Desarrollo de soluciones tecnológicas necesarias basadas en 5G para el despliegue del vehículo conectado y validación de casos de uso (5GVEC)

Expediente: TSI-065100-2022-001

E15.1. ESTADO DEL ARTE DE ESTÁNDARES Y CERTIFICACIONES INTERNACIONALES EN EL CAMPO DE LA CIBERSEGURIDAD Y LA CONECTIVIDAD PARA LA MOVILIDAD SEGURA Y EFICIENTE

PARTE 1: CONECTIVIDAD

RESUMEN EJECUTIVO

Consorcio: DEKRA, ERICSSON, TINAMICA, TUPL, SOFTCRITS, PREMO, TOPdigital

Financia: Gobierno de España, Ministerio para la Transformación Digital y de la Función Pública; Financiado por la Unión Europea NextGenerationEU

Cofinancia: Plan de Recuperación, Transformación y Resiliencia

Tabla de contenido

1. INTRODUCCIÓN 2

2. OBJETIVOS PRINCIPALES 2

3. RESUMEN EJECUTIVO 2

4. PRINCIPALES CONCLUSIONES 3

1. INTRODUCCIÓN

Este entregable forma parte del Paquete de Trabajo 3 “Casos de uso y aplicaciones” y constituye la Parte 1 del entregable E15 que se ha dividido en Parte 1: Conectividad y Parte 2: Ciber seguridad.

La parte 1 recoge los resultados del estudio y análisis de los estándares de referencia principalmente relativos a los modelos de arquitectura y requisitos de la misma para dar soporte las comunicaciones vehiculares

2. OBJETIVOS PRINCIPALES

Este entregable refleja el estado del arte de estándares y certificaciones internacionales en el campo de la conectividad para la movilidad segura y eficiente.

Los objetivos principales del entregable son:

- Analizar las organizaciones de referencia y estándares relativos a los aspectos de conectividad del vehículo y ciberseguridad.
- Analizar los requisitos de infraestructura para la conducción automática y conectada
- Seleccionar los requisitos básicos de infraestructura que garanticen las condiciones requeridas para la conducción segura y eficiente en Europa de manera interoperable y estandarizada.

3. RESUMEN EJECUTIVO

En este entregable se recoge el análisis pormenorizado de organizaciones de referencia y estándares relativos a los aspectos de conectividad del vehículo principalmente enfocado a los requisitos de la arquitectura de red necesarios para dar soporte a la conducción conectada y segura. El análisis de estándares relativos a casos de uso y sus requisitos se recogen en el entregable E16.

El documento recoge una introducción a las tecnologías de comunicaciones vehiculares y las diferentes interfaces existentes entre vehículo a la red, vehículos a otros vehículos, además de conectividad entre vehículos e infraestructura vial.

Aunque existen diferentes organizaciones definiendo estos estándares, las arquitecturas y requisitos propuestos por 3GPP/ETSI son las que cobran más relevancia para este proyecto y cuyas conclusiones se recogen en este documento, destacando los requisitos básicos que debe cumplir una red 5G para que permita, de manera segura y eficiente, la conducción autónoma y conectada.

Entre las organizaciones de referencia analizadas además de ETSI/3GPP, se encuentran las siguientes:

UNECE (United Nations Economic Commission for Europe): ha creado recientemente un "task force" denominado: "Vehicular Communications Definition, Overview, and Considerations" cuyo objetivo es reflejar una visión general de la definición, estructura, valor, usos y consideraciones para las comunicaciones vehiculares que actualmente está en desarrollo.

C-Roads: plataforma que aglutina a los Estados miembros europeos y a los operadores de carreteras, con el objetivo estratégico de integrar y aplicar Sistemas de Transporte Inteligente Cooperativo (C-ITS) a través de las fronteras nacionales para que los sistemas sean interoperables a través de toda Europa.

5GAA (5G Automotive Association): Ha publicado varios informes técnicos de especial relevancia para este proyecto que muestran el consenso de la industria de la automoción, la tecnología y las empresas de telecomunicación.

SAE (Society of Automotive Engineers): Ha especificado los mensajes V2X en diferentes estándares para los diferentes tipos de aplicaciones V2X, principalmente sobre la interfaz de corto alcance PC5, sin pasar por ninguna red de comunicaciones móviles.

IEEE (Institute of Electrical and Electronics Engineers): Ha publicado una serie de estándares relativos V2X para facilitar la comunicación y la interoperabilidad entre vehículos y su entorno. La serie IEEE 1609 es un conjunto de estándares que incluye: IEEE 1609.2 (capa de seguridad), IEEE 1609.3 (capa de red), IEEE 1609.4 (gestión de servicios de aplicaciones) e IEEE 1609.11 (gestión de certificados).

AECC (Automotive Edge Computing Consortium): Concluye que las especificaciones actuales de 3GPP no cubren completamente el desafío del big data de automoción y propone investigar cómo rediseñar la arquitectura del sistema y reconsiderar las implementaciones de red para adaptarse mejor al tráfico de datos esperado mediante una nueva arquitectura llamada "Distributed Computing on Localized Networks".

UIT (Unión Internacional de Telecomunicaciones): Ha constituido en 2024 un grupo de expertos enfocado a las Tecnologías de Comunicaciones para la conducción automatizada del cual DEKRA es miembro (ITU C-ITS Expert Group on Communications Technology for Automated Driving). Se prevé tener resultados para 2026.

4. PRINCIPALES CONCLUSIONES

La conducción conectada y segura se ha considerado una de las aplicaciones claves de las redes 5G. Sin embargo, para casos de uso de conducción avanzada en los que requieren de streaming o datos de sensores (como platooning o teleoperación) es necesario implementar mejoras en las redes 5G para cubrir los requisitos de latencia, calidad de servicio y ancho de banda necesarios en los casos de uso avanzados. Por ese motivo, varias organizaciones siendo la más relevante 3GPP, han propuesto mejoras en la arquitectura de red general 5G para cubrir estas necesidades específicas.

