueva norma viene motivada por las necesidades de unificar la terminología y de concretar los niveles propietarios de seguridad definidos anteriormente (ASIL) y hacerlos aplicables también a la ciberseguridad.

Los objetivos del documento pretenden establecer:

- un conjunto de requisitos para la gestión de riesgos de ciberseguridad;
- un marco de trabajo de procesos de ciberseguridad, y
- una terminología unificada para fabricantes y suministradores.

El documento evita entrar en soluciones tecnológicas y proporciona a los fabricantes y suministradores un marco de trabajo en el que se tenga en cuenta a la ciberseguridad en todas las fases del desarrollo (la tradicional "V" de la ingeniería de sistemas).

Imagen 24. Modelo V de la ingeniería de sistemas



Al igual que la SAE J3061, la ISO/SAE 21434 recomienda a los fabricantes el uso de buenas prácticas en materia de ciberseguridad como los procesos TARA (*Threat Analysis and Risk Assessment*) de evaluación de riesgos y los procesos de prueba continua, poniendo especial énfasis en los *fuzz test*[9]

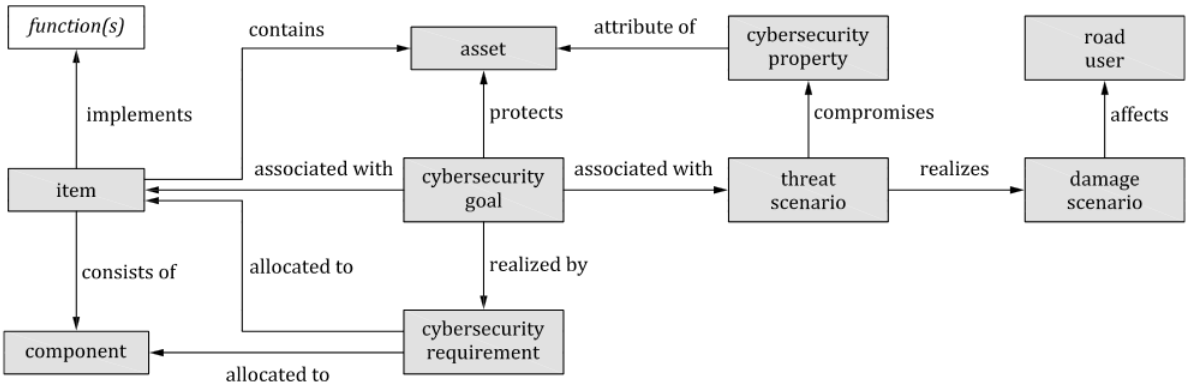
El *framework* de la ISO/SAE 21434 está basado en los siguientes aspectos esenciales:

- Gestión de la ciberseguridad durante todo el ciclo de vida del producto.
- Énfasis en métodos de evaluación de riesgos basados en identificación de activos y vulnerabilidades, análisis de amenazas y evaluación de impacto (TARA).
- Integración de objetivos de seguridad en la fase de objetivos de alto nivel de diseño del sistema.
- Verificación y validación de requisitos de ciberseguridad.
- Monitorización continuada de la ciberseguridad en fases de operación y mantenimiento.
- Creación de procedimientos y manuales de ciberseguridad.

[9] Los *fuzz tests* son pruebas donde se inyectan en las entradas del DUT datos aleatorios, incompletos o intencionadamente inválidos, con el objeto de monitorizar el comportamiento del sistema y los fallos de seguridad.

La idea a transmitir es que la ciberseguridad no es algo en lo que pensar cuando ya es demasiado tarde, sino que es necesario integrarla desde las primeras fases del proyecto hasta las últimas.

Imagen 25. Modelo de ciberseguridad en SAE/ISO 21434



Fuente: ISO

4.3. NHTSA

La NHTSA[10] (*National Highway Traffic Safety Administration*) es una agencia estadounidense perteneciente al Departamento de Transportes (DOT) involucrada principalmente en la mejora de la seguridad en las carreteras y la reducción de accidentes. A diferencia de otras entidades estandarizadoras, la NHTSA tiene potestad no sólo de crear estándares sino también de crear regulaciones y hacerlas cumplir.

Desde principios de la década de los 2010 se ha mostrado muy activa e interesada en la investigación y desarrollo de las comunicaciones V2X debido a la contribución que la implantación estas tecnologías tendría en la mejora de la seguridad vial.

La NHTSA también se interesa por la ciberseguridad de los vehículos, el desarrollo de los vehículos autónomos o la privacidad de los datos de los usuarios. En su sitio web[11] se pueden consultar multitud de investigaciones, recomendaciones, buenas prácticas y estudios sobre la viabilidad de la tecnología y la ciberseguridad.

[10] https://www.nhtsa.gov
[11] https://www.nhtsa.gov/technology-innovation

4.4. ETSI

El ETSI[12] (*European Telecommunications Standards Institute*) es el Instituto Europeo de Estándares de Telecomunicación. Aunque fue creado en 1988 como una organización independiente, trabaja estrechamente con las instituciones europeas y sus normas y documentos suelen servir de referencia en el ámbito de la UE.

Sus esfuerzos en los últimos años han ido destinados a la creación del estándar C-ITS, una arquitectura completa de comunicaciones V2X basada en IEEE 802.11p que a día de hoy está lista para ser desplegada. La documentación de la Release 1 es de libre acceso y puede ser descargada desde su sitio web[13].

La información se encuentra desperdigada numerosos entregables varios tipos: especificaciones técnicas (TR), *technical reports* (TS), etc. Los documentos más representativos desde los que comenzar la búsqueda de información son.

- ETSI TR 101 607 (última revisión: 2020). Lista de todos los entregables que forman la Release 1.
- ETSI TR 102 638 (última revisión: 2009). Aplicaciones de comunicaciones V2X.
- ETSI EN 302 663 (última revisión: 2020). Especificación de la capa física (PHY) y de acceso al medio (MAC) ITS-G5.
- ETSI TS 102 940 (última revisión: 2021). Arquitectura y gestión de la seguridad.
- ETSI TS 103 097 (última versión 2021). Certificados de seguridad en C-ITS.
- ETSI TR 102 165 (última revisión: 2022). Método para el análisis de riesgos, vulnerabilidades y amenazas.