En cualquier caso, una vez analizadas las prestaciones que ofrece la red 5G y los requisitos específicos de comunicaciones V2X, se prevé que con la red celular mejorada, contemplando la

cobertura, las características de radio, y las capacidades demandadas por los casos de uso avanzados e incluyendo además funciones de red como MEC, QoS y Network Slicing, se podrán cubrir los requisitos específicos para la conducción avanzada, segura y eficiente.

Esta es la arquitectura mejorada que se propone en 3GPP/ETSI recogida en este documento.

Por otro lado, AECC ha analizado el volumen de datos que va a conllevar en el futuro la conectividad vehicular, afirmando que el volumen de datos transmitidos entre los vehículos y la nube será de unos 100 petabytes al mes por lo que concluyen que la arquitectura de red propuesta por 3GPP no será suficiente y proponen un nuevo modelo llamado “Distributed Computing on Localized Networks”, rediseñando la arquitectura del sistema y reconsiderando las implementaciones de red para adaptarse mejor al tráfico de red esperado.

En conclusión, como se recoge en este documento, diferentes organizaciones proponen diferentes arquitecturas de referencia que incluyen más o menos variaciones entre ellas, aunque el objetivo final debe ser la interoperabilidad y avanzar incorporando nuevas funciones de red para que cubran las necesidades de los casos de uso avanzados además del volumen de tráfico esperado.

Desarrollo de soluciones tecnológicas necesarias basadas en 5G para el despliegue del vehículo conectado y validación de casos de uso (5GVEC)

Expediente: TSI-065100-2022-001

E15. ESTADO DEL ARTE DE ESTÁNDARES Y CERTIFICACIONES INTERNACIONALES EN EL CAMPO DE LA CIBERSEGURIDAD Y LA CONECTIVIDAD PARA LA MOVILIDAD SEGURA Y EFICIENTE

Parte 2: Ciberseguridad

Resumen ejecutivo

Consorcio: DEKRA, ERICSSON, TINAMICA, TUPL, SOFTCRITS, PREMO Innovating in Magnetics, TOPdigital Grupo Empresarial

Financia: Gobierno de España, Ministerio para la Transformación Digital y de la Función Pública; Financiado por la Unión Europea NextGenerationEU

Cofinancia: Plan de Recuperación, Transformación y Resiliencia

Tabla de contenido

1. INTRODUCCIÓN 2

2. OBJETIVOS PRINCIPALES 2

3. RESUMEN EJECUTIVO 3

4. PRINCIPALES CONCLUSIONES 3

1. INTRODUCCIÓN

El presente documento es un resumen ejecutivo correspondiente al entregable E16: Análisis y selección de casos de uso de conducción conectada y automatizada, parte 2 - ciberseguridad, desarrollado en el marco del proyecto 5GVEC.

Este documento constituye la continuación del análisis realizado en la Parte 1 (Conectividad) y se centra específicamente en el estudio de los estándares, regulaciones y marcos normativos relacionados con la ciberseguridad del vehículo conectado.

La creciente complejidad de los vehículos modernos, caracterizados por una elevada conectividad, múltiples ECUs (Electronic Control Unit) y una intensa interacción con sistemas externos, hace imprescindible disponer de un marco normativo sólido que permita garantizar la protección de los sistemas, los datos y la seguridad de los pasajeros. En este contexto, el documento proporciona una visión estructurada y actualizada de las principales iniciativas regulatorias y de estandarización a nivel internacional en el ámbito de la ciberseguridad del vehículo.

2. OBJETIVOS PRINCIPALES

El objetivo principal del documento es analizar y recopilar el estado del arte de los estándares y regulaciones internacionales más relevantes en materia de ciberseguridad aplicables al vehículo conectado, con especial énfasis en los requisitos de seguridad asociados a los distintos componentes del vehículo y sus interfaces de comunicación.

De manera concreta, el documento persigue:

1. Identificar las organizaciones de referencia responsables de la regulación y estandarización de la ciberseguridad en el ámbito del vehículo conectado.

2. Analizar las regulaciones y estándares internacionales más relevantes, prestando especial atención a aquellos de obligado cumplimiento o de mayor aceptación en la industria.

3. Extraer y sistematizar los requisitos de seguridad definidos en dichos estándares, considerando los distintos componentes del ecosistema del vehículo conectado.

4. Establecer una base común que permita, en fases posteriores del proyecto, definir escenarios de ataque y metodologías de certificación alineadas con los requisitos identificados.

3. RESUMEN EJECUTIVO

El documento presenta un análisis exhaustivo de los principales marcos regulatorios, estándares y guías técnicas relacionados con la ciberseguridad del vehículo conectado. En primer lugar, se identifican las organizaciones internacionales de referencia, entre las que destacan UNECE, ISO/SAE, ITU-T y ETSI, así como otras instituciones y asociaciones relevantes que contribuyen al desarrollo de buenas prácticas y recomendaciones en el sector.

A partir de esta identificación, se realiza un estudio detallado de las regulaciones UNECE R155 y R156, que establecen, respectivamente, los requisitos para la gestión de la ciberseguridad (CSMS) y la gestión segura de actualizaciones de software (SUMS) a lo largo del ciclo de vida del vehículo. Asimismo, se analiza la norma ISO/SAE 21434, que define un marco integral para la ingeniería de la ciberseguridad en vehículos de carretera, junto con diversas recomendaciones de la ITU-T y especificaciones técnicas del ETSI orientadas a la protección de las comunicaciones V2X y de los sistemas ITS.