4.5. 3GPP

En 1998, varias entidades encargadas de la creación de estándares para la telefonía móvil se unieron en un consorcio cuyo objetivo era el desarrollo de la tercera generación de sistemas de telefonía móvil (3G). El grupo se conoce como 3GPP[14] (*3rd Generation Partnership Project*), y tras terminar la especificación del 3G ha continuado trabajando en el desarrollo de los sucesivos estándares, UMTS, LTE, 5G y 6G.

[12] https://www.etsi.org
[13] https://www.etsi.org/standards
[14] https://www.3gpp.org/

La publicación de los estándares se hace en forma de Releases, que son conjuntos de especificaciones técnicas, informes y otros entregables que se van distribuyendo en su sitio web[15] a medida que se van liberando y revisando. La duración de la publicación de una Release oscila entre un año y un año y medio, tiempo durante el cual los entregables pueden ser revisados varias veces.

A continuación hacemos un breve repaso de las Releases de 3GPP con los hitos más importantes en cuanto a comunicaciones V2X se refiere.

- Release 8 (2008). Se publica la primera especificación del estándar LTE (*Long-Term Evolution*).

- Release 10 (2011). Se publica el estándar LTE Advanced, primer estándar candidato a cumplir con los requerimientos de 4G establecidos por la ITU.

- Release 12 (2015). Se publica una nueva función de LTE que permite la comunicación directa D2D, o *sidelink*, entre dispositivos LTE. Concebida con propósitos de acceso a móviles sin cobertura en caso de emergencia, se convertirá en el germen de la nueva tecnología C-V2X.

- Release 13 (2016). Introducción de LTE Advanced-Pro, presentado a la ITU como candidato a convertirse a 4.5G y más tarde aprobado como tal.

- Release 14 (2016). Se publica una modificación de la función D2D que mejora la latencia y el rendimiento. El nuevo desarrollo se denomina LTE-V o LTE-V2X y es presentado como método de implementación redes VANET y comunicaciones vehiculares.

- Release 15 (2018). Conocida por ser la Release introductoria del 5G. Se publica la especificación de Advanced V2X o LTE-eV2X, que mejora la latencia y rendimiento de LTE-V.

- Release 16 (2020). Publicación de 5G NR-V2X (*New Radio V2X*), como una implementación de V2X basado en el *sidelink* 5G que incorpora latencia y rendimiento superior a IEEE 802.11p.

- Release 17 (2022). La publicación de esta Release ha concluido a principios de 2022 y se ha centrado en aspectos de mejora de la calidad de servicio y de provisión de mejora de servicios, conocidas como 5G NR-eV2X.

[15] https://www.3gpp.org/specifications/specifications

4.6. UNECE

La UNECE[16] (*United Nations Economic Commission for Europe*) es una de las 5 comisiones regionales (además de África, Asia-Pacífico, Latinoamérica-Caribe y Asia occidental) dedicadas a promocionar la cooperación económica entre países miembros que, en caso de la UNECE, abarca a Europa y otras naciones no europeas como Turquía, Israel, EE.UU., Canadá y países de Asia Central. La UNECE fue fundada en 1947 y tiene su sede en Ginebra y, como el resto de las comisiones mundiales, depende del Consejo Económico y Social de la ONU.

Dentro de la UNECE existen varios grupos de trabajo o *working parties* (WP) dedicados a cuestiones como políticas ambientales, comercio internacional, energías sostenibles o aspectos relacionados con la integración económica y la cooperación de los estados miembros.

Dentro de ellos, destaca el WP.29 (*World Forum for Harmonization of Vehicle Regulations*) cuya función es la gestión y creación de acuerdos multilaterales en el ámbito del transporte, cubriendo aspectos esenciales como la seguridad o la protección medioambiental.

En el verano de 2020 se adoptaron dos regulaciones, UN R155 [69] y UN R156 [70], que pretenden definir un marco de trabajo para la ciberseguridad aplicada a los automóviles. Ambas normas entraron en vigor en enero de 2021, siendo puestas a disposición de los estados miembros que quisieran adoptarlas.

La Unión Europea, Corea del Sur y Japón ya han anunciado que la normativa UNECE R155 se hará cumplir en sus territorios. En el caso de la UE, será aplicable para todos los modelos que los fabricantes quieran homologar a partir del 1 de julio de 2022, y a partir del 1 de julio de 2022 se exigirá para todos los vehículos nuevos. El no cumplimiento de la norma prevé sanciones de hasta 30.000 € por cada vehículo vendido. Varios fabricantes como Toyota, Seat y Volkswagen han anunciado que están adoptando medidas para adaptarse a la nueva regulación [71].

A diferencia de otras entidades estandarizadoras, dentro del WP.29 existe un grupo dedicado exclusivamente a la regulación y a la creación de documentos relacionados con los CAV denominado GRVA[17] (*Working Party on Automated/Autonomous and connected Vehicles*). En su wiki de internet[18] se pueden consultar sus calendarios de reuniones así como las agendas y minutas de las mismas.

[16] https://unece.org
[17] https://unece.org/transport/vehicle-regulations/working-party-automatedautonomous-and-connected-vehicles-introduction
[18] https://wiki.unece.org/pages/viewpage.action?pageId=63310525

4.6.1. UNECE R155

La norma UNECE R155 establece un marco para la homologación de los vehículos en materia tanto de las medidas de seguridad implementadas en los modelos como de los sistemas de gestión de ciberseguridad (CSMS, *Cibersecurity Management Systems*) de las organizaciones. La UNECE R155 considera que los métodos recogidos en los CSMS han de abarcar procesos tanto organizativos como de responsabilidad y gobernanza, además de ser sistemáticos y orientados a la gestión de riesgos asociados a las amenazas de ciberseguridad de los vehículos. La norma es de aplicación para vehículos de categoría:

- M, coches y autobuses;
- N, furgonetas y camiones;
- O, remolques y caravanas que equipen al menos una ECU; y
- L_6 y L_7, cuadriciclos ligeros y sin cabina con al menos nivel 3 de conducción autónoma.

Para conseguir la aprobación, en primer lugar el fabricante debe obtener el Certificado de Aprobación de su sistema de gestión de ciberseguridad (CSMS). Para ello debe aportar a la Autoridad de Aprobación designada en cada Estado miembro:

- documentación detallada sobre el CSMS, y
- documentación que demuestre que el CSMS cumple con los requisitos de ciberseguridad definidos en el Anexo 5 de la norma.

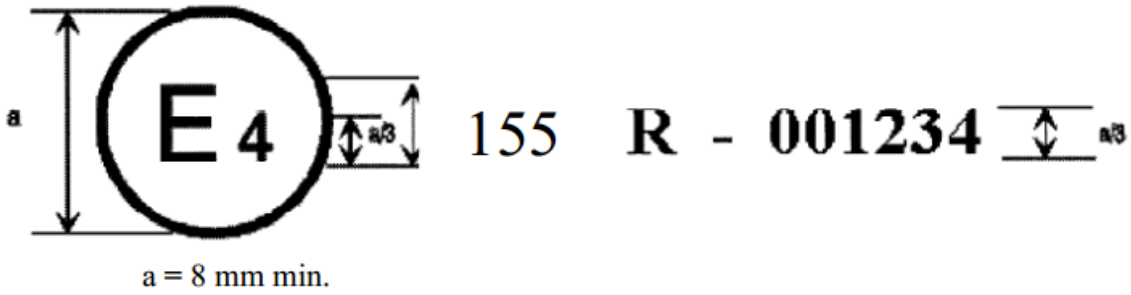
Una vez aportada la documentación, los servicios técnicos de la AP concederán o denegarán un Certificado de Cumplimiento del CSMS el cual es válido por 3 años, tras los cuales puede renovarse. Durante los 3 años de vigencia, el certificado puede revocarse si la AP lo considera oportuno.

El Certificado de Cumplimiento del CSMS acredita la ciberseguridad de los procesos del fabricante a nivel organizativo. No obstante, para cada modelo de vehículo que el fabricante quiera homologar, es necesario aportar, además del Certificado de Cumplimiento del CSMS, la siguiente documentación:

- Un plan de gestión de riesgos donde se muestren las políticas de mitigación del modelo en particular que se quiere homologar.
- Un plan de medidas para la actualización segura del software.
- Un plan de pruebas técnicas que el fabricante considere suficientes para validar la idoneidad de las medidas propuestas.
- Mapas de procesos aplicados a la ciberseguridad en todo el ciclo de vida del producto.

Una vez terminada la certificación de aprobación del tipo de vehículo, el vehículo está obligado a portar un identificativo que certifique su conformidad con R155.

Imagen 26. Identificativo de cumplimiento con la norma R155



Fuente: UNECE R155

En el Anexo 5 de la norma se establecen los requisitos exigidos en materia de ciberseguridad a los fabricantes. También se hace un análisis TVA (amenazas, vulnerabilidades y ataques) más comunes.

Muchas de las vulnerabilidades se corresponden a ataques internos, dentro de la red del vehículo como accesos no autorizados al CAN bus, puertos USB, etc.

En la tabla A1, sección 4.3.2 se listan las vulnerabilidades asociadas a los canales de comunicación externos identificadas por la UNECE, varias de las cuales coinciden con las indicadas en el capítulo 3 de este documento; por ejemplo, DoS, *spoofing* de mensajes, ataques Sybil, MITM y *black hole*.

No obstante, cabe mencionar que muchos requisitos, en la forma en que están escritos, son de difícil cumplimiento por parte de los fabricantes. Por ejemplo, se requiere que se incorporen mecanismos de autenticación y protección tanto para la información transmitida como la recibida. En el caso de la información transmitida, el vehículo puede integrar mecanismos como los vistos en este TFM para la protección de la misma. Sin embargo, en el caso de la información recibida, poco o nada puede hacer el fabricante del vehículo para asegurarse que el otro extremo de la comunicación, el extremo del transmisor, incorpora los mecanismos necesarios para su autenticado o cifrado.

En cualquier caso, asumiremos que el vehículo debe estar preparado para gestionar mensajes entrantes cifrados y autenticados, aunque no esté en su mano aplicar en origen estos métodos de protección.

A continuación mostramos una tabla que recoge los requisitos exigidos por la UNECE R155 relacionados con las comunicaciones externas.

Se añade una columna con la contramedida propuesta para poder cumplir con el requisito.

Tabla 16. Requisitos UNECE R155 de seguridad de las comunicaciones

Requisito R155		Amenaza	Contramedida	Observaciones
Ref.	Descripción			
M10	El vehículo deberá verificar la autenticidad e integridad de los mensajes que recibe	*Spoofing* y suplantación mensajes V2X o GNSS por suplantación Ataque de suplantación (mensajes de fuentes falsas) Ataque MITM	Autenticación	El fabricante del vehículo no puede garantizar la autenticación en el sistema transmisor
		Reenvío de paquetes (replay attack)		
M11	Se deberán implementar métodos seguros para el almacenamiento de claves seguras	Ataques Sybil (simulación de varios vehículos en la vía)	Autenticación	
M12	La información sensible transmitida o recibida deberá ser protegida adecuadamente	Interceptación o escucha no autorizada de transmisiones	Cifrado	Ha de ser implementado igualmente en el extremo opuesto de la comunicación
M13	Se deberán emplear medios de recuperación frente a ataques DoS	Envío masivo de paquetes (*spamming*/DoS)	Detección DoS	
		Ataque *black hole*	Detección DoS	
M14	Se deberán considerar métodos para la protección contra *malware*	*Malware*	Actualizaciones OTA	
M16	Se implementarán métodos de actualización del sistema	Corrupción de actualizaciones OTA	Firmado digital de actualizaciones	Ha de ser implementado en el servidor de actualizaciones

5. CONCLUSIONES

El objetivo marcado al principio de este TFM ha sido alcanzado. Se ha realizado un estudio de las vulnerabilidades, amenazas y riesgos de las comunicaciones V2X desde el punto de vista de la ciberseguridad, y se han propuesto contramedidas que las subsanen o las mitiguen.