El documento culmina con la identificación y clasificación de los requisitos de seguridad extraídos de los estándares seleccionados. Estos requisitos se estructuran en función del componente objetivo del ataque (hardware, comunicaciones intravehículo, comunicaciones extravehículo, software/firmware y servidores backend) y de las propiedades de seguridad afectadas (confidencialidad, integridad, autenticidad, disponibilidad y anonimato). El resultado se plasma en tablas comparativas que facilitan la trazabilidad entre requisitos, vectores de ataque y estándares de referencia.

4. PRINCIPALES CONCLUSIONES

El análisis realizado evidencia que la ciberseguridad del vehículo conectado requiere un enfoque integral y multidimensional, dado el elevado número de componentes, interfaces y actores implicados en su funcionamiento. Los estándares y regulaciones analizados coinciden en la necesidad de garantizar, como pilares fundamentales, la confidencialidad, integridad y disponibilidad de los datos y sistemas, así como la autenticidad de las comunicaciones y la protección de la privacidad de los usuarios.

El documento concluye que las regulaciones y normas internacionales, en particular las desarrolladas por la UNECE y la ISO/SAE, constituyen el marco de referencia más sólido para evaluar y certificar la ciberseguridad de los vehículos conectados. La sistematización de los requisitos de seguridad realizada en este entregable proporciona una base técnica y normativa homogénea que permitirá, en las siguientes fases del proyecto, definir escenarios de ataque y metodologías de pruebas alineadas con los estándares internacionales y con las necesidades reales de la industria automotriz.

Desarrollo de soluciones tecnológicas necesarias basadas en 5G para el despliegue del vehículo conectado y validación de casos de uso (5GVEC)

Expediente: TSI-065100-2022-001

E16. ANÁLISIS Y SELECCIÓN DE CASOS DE USO DE CONDUCCIÓN CONECTADA Y AUTOMATIZADA

PARTE 1: CONECTIVIDAD

RESUMEN EJECUTIVO

Consorcio: DEKRA, ERICSSON, TINAMICA, TUPL, SOFTCRITS, PREMO Innovating in Magnetics, TOPdigital Grupo Empresarial

Financia: Gobierno de España, Ministerio para la Transformación Digital y de la Función Pública; Financiado por la Unión Europea NextGenerationEU

Cofinancia: Plan de Recuperación, Transformación y Resiliencia

Tabla de contenido

1. INTRODUCCIÓN 2

2. OBJETIVOS PRINCIPALES 2

3. RESUMEN EJECUTIVO 2

4. PRINCIPALES CONCLUSIONES 3

1. INTRODUCCIÓN

Este entregable forma parte del Paquete de Trabajo 3 “Casos de uso y aplicaciones”, y constituye la Parte 1 del entregable E16 que se ha dividido en Parte 1: Conectividad y Parte 2: Ciber seguridad.

La parte 1 recoge los resultados del estudio y análisis de casos de uso de conducción conectada y automatizada propuestos por organizaciones de estandarización (ETSI, 3GPP, UNECE, ISO), asociaciones de la industria (5GAA, CCAM, C-ROAD, Car2Car Consortium, ITS America) y otros proyectos europeos (Autopilot, Headstart, 5GMobix).

Además, se ha realizado una pre-selección de los casos de uso más destacados para desplegar y validar en el proyecto.

2. OBJETIVOS PRINCIPALES

El objetivo principal del entregable es analizar y seleccionar los casos de uso de conducción conectada y automatizada de referencia para este proyecto basándose en publicaciones y estándares que recogen la gran variedad de casos de uso aplicables a la movilidad conectada.

3. RESUMEN EJECUTIVO

En este entregable se recoge el análisis pormenorizado de casos de uso de conducción conectada propuestos por las organizaciones relevantes de estandarización, asociaciones y otros proyectos europeos como como 3GPP, 5GAA, ETSI, UNECE, ISO, CCAM, C-Road, y proyectos europeos de referencia como Autopilot, 5G-MOBIX, Headstart y Car2Car Consortium.

Se han identificado, seleccionado y priorizado aquellos casos de uso considerados esenciales, que se distinguen por ser coincidentes en las selecciones de casos de uso de los diferentes organismos como de interés para este proyecto, tanto para comunicaciones V2V/V2I como V2N (basados en la conectividad 5G)

Hay algunos casos de uso en los que, según sus requisitos de latencia, alcance o ancho de banda, pueden implementarse usando indistintamente comunicaciones de corto alcance PC5 o utilizando las comunicaciones móviles 5G a través del interfaz Uu.

En otros casos de uso es necesario utilizar el interfaz de corto alcance (requisitos de latencia) y en otros es la interfaz Uu la que aplica, sobre todo cuando existe intercambio de información con la Nube y el intercambio de información es mayor, tendencia a la que apunta en los nuevos casos de uso de comunicaciones vehiculares y donde factores como la calidad del dato, la privacidad y la ciberseguridad son requisitos más restrictivos.

Como conclusión, en la actualidad ambos interfaces de largo y corto alcance deben coexistir para poder desplegar casos de uso con requerimientos muy diferentes.

En el futuro, gracias a las mejoras de las comunicaciones celulares en cobertura, en capacidad radio y en la incorporación de nuevas funciones, es posible que todos los casos de uso puedan ser implementados a través de comunicaciones celulares.

Finalmente, se han identificado, seleccionado y priorizado aquellos casos de uso considerados esenciales, que se distinguen por ser coincidentes en las selecciones de casos de uso de los diferentes organismos como de interés para este proyecto, tanto para comunicaciones V2V/V2I como V2N (basados en la conectividad 5G) y evaluar así su adecuación. Se pretende continuar con el desarrollo, despliegue y validación de estos casos de uso seleccionados.

4. PRINCIPALES CONCLUSIONES

Se han analizado los casos propuestos por diferentes organizaciones de estandarización y se ha seleccionado un grupo de casos de uso representativo que permitan verificar los requisitos de las comunicaciones vehiculares. Cada una de ellas está proponiendo y priorizando casos de uso aunque en su mayor parte son comunes a todas ellas. Entre casi todas las organizaciones hay acuerdos de colaboración que garanticen la coherencia de los estándares y recomendaciones a nivel global.