Se han investigado las arquitecturas CAV y las tecnologías V2X más relevantes hoy en día. Hemos visto que las basadas en Wi-Fi están suficientemente probadas, sus limitaciones son conocidas y tienen suficiente madurez como para ser desplegadas. Existen estándares, DSRC/WAVE y C-ITS, que definen completamente la arquitectura de los sistemas, y ya hay ejemplos de funcionamiento en carreteras de Europa, Japón y EE.UU. No obstante, aparentemente el despliegue de las comunicaciones V2X basadas en Wi-Fi se está encontrando con más escollos de los que cabría esperar.

En paralelo se está desarrollando C-V2X, otra tecnología basada en LTE y 5G. Ésta ofrece mejor rendimiento en algunos aspectos pero no está probada completamente ni existe ningún estándar que defina una arquitectura completa; además, 5G NR-V2X no es compatible hacia atrás con LTE-V2X. A día de hoy no está claro cuál de las dos opciones será la dominante en el futuro, pero parece evidente que los intereses enfrentados de fabricantes y países, alineados a favor de una u otra tecnología, están bloqueando un esfuerzo común por parte de la industria orientado al desarrollo y la implantación definitiva de V2X en las carreteras de todo el mundo.

La digitalización de los automóviles va a ir incrementándose. Los vehículos se van a convertir en plataformas interconectadas de gestión de grandes volúmenes de datos, lo que significa que también serán más vulnerables a ataques. En este TFM hemos analizado la ciberseguridad de las comunicaciones V2X, descubriendo que son vulnerables a varios ataques debido a la exposición de las superficies de ataque y del canal inalámbrico. Por tanto, es primordial protegerlas frente a las amenazas, no hacerlo podría acarrear consecuencias catastróficas.

En particular, los ataques dirigidos contra la disponibilidad de los servicios, como DoS o la interferencia intencionada, pueden ser muy dañinos. Asimismo, las redes deben estar protegidas contra el *malware* y la falsificación de mensajes. En este sentido, cobra vital importancia que se implementen medios de autenticación, y de detección de ataques, así como que se asegure el acceso de los vehículos a actualizaciones de software seguras. Sin embargo, es necesario llegar a un compromiso, ya que un exceso en el uso de medios criptográficos de firma digital y de cifrado de información sobrecargaría el sistema en términos de tiempos de

procesamiento, degradando su rendimiento y su latencia, un parámetro que es clave en V2X. También hemos visto que se están proponiendo formas de aplicar técnicas novedosas de ML/DL y *blockchain* a la ciberseguridad de las comunicaciones V2X.

En los últimos años varios reguladores y organizaciones de estandarización han empezado a poner el foco en la ciberseguridad de los vehículos. La involucración de la UNECE, entidad perteneciente a la ONU, da una idea de la importancia a nivel global que se le está dando al hecho de que a partir de ahora los automóviles han de ser ciberseguros. Esta normativa se va a empezar a aplicar en la UE a partir del 1 de julio de 2022, antes incluso de que las vías estén preparadas para V2X y de que se venda un significativo número de modelos con soporte a dichas comunicaciones.

Del estudio realizado en este TFM se desprende que la tecnología CAV tiene potencial para traer un cambio revolucionario a la sociedad en la que vivimos, con profundas ramificaciones socio-económicas e incluso éticas. La práctica eliminación de los accidentes de tráfico y los embotellamientos, así como una drástica reducción de las emisiones, tendría gran impacto en los modelos de movilidad urbanos y en el día a día de las personas, y permitiría plantearse un amplio reordenamiento del espacio en las grandes ciudades. Asimismo, el que un algoritmo conduzca autónomamente, sin intervención humana, un vehículo con ocupantes humanos suscita un interesante debate ético sobre la posibilidad de que las decisiones de una máquina puedan llegar a suponer un riesgo para la vida de las personas.

Finalmente, en cuanto a las futuras líneas de investigación relacionadas con este TFM se pueden sugerir la investigación de protocolos de criptografía ligera (*lightweight cryptography*) aplicables a la autenticación en V2X, la investigación y desarrollo de nuevos protocolos de autenticación seguros para C-V2X y la búsqueda de nuevas formas de aplicar ML/DL y *blockchain* a la ciberseguridad en V2X.

6. GLOSARIO

5G NR	*5G New Radio*
ADAS	*Advanced Driver Assistance Systems*
C-ITS	*Cooperative-Intelligent Transport System*
C-V2X	*Cellular-Vehicle to Everything*
CAN	*Controller Area Network*
CAV	*Connected Autonomous Vehicle*
DoS	*Denial of Service*
DSRC	*Dedicated Short-Range Communications*
ECU	*Electronic Control Unit*
LTE-V2X	*Long Term Evolution – Vehicle to Everything*
MITM	*Main In the Middle*
OBU	*On-Board Unit*
RSU	*RoadSide Unit*
V2I	*Vehicle to Infrastructure*
V2N	*Vehicle to Network*
V2P	*Vehicle to Pedestrian*
V2V	*Vehicle to Vehicle*
V2X	*Vehicle to Everything*
VANET	*Vehicular Ad-hoc NETwork*
WAVE	*Wireless Access in Vehicular Environments*

7. BIBLIOGRAFÍA

[1] *History of the autonomous car* [en línea] [fecha de consulta: 7 de marzo de 2022]. Disponible en: https://www.titlemax.com/resources/history-of-the-autonomous-car

[2] *The grand challenge* [en línea] [fecha de consulta: 7 de marzo de 2022]. Disponible en: https://www.darpa.mil/about-us/timeline/-grand-challenge-for-autonomous-vehicles

[3] *Autopilot and full self-driving capability* | *Tesla* [en línea] [fecha de consulta: 7 de marzo de 2022]. Disponible en: https://www.tesla.com/support/autopilot

[4] TED. *How a driverless car sees the road* [vídeo en línea]. 2015 [consulta: 11 de marzo de 2022]. Disponible en: https://www.youtube.com/watch?v=tiwVMrTLUWg