Respecto a la interfaz más adecuada para la comunicación vehicular (V2V/V2I o V2N) va a depender de los requisitos específicos para la implementación de cada caso de uso. Como conclusión, en la actualidad ambos interfaces de largo y corto alcance deben coexistir para poder desplegar casos de uso con requerimientos muy diferentes.

En el futuro, gracias a las mejoras de las comunicaciones celulares en cobertura, en capacidad radio y en la incorporación de nuevas funciones es posible que todos los casos de uso puedan ser implementados a través de comunicaciones celulares.

A continuación, se muestra una tabla con el tipo de comunicación recomendado actualmente.

Caso de uso	Tecnología de comunicación válida	Tecnología de comunicación recomendada
Advertencias de peligros en la vía	V2I y V2N	V2N
Aproximación de un vehículo de emergencia	V2V/V2I y V2N	V2V/V2I
Mapas HD y recomendaciones de ruta	V2I y V2N	V2N

Caso de uso	Tecnología de comunicación válida	Tecnología de comunicación recomendada
Valet parking automatizado	V2V/V2I y V2N	V2N
Alerta y Predicción de Riesgo de Colisión con Usuarios Vulnerables de la Carretera	V2V/V2I y V2N	V2V/V2I
Teleoperación	V2N	V2N

Tabla 1. *Tecnologías recomendadas para cada Caso de uso*

Desarrollo de soluciones tecnológicas necesarias basadas en 5G para el despliegue del vehículo conectado y validación de casos de uso (5GVEC)

Expediente: TSI-065100-2022-001

E16. ANÁLISIS Y SELECCIÓN DE CASOS DE USO DE CONDUCCIÓN CONECTADA Y AUTOMATIZADA

Parte 2: Ciberseguridad

Resumen ejecutivo

Consorcio:

Financia:

Cofinancia:

Tabla de contenido

1. INTRODUCCIÓN 2

2. OBJETIVOS PRINCIPALES 2

3. RESUMEN EJECUTIVO 3

4. PRINCIPALES CONCLUSIONES 3

1. INTRODUCCIÓN

El presente documento es un resumen ejecutivo correspondiente al entregable E16: Análisis y selección de casos de uso de conducción conectada y automatizada, parte 2 - ciberseguridad, desarrollado en el marco del proyecto 5GVEC. Este entregable recoge y desarrolla los escenarios de ataque relevantes para evaluar la seguridad del vehículo conectado, tomando como base el análisis previo de requisitos de seguridad realizado en el entregable E15: Estado del arte de estándares y certificaciones internacionales.

La creciente conectividad de los vehículos, junto con el uso de comunicaciones V2X, actualizaciones OTA y servicios remotos, amplía de forma significativa la superficie de ataque. En este contexto, el documento aborda la necesidad de identificar, clasificar y describir escenarios de ataque representativos que permitan evaluar la robustez de los sistemas del vehículo conectado frente a amenazas que puedan comprometer su funcionamiento y la seguridad de los usuarios.

2. OBJETIVOS PRINCIPALES

El principal objetivo del documento es identificar y definir escenarios de ataque de ciberseguridad aplicables al vehículo conectado, alineados con los requisitos de seguridad establecidos en los estándares y regulaciones internacionales del sector de automoción.

1. Identificar los tipos de amenazas y ataques más relevantes que afectan a los vehículos conectados.
2. Definir un conjunto estructurado de casos de uso o escenarios de ataque, organizados según el componente del vehículo afectado.
3. Relacionar cada escenario de ataque con los estándares y normativas aplicables, garantizando la trazabilidad con los requisitos de seguridad analizados previamente.
4. Proporcionar una base sólida para el desarrollo posterior de metodologías de prueba, arquitectura de ensayos y planes de validación, que se abordarán en los entregables E17 y E18.

3. RESUMEN EJECUTIVO

El documento presenta un análisis exhaustivo de las amenazas de ciberseguridad en el vehículo conectado, comenzando por la identificación de los principales tipos de ataques, como malware, ransomware, inyección SQL, ataques Man-in-the-Middle, denegación de servicio, ataques de día cero, suplantación de identidad y amenazas persistentes avanzadas. Estas amenazas afectan tanto a los sistemas internos del vehículo como a sus comunicaciones con el exterior.

A partir de este análisis, se definen escenarios de ataque detallados, organizados en cinco grandes categorías: hardware, comunicaciones intravehículo, comunicaciones exteriores, software y servidores backend. Para cada escenario se describe de forma homogénea el trasfondo del ataque, el activo comprometido, los estándares a los que aplica, el objetivo perseguido, las precondiciones necesarias, la descripción del ataque y el veredicto esperado.

El documento establece además una correspondencia directa entre los escenarios de ataque y los estándares internacionales de referencia, tales como ISO/SAE 21434, UNECE R155 y R156. Esta trazabilidad facilita la evaluación del cumplimiento normativo y la posterior definición de pruebas de seguridad alineadas con los requisitos regulatorios del sector.

4. PRINCIPALES CONCLUSIONES

El análisis realizado pone de manifiesto que el vehículo conectado se enfrenta a una amplia variedad de amenazas de ciberseguridad que pueden afectar a la confidencialidad, integridad y disponibilidad de sus sistemas. La combinación de hardware complejo, redes internas, comunicaciones exteriores, software embebido y servicios backend incrementa notablemente la superficie de ataque y la complejidad de su protección.

La identificación sistemática de escenarios de ataque permite anticipar posibles vulnerabilidades y constituye un paso fundamental para diseñar estrategias de evaluación y mitigación adecuadas. El documento concluye que garantizar la seguridad del vehículo conectado requiere un enfoque integral, que contemple todos los componentes del ecosistema y esté alineado con los estándares y regulaciones internacionales.