[5] AHANGAR, M. Nadeem, AHMED, Qasim Z., KAHN, Fahd A. y HAFEEZ, Maryam. A survey of autonomous vehicles: enabling communication technologies and challenges. En: *Sensors* [en línea]. 2021. Vol. 21, nº 3, 706. ISSN 1424-8220 [consulta: 11 de marzo de 2022]. Disponible en: https://doi.org/10.3390/s21030706

[6] JUNG, Chanyoung, LEE, Daegyu, LEE, Seungwook y SHIM, David H. V2X-communication-aided autonomous driving: system design and experimental validation. En: *Sensors* [en línea]. 2020. Vol. 20, nº 10, 2903. ISSN 1424-8220 [consulta: 11 de marzo de 2022]. Disponible en: https://doi.org/10.3390/s20102903

[7] VARGHESE, Jaycil y BOONE, Randy. Overview of autonomous vehicle sensors and systems. En: *Proceedings of the 2015 international conference on operations excellence and service engineering, Orlando, Florida, USA, September 2015* [en línea]. 2015. Págs. 178-191. [consulta: 11 de marzo de 2022]. Disponible en: http://iieom.org/ICMOE2015/papers/140.pdf

[8] EIZA, Mahmoud H. y NI, Qiang. Driving with sharks: rethinking connected vehicles with vehicle cybersecurity. En: *IEEE Vehicular technology magazine* [en línea]. 2017. Vol. 12, nº 2, págs. 45-51. ISSN: 1556-6080 [consulta: 12 de marzo de 2022]. Disponible en: https://doi.org/10.1109/MVT.2017.2669348

[9] *5G and autonomous vehicles – accelerating data communication* speed [en línea] [fecha de consulta: 13 de marzo de 2022]. Disponible en: https://www.mewburn.com/news-insights/5g-and-autonomous-vehicles-accelerating-data-communication-speed

[10] *CAN for better autonomous vehicles* [en línea] [fecha de consulta: 13 de marzo de 2022]. Disponible en: https://www.microcontrollertips.com/can-for-better-autonomous-vehicles-faq

[11] AMJAD, Zubair, SIKORA, Axel, HILT, Benoit y LAUFFENBURGER, Jean-Philippe. Low latency V2X applications and network requirements: performance evaluation. En: *IEEE Intelligent vehicles symposium* [en línea]. 2018. Págs. 220-225. ISBN: 978-1-5386-4452-2 [consulta: 14 de marzo de 2022]. Disponible en: https://doi.org/10.1109/IVS.2018.8500531

[12] LU, Ning, CHENG, Nan, ZHANG, Ning, SHEN, Xuemin y MARK, Jon W. Connected vehicles: solutions and challenges. En: *IEEE Internet of things journal* [en línea]. 2014. Vol. 1, nº 4, págs. 289-299. ISSN: 2327-4662 [consulta: 14 de marzo de 2022]. Disponible en: https://doi.org/10.1109/JIOT.2014.2327587

[13] HASAN, Ahmed Shoeb, HOSSAIN, Md. Shohrab y ATIQUZZAMAN, Mohammed. Security threats in vehicular ad hoc networks. En: *International conference on advances in computing, communications and informatics (ICACCI), Jaipur, India, September 2016* [en línea]. 2016. Págs. 404-411. ISBN:978-1-5090-2029-4 [consulta: 17 de marzo de 2022]. Disponible en: https://doi.org/10.1109/ICACCI.2016.7732079

[14] GHORI, Muhammad, ZAMLI, Kamal, QUOSTHONI, Nik, HISYAM, Muhammad y MONTASER, Mohamed. Vehicular ad-hoc network (VANET): review. En: *2018 IEEE International conference on innovative research and development (ICIRD), Bangkok, Thailand, May 2018* [en línea]. 2018. Págs. 1-6. ISBN:978-1-5386-5696-9 [consulta: 17 de marzo de 2022]. Disponible en: https://doi.org/10.1109/ICIRD.2018.8376311

[15] ARENA, Fabio, PAU, Giovanni y SEVERINO, Alessandro. A review on IEEE 802.11p for intelligent transportation systems. En: *Journal of sensor and actuator networks* [en línea]. 2020. Vol. 9, nº 2, 22. ISSN 2224-2708 [consulta: 18 de marzo de 2022]. Disponible en: https://doi.org/10.3390/jsan9020022

[16] BAEE, Mir Ali Rezazadeh, SIMPSON, Leonie, FOO, Enest y PIEPRZYK, Josef. Broadcast authentication in latency-critical applications: on the efficiency of IEEE 1609.2. En: *IEEE Transactions on vehicular technology* [en línea]. 2019. Vol. 68, nº 12, págs. 11577-11587. ISSN: 1939-9359 [consulta: 18 de marzo de 2022] Disponible en: https://doi.org/10.1109/TVT.2019.2945339

[17] FESTAG, Andreas. Standards for vehicular communications – from IEEE 802.11p to 5G. En: *Elektrotech. Inftech.* [en línea]. 2015. Vol. 132, págs. 409 – 416. [consulta: 19 de marzo de 2022]. Disponible en: https://doi.org/10.1007/s00502-015-0343-0

[18] *NXP, Volkswagen and several European projects bet on WiFi DSRC for V2X | IoT times* [en línea] [fecha de consulta: 19 de marzo de 2022]. Disponible en: https://iot.eetimes.com/nxp-volkswagen-and-several-european-projects-bet-on-wifi-dsrc-for-v2x

[19] *NXP, Volskwagen and partners continue to accelerate the V2X rollout | NXP semiconductors* [en línea] [fecha de consulta: 19 de marzo de 2022]. Disponible en: https://www.nxp.com/company/blog/nxp-volkswagen-and-partners-continue-to-accelerate-the-v2x-rollout:BL-THE-V2X-ROLLOUT

[20] NAGHSH, Zahra y VALAEE, Shahrokh. Delay-aware conflict-free scheduling for LTE-V, sidelink 5G V2X vehicular communication, in highways. En: *52nd Asilomar conference on signals, systems and computers* [en línea]. 2018. Págs. 1452-1456 ISSN: 2576-2303 [consulta: 20 de marzo de 2022]. Disponible en: https://doi.org/10.1109/ACSSC.2018.8645203