Estos escenarios de ataque servirán como base para la definición y ejecución de pruebas de seguridad en las siguientes fases del proyecto, permitiendo evaluar de manera objetiva la resistencia de las ECUs (Electronic Control Unit) y de los sistemas asociados frente a ataques que podrían comprometer la seguridad del vehículo y de sus usuarios.

Desarrollo de soluciones tecnológicas necesarias basadas en 5G para el despliegue del vehículo conectado y validación de casos de uso (5GVEC)

Expediente: TSI-065100-2022-001

E17. METODOLOGÍAS DE PRUEBA Y ARQUITECTURA DE ENSAYOS

PARTE 1: CONECTIVIDAD

RESUMEN EJECUTIVO

Consorcio: DEKRA, ERICSSON, TINAMICA, TUPL, SOFTCRITS, PREMO Innovating in Magnetics, TOPdigital Grupo Empresarial

Financia: Gobierno de España, Ministerio para la Transformación Digital y de la Función Pública; Financiado por la Unión Europea NextGenerationEU

Cofinancia: Plan de Recuperación, Transformación y Resiliencia

Tabla de contenido

1. INTRODUCCIÓN 2

2. OBJETIVOS PRINCIPALES 2

3. RESUMEN EJECUTIVO 3

4. PRINCIPALES CONCLUSIONES 3

1. INTRODUCCIÓN

Este entregable recoge los resultados de la Tarea 3 de la A5 del proyecto 5GVEC. La tarea consiste en el diseño y desarrollo de métodos de medida y análisis, así como el diseño y desarrollo de herramientas de validación.

En los trabajos realizados en esta tarea se destacan los siguientes puntos:

- Definición de una metodología genérica de validación, cuyo objetivo es el desarrollo de la sistemática que permita evaluar soluciones de conducción conectada y automática frente a los estándares de referencia. Por otro lado, se han recogido los estándares aplicables a dispositivos de corto alcance en diferentes regiones y los esquemas de certificación para OBUs (On-Board Unit) y RSUs (RoadSide Unit).

  A partir de este análisis se han seleccionados los aspectos más relevantes en materia de metodología de pruebas aplicables a este proyecto y sus casos de uso como, por ejemplo, la identificación de los interfaces para los puntos de control y observación y la definición de los KPIs.

- Definición de la arquitectura de ensayos. Se ha definido la arquitectura de pruebas necesaria para realizar la validación, tanto de dispositivos como de aplicaciones ITS, considerando todos los elementos necesarios para pruebas en laboratorio o en movilidad para garantizar la calidad de los ensayos realizados. Se han definido dos entornos de prueba diferenciados: pista de pruebas con conectividad V2X y 5G (para ensayos en movilidad) y pruebas de conformidad en laboratorio.

- Diseño y desarrollo de los procedimientos de prueba para los casos de uso de este proyecto.

- Definición de planes de prueba para las tecnologías asociadas a la movilidad conectada. Para cada caso de prueba se han incluido al menos los siguientes campos: Identificador del caso de prueba, Objetivo de la prueba, Secuencia de la prueba, Estímulos necesarios, Captura de datos, Verificación del resultado.

2. OBJETIVOS PRINCIPALES

El objetivo principal de este documento es:

1. Establecer metodologías de prueba basadas en requisitos de infraestructura, garantizando la efectividad y eficiencia de las comunicaciones vehiculares.

2. Definir procedimientos técnicos y planes de prueba que faciliten la ejecución de validaciones robustas y fiables.

3. Identificar herramientas de soporte que aseguren la validación de los requisitos de seguridad.

3. RESUMEN EJECUTIVO

Este documento ha presentado un enfoque integral para la validación de casos de uso en comunicaciones vehiculares, cubriendo desde los requisitos técnicos de la infraestructura hasta las metodologías de prueba y herramientas de soporte necesarias para garantizar la funcionalidad, el rendimiento y la conectividad de las soluciones implementadas. La metodología propuesta junto con los KPIs (Key Performance Indicators) definidos, aseguran una validación eficaz y precisa de los casos de uso del proyecto representativos de las comunicaciones vehiculares V2X.

Se ha definido una metodología genérica de validación, donde se han considerado los diferentes tipos de prueba, los estándares aplicables en diferentes regiones, los esquemas de certificación, se ha adaptado a los casos de uso que se van a implementar en el proyecto 5GVEC y definidos en el E16.

Los resultados clave han sido:

- Identificación y priorización de casos de uso representativos, alineados con las normativas y necesidades de diversos organismos.
- Definición de KPIs y sus procedimientos de medida, que permiten medir la eficacia y eficiencia de los sistemas, abarcando aspectos funcionales, de conectividad, rendimiento y seguridad (recogidos en la Parte 2 de este entregable).
- Propuestas de entornos de prueba diferenciados que facilitan la validación de cada caso de uso, asegurando que se cumplan los criterios de aceptación establecidos.

4. PRINCIPALES CONCLUSIONES

Este documento ha presentado un enfoque integral para la validación de casos de uso en comunicaciones vehiculares, cubriendo desde los requisitos técnicos de la infraestructura hasta las metodologías de prueba y herramientas de soporte necesarias para garantizar la funcionalidad, el rendimiento y la conectividad de las soluciones implementadas. La metodología propuesta junto con los KPIs definidos, aseguran una validación eficaz y precisa de los casos de uso del proyecto representativos de las comunicaciones vehiculares V2X.

La definición de una metodología genérica de validación, donde se han considerado los diferentes tipos de prueba, los estándares aplicables en diferentes regiones, los esquemas de certificación, se ha adaptado a los casos de uso que se van a implementar en el proyecto 5GVEC y definidos en el E16. Los KPI más relevantes para validar los casos de uso se dividen en 3 categorías principales:

1. **Funcional:** Los KPI funcionales dependen de la definición y los requisitos funcionales de cada caso de uso específico.
2. **Rendimiento y conectividad:** La definición de los KPI más importantes a evaluar en las validaciones de desempeño de conectividad para casos de uso son:

- Latencia: El tiempo de transmisión o latencia es el tiempo necesario para transferir una determinada información desde un origen a un destino, medido en las interfaces del servicio de comunicación, desde el momento en que es transmitida por el origen hasta el momento en que se recibe exitosamente en el destino.

- Ancho de banda: El ancho de banda representa la capacidad máxima de transmisión de datos que un canal de comunicación puede transportar en un período de tiempo.

- Fiabilidad/disponibilidad: La fiabilidad se refiere a la probabilidad de éxito al transmitir X bytes dentro de un determinado retraso. Esto asegura que la comunicación entre los componentes del sistema sea consistente y sin interrupciones significativas, especialmente en aplicaciones críticas como la comunicación entre vehículos o con la infraestructura. La disponibilidad mide si el sistema está listo para su uso en un momento determinado.

- PLR (índice de pérdida de paquetes): el índice de pérdida de paquetes representa la relación entre el número de paquetes perdidos y el número total de paquetes enviados.

- El rango de comunicación: es la distancia máxima en la que la comunicación radio es efectiva entre dos sistemas.

- Tiempo de recuperación: Este indicador mide el tiempo máximo aceptable que una aplicación, computadora, red o sistema puede estar inactiva después de un desastre inesperado, una falla o un evento comparable.

En la arquitectura de prueba se han definido dos entornos diferenciados: en laboratorio y pruebas en campo, que se ejecutarán dependiendo del caso de uso y parámetro a medir. Se han detallado las herramientas de medida, simulación y de despliegue, incluyendo las redes 5G pública y privada, los dispositivos, las aplicaciones, vehículos, etc.

Respecto al diseño y desarrollo de los procedimientos de prueba para los casos de uso de este proyecto, se han definido las condiciones iniciales de las pruebas y las interfaces de medida. Se ha incluido una descripción de alto nivel de cada caso de uso, su clasificación, los beneficios y comportamiento esperado, los KPIs más relevantes de funcionalidad y conectividad y los elementos requeridos de la arquitectura de pruebas para la validación de los KPIs.

Finalmente se han desarrollado los planes y casos de prueba para cada caso de uso, donde para cada caso de prueba se han incluido al menos los siguientes campos: Identificador del caso de prueba, Objetivo de la prueba, Secuencia de la prueba, Estímulos necesarios, Captura de datos, Verificación del resultado

Desarrollo de soluciones tecnológicas necesarias basadas en 5G para el despliegue del vehículo conectado y validación de casos de uso (5GVEC)

Expediente: TSI-065100-2022-001

E17. METODOLOGÍAS DE PRUEBA Y ARQUITECTURA DE ENSAYOS

Parte 2: Ciberseguridad

Resumen ejecutivo

Consorcio: DEKRA, ERICSSON, TINAMICA, TUPL, SOFTCRITS, PREMO, TOPdigital

Financia: Gobierno de España, Vicepresidencia Primera del Gobierno, Ministerio de Asuntos Económicos y Transformación Digital

Cofinancia: Financiado por la Unión Europea NextGenerationEU, Plan de Recuperación, Transformación y Resiliencia

Tabla de contenido

1. INTRODUCCIÓN 2

2. OBJETIVOS PRINCIPALES 2

3. RESUMEN EJECUTIVO 2

4. PRINCIPALES CONCLUSIONES 3

1. INTRODUCCIÓN

El presente documento es un resumen ejecutivo correspondiente al entregable E17: Metodologías de prueba y arquitectura de ensayos, parte 2 - ciberseguridad, desarrollado en el marco del proyecto 5GVEC. Este entregable establece la base metodológica y técnica necesaria para la evaluación de la ciberseguridad en vehículos conectados, sirviendo como marco de referencia para la ejecución posterior de pruebas prácticas.

El documento define de forma estructurada las fases del proceso de evaluación, los criterios de aplicabilidad, la nomenclatura de los casos de uso y la arquitectura de ensayos, integrando herramientas y entornos de prueba asociados a los distintos subsistemas del vehículo. De este modo, el entregable proporciona una guía técnica completa y sistemática para abordar la validación de la seguridad en escenarios vehiculares complejos.

2. OBJETIVOS PRINCIPALES

Los objetivos principales del entregable E17, parte 2 – ciberseguridad, se centran en:

1. Definir una metodología de pruebas estructurada y reproducible para la evaluación de la ciberseguridad en vehículos conectados.
2. Establecer las fases del proceso de evaluación (descubrimiento, análisis y explotación), adaptadas al contexto específico del entorno vehicular.
3. Caracterizar los casos de uso de seguridad mediante criterios objetivos de aplicabilidad, tales como nivel de acceso, nivel de privilegio e interacción del usuario.
4. Proponer una arquitectura de ensayos que integre herramientas y entornos de prueba asociados a hardware, comunicaciones, software y servidores backend.

3. RESUMEN EJECUTIVO

El entregable E17 presenta una metodología integral para la evaluación de la ciberseguridad en vehículos conectados, alineada con los requisitos y recomendaciones de estándares internacionales. La metodología se estructura en tres fases principales: descubrimiento y recogida de información, análisis y explotación, que se aplican de forma transversal a los distintos subsistemas del vehículo: hardware, comunicaciones intravehículo, comunicaciones exteriores, software y servidores backend.

El documento detalla las técnicas y procedimientos asociados a cada fase, incorporando escenarios de ataque representativos y una categorización de requisitos de aplicabilidad que permite adaptar la metodología a diferentes contextos de evaluación. Asimismo, se define una nomenclatura jerárquica para los casos de uso que mejora la identificación de estos, facilita la trazabilidad y permite la ampliación sistemática de nuevos escenarios.