[21] MOLINA-MASEGOSA, Rafael y GOZÁLVEZ, Javier. LTE-V for sidelink 5G V2X vehicular communications: a new 5G technology for short-range vehicle-to-everything communications. En: *IEEE Vehicular technology magazine* [en línea]. 2017. Vol. 12, nº 4, págs. 30-39. ISSN: 1556-6072 [consulta: 20 de marzo de 2022]. Disponible en: https://doi.org/10.1109/MVT.2017.2752798

[22] ALI, Zoraze, LAGÉN, Sandra, GIUPPONI, Lorenza y ROUIL, Richard. 3GPP NR V2X mode 2: overview, models and system-level evaluation. En: *IEEE Access* [en línea]. 2021. Vol. 9, págs. 89554-89579. ISSN: 2169-3536 [consulta: 20 de marzo de 2022]. Disponible en: https://doi.org/10.1109/ACCESS.2021.3090855

[23] CASTAÑEDA-GARCÍA, Mario, MOLINA-GALÁN, Alejandro, BOBAN, Mate, GOZÁLVEZ, Javier, COLL-PERALES, Baldomero, SAHIN, Taylan y KOUSARIDAS, Apostolos. A tutorial on 5G NR V2X communications. En: *IEEE Communications surveys & tutorials*. 2021. Vol. 23, nº 3, págs. 1972-2026.ISSN: 1553-877X [consulta: 20 de marzo de 2022]. Disponible en: https://doi.org/10.1109/COMST.2021.3057017

[24] ASHRAF, Shehzad A., BLASCO, Ricardo, DO, Hieu, FODOR, Gábor, ZHANG, Congchi y SUN, Wanlu. Supporting vehicle-to-everything services by 5G new radio Release-16 systems. En: *IEEE Communications standards magazine* [en línea]. 2020. Vol. 14, nº 1, págs. 26-32. ISSN: 2471-2833 [consulta: 20 de marzo de 2022]. Disponible en: https://doi.org/10.1109/MCOMSTD.001.1900047

[25] *Our members – 5G Automotive Association* [en línea] [fecha de consulta: 21 de marzo de 2022]. Disponible en: https://5gaa.org/membership/our-members

[26] *El primer tramo de autopista inteligente en España para coches autónomos estará en el País Vasco y será operativo en 2024* [en línea] [fecha de consulta: 21 de marzo de 2022]. Disponible en: https://www.motorpasion.com/futuro-movimiento/primera-autopista-inteligente-espanola-para-coches-autonomos-estara-pais-vasco-abrira-2024-tendra-57-km-largo

[27] SHI, Mengkai, LU, Chang, ZHANG, Yi y YAO, Danya. DSRC and LTE-V communication performance evaluation and improvement based on typical V2X application at intersection. En: *2017 Chinese automation congress (CAC)* [en línea]. 2017. Págs. 556-561. ISBN:978-1-5386-3524-7 [consulta: 25 de marzo de 2022]. Disponible en: https://doi.org/10.1109/CAC.2017.8242830

[28] CHEN, Shanzhi, HU, Jinling, SHI, Yan y ZHAO, Li. LTE-V: A TD-LTE-based V2X solution for future vehicular network. En: *IEEE Internet of things journal* [en línea]. 2016. Vol. 3, nº 6, págs. 997-1005. ISSN: 2327-4662 [consulta: 25 de marzo de 2022]. Disponible en: https://doi.org/10.1109/JIOT.2016.2611605

[29] BIN ALI, Chaeriah, ARMI, Nasrullah, MITAYANI, Arumjeni, KURNIAWAN, Dayat, SURYADI SATYAWAN, Arief y SUBEKTI, Agus. Analysis of IEEE 802.11p MAC protocol for safety message broadcast in V2V communication. En: *2020 International conference on radar, antenna, microwave, electronics and telecommunications (ICRAMET)* [en línea]. 2020. Págs. 320-324. Electronic ISBN: 978-1-7281-8922-2 [consulta: 29 de marzo de 2022]. Disponible en: https://doi.org/10.1109/ICRAMET51080.2020.9298654

[30] NAIK, Gaurang, CHOUDHURY, Biplav y PARK, Jung-Min. IEEE 802.11bd & 5G NR V2X: evolution of radio access technologies for V2X communications. En: *IEEE Access* [en línea]. 2019. Vol. 7, págs. 70169-70184. ISSN: 2169-3536 [consulta: 29 de marzo de 2022]. Disponible en: https://doi.org/10.1109/ACCESS.2019.2919489

[31] ANWAR, Waqar, FRANCHI, Norman y FETTWEIS, Gerhard. Physical layer evaluation of V2X communications technologies: 5G NR-V2X, LTE-V2X, IEEE 802.11bd and IEEE 802.11p. En: *IEEE 90th Vehicular technology conference (VTC2019-Fall)* [en línea]. 2019. Págs. 1-7. ISSN: 2577-2465 [consulta: 29 de marzo de 2022]. Disponible en: https://doi.org/10.1109/VTCFall.2019.8891313

[32] NOOR-A-RAHIM, Md, LIU, Zilong, HAEYOUNG, Lee, KHYAM, Mohammad Omar, HE, Jianhua, PESCH, Dirk, MOESSNER, Klaus, SAAD, Walid y POOR, H. Vincent. *6G for vehicle-to-everything (V2X) communications: enabling technologies, challenges and opportunities* [en línea]. 2020. [consulta: 29 de marzo de 2022]. Disponible en: https://doi.org/10.48550/arXiv.2012.07753

[33] *El 5G y los coches autónomos: por qué es la piedra angular de la guerra comercial entre China y EE.UU.* [en línea] [fecha de consulta: 31 de marzo de 2022]. Disponible en: https://www.motorpasion.com/industria/5g-coches-autonomos-que-piedra-angular-guerra-comercial-china-ee-uu

[34] *Guerra de estándares para el coche conectado EE.UU. y China ya apuestan por el 5G mientras Europa sigue debatiendo* [en línea] [fecha de consulta: 31 de marzo de 2022]. Disponible en: https://www.xataka.com/vehiculos/guerra-estandares-para-coche-conectado-eeuu-china-apuestan-5g-europa-sigue-debatiendo-wi-fi

[35] *El 5G gana terreno: Europa rechaza establecer el Wi-Fi como estándar para los coches conectados* [en línea] [fecha de consulta: 31 de marzo de 2022]. Disponible en: https://www.motorpasion.com/tecnologia/5g-gana-terreno-europa-rechaza-establecer-wi-fi-como-estandar-para-coches-conectados

[36] *EU Council rejects European Comission's Wi-Fi plans for connected and autonomous vehicles* [en línea] [fecha de consulta: 31 de marzo de 2022]. Disponible en: https://hsfnotes.com/cav/2019/07/18/eu-council-rejects-european-commissions-wi-fi-plans-for-connected-and-autonomous-vehicles

[37] *BMW pide a Alemania frenar los planes de establecer el Wi-Fi como estándar tecnológico para los coches conectados* [en línea] [fecha de consulta: 31 de marzo de 2022]. Disponible en: https://www.motorpasion.com/tecnologia/bmw-pide-a-europa-frenar-planes-establecer-wi-fi-como-estandar-tecnologico-para-coches-conectados

[38] *FCC modernizes 5.9 GHz band for Wi-Fi* [en línea] [fecha de consulta: 31 de marzo de 2022]. Disponible en: https://docs.fcc.gov/public/attachments/DOC-368228A1.pdf

[39] *Bulc urges 5G advocates to focus on autonomous driving, leave connected cars to Wi-Fi* [en línea] [fecha de consulta: 31 de marzo de 2022]. Disponible en: https://www.euractiv.com/section/road-safety/interview/bulc-urges-5g-advocates-to-focus-on-autonomous-driving-leave-connected-cars-to-wifi

[40] SHEEHAN, Barry, MURPHY, Finbarr, MULLINS, Martin y RYAN, Cian. Connected and autonomous vehicles: a cyber-risk classification framework. En: *Transportation research part A: policy and practice* [en línea]. 2019. Vol. 124, págs. 523-536. ISSN: 0965-8564 [fecha de consulta: 2 de abril 2022]. Disponible en: https://doi.org/10.1016/j.tra.2018.06.033

[41] LAURENDEAU, Christine y BARBEAU, Michel. Threats to security in DSRC/WAVE. En: *Ad-hoc, mobile, and wireless networks ADHOC-NOW* [en línea]. 2006. Lecture notes in computer science, vol 4104, págs. 266-280. Springer, Berlin, Heidelberg, New York. ISBN: 978-3-540-37248-6 [consulta: 8 de abril de 2022]. Disponible en: https://doi.org/10.1007/11814764_22

[42] MAROJEVIC, Vuk. *C-V2X Security requirements and procedures: survey and research directions* [en línea]. 2018. [consulta: 9 de abril de 2022]. Disponible en: https://arxiv.org/abs/1807.09338

[43] MUHAMMAD, Mujahid y SAFDAR, Ghazanfar Ali. Survey on existing authentication issues for cellular-assisted V2X communication. En: *Vehicular communications* [en línea]. 2018. Vol. 12, págs. 50-65. ISSN: 2214-2096 [consulta: 9 de abril de 2022]. Disponible en: https://doi.org/10.1016/j.vehcom.2018.01.008

[44] MONTEUUIS, Jean-Philippe, PETIT, Jonathan, ZHANG, Jun, LABIOD, Houda, MAFRICA, Stefano y SERVEL. Alain. *Attacker model for Connected and Automated Vehicles* [en línea]. 2018. [consulta: 10 de abril de 2022]. Disponible en: https://cscs.mpi-inf.mpg.de/files/2018/09/01-Attacker-model-for-Connected-and-Automated-Vehicles.pdf

[45] McCALL, Sophia, YUCEL, Cagatay y KATOS Vasilios. Education in cyber physical systems security: the case of connected autonomous vehicles. En: *2021 IEEE Global engineering education conference (EDUCON)* [en línea]. 2021. Págs. 1379-1385. ISSN: 2165-9567 [consulta: 12 de abril de 2022]. Disponible en: https://doi.org/10.1109/EDUCON46332.2021.9454086

[46] CYBERCAMP. *Car hacking* [vídeo en línea]. 2019 [consulta: 12 de abril de 2022]. Disponible en: https://cybercamp.es/videos/car-hacking

[47] MILLER, Charlie. Lessons learned from hacking a car. En: *IEEE Design & test* [en línea]. 2019. Vol. 36, págs. 7-9. ISSN: 2168-2364 [consulta: 12 de abril de 2022]. Disponible en: https://doi.org/10.1109/MDAT.2018.2863106

[48] *Hackers under the hood E&T magazine* [en línea] [fecha de consulta: 12 de abril de 2022]. Disponible en: https://eandt.theiet.org/content/articles/2020/03/hackers-under-the-hood

[49] *Car hacking: hackers driving your car | Medium* [en línea] [fecha de consulta: 12 de abril de 2022]. Disponible en: https://medium.com/resethacker/car-hacking-hackers-driving-your-car-64ce577a367f

[50] MOHD, Tauheed Khan, MAJUMDAR, Subhrajit, MATHUR, Akshay y JAVAID, Ahmad Y. Simulation and analysis of DDoS attack on connected autonomous vehicular network using OMNET++. En: *9th IEEE Annual ubiquitous computing, electronics & mobile communication conference (UEMCON)* [en línea]. 2018. Págs. 502-508. ISBN: 978-1-5386-7693-6 [consulta: 16 de abril de 2022]. Disponible en: https://doi.org/10.1109/UEMCON.2018.8796717

[51] ZHANG, Tao, ANTUNES, Helder y AGGARWAL, Siddhartha. Defending connected vehicles against malware: challenges and a solution framework. En: *IEEE Internet of things journal* [en línea]. 2014. Vol. 1, nº 1, págs. 10-21. ISSN: 2327-4662 [consulta: 17 de abril de 2022]. Disponible en: https://doi.org/10.1109/JIOT.2014.2302386

[52] *Keen security lab blog* [en línea] [fecha de consulta: 17 de abril de 2022]. Disponible en: https://keenlab.tencent.com/en/