Como complemento a la metodología, el entregable reúne una arquitectura de ensayos basada en un amplio conjunto de herramientas técnicas, organizadas por subsistema y fase metodológica. Estas herramientas abarcan desde la recogida de información y el análisis pasivo,

hasta la explotación controlada de vulnerabilidades, proporcionando una base sólida para la implementación práctica de los procesos de evaluación definidos.

4. PRINCIPALES CONCLUSIONES

El entregable E17 pone de manifiesto la necesidad de contar con una metodología estructurada y específica para el entorno vehicular, capaz de abordar de forma coherente la complejidad y diversidad de los sistemas que conforman un vehículo conectado.

La definición clara de fases, criterios de aplicabilidad y casos de uso permite sistematizar el proceso de evaluación de la ciberseguridad, reduciendo la dependencia de enfoques ad-hoc y mejorando la reproducibilidad de los resultados. Asimismo, la arquitectura de ensayos propuesta demuestra la importancia de combinar herramientas de distinta naturaleza para cubrir de forma integral las superficies de ataque del vehículo.

En conjunto, este entregable establece una base metodológica sólida sobre la que se apoyará la ejecución y validación práctica de las pruebas de seguridad en entregables posteriores, contribuyendo a una evaluación más consistente, trazable y alineada con procesos de certificación y cumplimiento normativo en el ámbito del vehículo conectado.

Desarrollo de soluciones tecnológicas necesarias basadas en 5G para el despliegue del vehículo conectado y validación de casos de uso (5GVEC)

Expediente: TSI-065100-2022-001

RESUMEN EJECUTIVO

E18. PLANES DE PRUEBA Y EJECUCIÓN

Parte 1: Conectividad

Consorcio:

Financia:

Cofinancia:

Tabla de contenido

1. INTRODUCCIÓN 2

2. OBJETIVOS PRINCIPALES 2

3. RESUMEN EJECUTIVO 2

4. PRINCIPALES CONCLUSIONES 4

1. INTRODUCCIÓN

Este entregable recoge los resultados de la Tarea 4 de la A5 del proyecto 5GVEC. La tarea consiste en la definición, ejecución y conclusiones de los casos de uso implementados en el proyecto. Se incluyen las herramientas empleadas, las métricas obtenidas, así como las recomendaciones de mejora, conclusiones y lecciones aprendidas tras la validación de los prototipos implementados.

Se corresponde con los planes de prueba y ejecución del proyecto. Incluye:

- Los planes de prueba aplicados a los prototipos.
- Los resultados de ejecución obtenidos.
- Las recomendaciones de mejora, conclusiones sobre logros y lecciones aprendidas.

Los casos de uso a validar fueron presentados en los entregables anteriores y corresponden con:

- Advertencia de peligro en la vía (LHW)
- Protección de usuarios vulnerables (VRU)
- Intersección Inteligente (SIN)
- Aparcamiento autónomo (AVP)
- Detección de trayectoria con AI (CAI)
- Ejecución y detección de trayectorias predefinidas (TRAY)

2. OBJETIVOS PRINCIPALES

El objetivo principal de definir y ejecutar los planes de prueba aplicables a los casos de uso de conducción conectada y es plasmar las recomendaciones de mejora para los resultados y prototipos desarrollados en el proyecto, conclusiones sobre los logros alcanzados y lecciones aprendidas durante la ejecución del mismo. Así mismo, se incluirán también los diferentes planes de pruebas y ejecución desarrollados a lo largo del proyecto

3. RESUMEN EJECUTIVO

Como conclusión final cabe destacar que las comunicaciones vehiculares son una herramienta de gran utilidad para mejorar la seguridad vial. En este momento, tanto la tecnología, dispositivos y aplicaciones basadas en redes móviles 5G o las basadas en comunicaciones de corto alcance están disponibles y son plenamente efectivas permitiendo alertar a los conductores de peligros inminentes con la antelación necesaria para garantizar una reacción segura ante la situación de riesgo.

Durante las pruebas realizadas se ha investigado sobre que tecnología es más recomendable según el uso:

- V2N aporta cobertura y escalabilidad, pero con latencia variable y en algunos casos genera falso positivos o demasiadas advertencias que pueden distraer al conductor.
- V2I/V2V aportan inmediatez y fiabilidad, especialmente para eventos cortos o críticos.

Además de los casos de uso centrados en la seguridad vial como avisos de peligro, las comunicaciones V2N/V2I/V2V y el análisis comparativo de redes 5G públicas y privadas, el proyecto ha incorporado la validación de otros escenarios avanzados que amplían el alcance técnico de la movilidad conectada como son algunas funciones de conducción autónoma sobre red 5G, evaluadas mediante dos casos de uso adicionales:

- Ejecución de trayectorias autónomas en carretera donde se evaluó la capacidad del vehículo para seguir rutas predefinidas de forma completamente autónoma, integrando sistemas de percepción, planificación y control. Las pruebas se llevaron a cabo en una pista de conducción autónoma, cubriendo varios escenarios y condiciones de operación. Las mediciones recogidas permitieron analizar la precisión en el seguimiento de trayectorias, la estabilidad del comportamiento y los requerimientos de comunicación.
- Aparcamiento automatizado (Automated Valet Parking) donde se verificó el funcionamiento de maniobras de estacionamiento completamente automatizadas, donde el vehículo interactúa con la infraestructura y la red para completar el proceso sin intervención del conductor. Se midieron aspectos como fiabilidad, tiempos de ejecución, precisión y dependencia de la conectividad en las distintas fases del aparcamiento.