[53] ABDULLAHI, Ahmed, DARGAHI, Tooska y BABAIE, Meisam. Vulnerability assessment of vehicle to infrastructure communication: a case study of unmanned ground vehicle. En: *IEEE Globecom workshops* [en línea]. 2020. Págs. 1-6. ISBN: 978-1-7281-7307-8 [consulta: 19 de abril de 2022]. Disponible en: https://doi.org/10.1109/GCWkshps50303.2020.9367408

[54] WHYTE, William, PETIT, Jonathan, KUMAR, Virendra, MORING, John y RICHARD, Roy. Threat and countermeasures analysis for WAVE service advertisement En: *IEEE 18th International conference on intelligent transportation systems* [en línea]. 2015. Págs. 1061-1068. ISSN: 2153-0017 [consulta: 20 de abril de 2022]. Disponible en: https://doi.org/10.1109/ITSC.2015.176

[55] PARKINSON, Simon, WARD, Paul, WILSON, Kyle y MILLER, Jonathan. Cyber threats facing autonomous and connected vehicles: future challenges. En: *IEEE Transactions on intelligent transportation systems* [en línea]. 2017. Vol. 18, nº 11, págs. 2898-2915. ISSN: 1558-0016 [consulta: 25 de abril de 2022]. Disponible en: https://doi.org/10.1109/TITS.2017.2665968

[56] STEPZINSKI, Michael y SENGUPTA, Shamik. Cybersecurity analysis in dedicated short-range communications in vehicular networks. En: *11th IEEE Annual ubiquitous computing, electronics & mobile communication conference (UEMCON)* [en línea]. 2020. Págs. 21-27. ISBN: 978-1-7281-9656-5 [consulta: 25 de abril de 2022]. Disponible en: https://doi.org/10.1109/UEMCON51285.2020.9298044

[57] LYAMIN, Nikita, VINEL, Alexey, JONSSON, Magnus y LOO, Jonathan. Real-time detection of Denial-of-Service attacks in IEEE 802.11p vehicular networks. En: *IEEE Communications letters* [en línea]. 2014. Vol. 18, nº 1, págs. 110-113. ISSN: 1558-2558 [consulta: 25 de abril de 2022]. Disponible en: https://doi.org/10.1109/LCOMM.2013.102213.132056

[58] *Understanding automotive OTA* [en línea] [fecha de consulta: 26 de mayo de 2022]. Disponible en: https://www.pathpartnertech.com/understanding-automotive-ota-over-the-air-update

[59] CHIDARA, Nagarjuna, NIBHANUPUDI, Chinmayi y VENKATARAMAN, Hrishikesh. Integration of different cryptographic techniques for real-time V2V communication: poster. En: *Proceedings of the 17th ACM international symposium on mobile ad hoc networking and computing (MobiHoc '16)* [en línea]. 2016. Págs. 379–380. [consulta: 27 de abril de 2022]. Disponible en: https://doi.org/10.1145/2942358.2942404

[60] LO, Nai-Wei y TSAI, Hsiao-Chien. Illusion attack on VANET applications – a message plausibility problem. En: *IEEE Globecom workshops* [en línea]. 2007. Págs. 1-8. ISSN: 2166-0077 [consulta: 28 de abril de 2022]. Disponible en: https://doi.org/10.1109/GLOCOMW.2007.4437823

[61] MENDIBOURE, Léo, CHALOUF, Mohamed y KRIEF, Francine. Toward new intelligent architectures for the internet of vehicles. En: *Intelligent network management and control*. 2021. Págs. 193-215. [consulta: 2 de mayo de 2022]. Disponible en: http://dx.doi.org/10.1002/9781119817840.ch8

[62] EL-REWINI, Zeinab, SADATSHARAN, Karthikeyan, SUGUNARAJ, Niroop, SELVARAJ, Daisy Flora, PLATHOTTAM, Siby Jose y RANGANATHAN, Prakash. Cybersecurity attacks in vehicular sensors. En: *IEEE Sensors journal* [en línea]. 2020. Vol. 20, nº 22, págs. 13752-13767. ISSN: 1558-1748 [consulta: 30 de abril de 2022]. Disponible en: https://doi.org/10.1109/JSEN.2020.3004275

[63] MENDIBOURE, Léo, MAALOUL, Saasi y ANISS, Hasnaa. Towards an adaptive blockchain for internet of vehicles. En: *Communication technologies for vehicles* [en línea]. 2021. Lecture notes in computer science, vol. 13120. Springer, Cham. ISBN: 978-3-030-92684-7 [consulta: 30 de abril de 2022]. Disponible en: https://doi.org/10.1007/978-3-030-92684-7_4

[64] KHAN, Adnan, BALAN, Kuhanraj, JAVED, Yasir, TARMIZI, Seleviawati y ABDULLAH, Johari. Secure trust-based blockchain architecture to prevent attacks in VANET. En: *Sensors* [en línea]. 2019. Vol. 19, nº 22, 4988. ISSN: 1424-8220 [consulta: 1 de mayo de 2022]. Disponible en: https://doi.org/10.3390/s19224954

[65] SAE J3016_202104. *Taxonomy and definitions for terms related to on-road motor vehicle automated driving systems*. Disponible en: https://www.sae.org/standards/content/j3016_202104

[66] SAE J3061_202112. *Cybersecurity guidebook for cyber-physical vehicle systems*. Disponible en: https://www.sae.org/standards/content/j3061_202112

[67] ISO 26262-1:2018. *Road vehicles —functional safety — Part 1: vocabulary*. Disponible en: https://www.iso.org/standard/68383.html

[68] ISO/SAE 21434:2021. *Road vehicles — cybersecurity engineering*. Disponible en: https://www.iso.org/standard/70918.html

[69] UN REGULATION No. 155. *Cyber security and cyber security management system*. Disponible en: https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security

[70] UN REGULATION No. 156. *Software update and software update management system*. Disponible en: https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update

[71] *Un año para que solo se puedan homologar coches ciberseguros. ¿Están listas las marcas?* [en línea] [fecha de consulta: 8 de mayo de 2022]. Disponible en: https://hackercar.com/homologar-coches-ciberseguros-marcas