Estas validaciones complementan y amplían los resultados obtenidos en otros casos de uso del proyecto, permitiendo extraer las siguientes conclusiones adicionales:

- Las capacidades de la red 5G resultan adecuadas para soportar funciones avanzadas que van desde la transmisión de eventos críticos (VRU, colisiones, peligros locales) hasta maniobras autónomas complejas.
- Se ha desarrollado y aplicado una metodología de validación común que integra herramientas de medición, especificaciones de test, captura de métricas y análisis comparativo entre diferentes enfoques de conectividad.
- El proyecto ha permitido avanzar en la definición de procedimientos, protocolos y herramientas de ensayo orientados a tecnologías de conducción conectada y autónoma, alineados con estándares europeos y regulaciones en evolución.
- Se ha definido además una línea base para la evaluación de seguridad en redes 5G privadas, especialmente relevante para entornos donde se combinan aplicaciones de movilidad, automatización vehicular e infraestructura inteligente.

4. PRINCIPALES CONCLUSIONES

Como conclusión final cabe destacar que las comunicaciones vehiculares son una herramienta de gran utilidad para mejorar la seguridad vial. En este momento, tanto la tecnología, dispositivos y aplicaciones basadas en redes móviles 5G o las basadas en comunicaciones de corto alcance están disponibles y son plenamente efectivas permitiendo alertar a los conductores de peligros inminentes con la antelación necesaria para garantizar una reacción segura ante la situación de riesgo.

.

Desarrollo de soluciones tecnológicas necesarias basadas en 5G para el despliegue del vehículo conectado y validación de casos de uso (5GVEC)

Expediente: TSI-065100-2022-001

E18. PLANES DE PRUEBA Y EJECUCIÓN

Parte 2: Ciberseguridad

Resumen ejecutivo

Consorcio:

Financia:

Cofinancia:

Tabla de contenido

1. INTRODUCCIÓN 3

2. OBJETIVOS PRINCIPALES 3

3. RESUMEN EJECUTIVO 3

4. PRINCIPALES CONCLUSIONES 4

1. INTRODUCCIÓN

El presente documento es un resumen ejecutivo correspondiente al entregable E18: Planes de prueba y ejecución, parte 2 - ciberseguridad, desarrollado en el marco del proyecto 5GVEC. Este entregable recoge la ejecución práctica de los planes de prueba definidos en los entregables previos y su aplicación en la validación de la ciberseguridad en sistemas de vehículo conectado.

El documento se centra en la descripción de las herramientas desarrolladas e integradas durante el proyecto, así como en la definición de los entornos de prueba y el análisis de los resultados obtenidos tras su aplicación sobre ECUs (Electronic Control Unit) comerciales y sistemas reales. De este modo, el entregable proporciona una visión aplicada y verificable de los mecanismos de evaluación de la ciberseguridad, complementando las tareas previas de análisis normativo, selección de casos de uso y definición metodológica.

2. OBJETIVOS PRINCIPALES

Los objetivos principales del entregable E18, parte 2 – ciberseguridad, se centran en:

1. Definir y ejecutar planes de prueba concretos para la validación de la ciberseguridad en los distintos subsistemas del vehículo conectado.
2. Desarrollar, integrar y validar herramientas específicas de ensayo orientadas a la identificación de vulnerabilidades reales en hardware, comunicaciones, software e infraestructuras backend.
3. Verificar el funcionamiento efectivo de las herramientas desarrolladas mediante su aplicación sobre ECUs comerciales y vehículos reales.
4. Analizar los resultados obtenidos en las pruebas realizadas.
5. Garantizar la trazabilidad entre casos de uso, herramientas de prueba y evidencias generadas, facilitando su aplicación en procesos de evaluación, auditoría y certificación.

3. RESUMEN EJECUTIVO

El entregable E18 recoge la ejecución y validación de los planes de prueba definidos para evaluar la ciberseguridad del vehículo conectado, con especial énfasis en la aplicación práctica de las herramientas desarrolladas durante el proyecto. Estas herramientas han sido diseñadas para evaluar la seguridad de los distintos subsistemas del vehículo: hardware, comunicaciones intravehículo, comunicaciones exteriores, software y servidores backend.

A lo largo del documento se describen las diferentes herramientas desarrolladas, los entornos de prueba usados para la validación, así como los resultados obtenidos tras la realización de las pruebas sobre ECUs comerciales y sistemas reales. Las pruebas realizadas permiten identificar vulnerabilidades en ámbitos clave como los buses CAN, los sistemas de infotainment, las redes Wi-Fi internas, sistemas de posicionamiento GNSS (Global Navigation Satellite System), librerías de terceros usadas durante el desarrollo del firmware, los mecanismos de autenticación y los sistemas de acceso remoto al vehículo.

El análisis de los resultados pone de manifiesto la eficacia de las herramientas desarrolladas para detectar configuraciones inseguras, debilidades criptográficas y escenarios de ataque realistas. De este modo, el entregable E18 consolida un marco práctico de validación que conecta directamente los objetivos de evaluación con los mecanismos de verificación y los hallazgos obtenidos durante los ensayos.

4. PRINCIPALES CONCLUSIONES

Las pruebas realizadas en el marco del entregable E18 demuestran que la aplicación sistemática de herramientas específicas de ciberseguridad permite identificar vulnerabilidades relevantes en los distintos subsistemas del vehículo conectado, muchas de ellas con impacto directo sobre la seguridad, la privacidad y la integridad de los sistemas.

Los resultados obtenidos evidencian que debilidades en configuraciones, mecanismos criptográficos, gestión de credenciales o comunicaciones pueden ser explotadas mediante escenarios de ataque realistas, especialmente cuando no se aplican medidas de protección adecuadas. Asimismo, se confirma la importancia de validar estos aspectos sobre sistemas reales, ya que permite evaluar no solo la existencia de vulnerabilidades, sino también su viabilidad práctica y sus posibles consecuencias.

En conjunto, el entregable pone de manifiesto la necesidad de integrar procesos de prueba y validación de ciberseguridad de forma continua, apoyándose en herramientas automatizadas y metodologías estructuradas, como base para mejorar la robustez de los sistemas vehiculares y facilitar su evaluación en contextos de certificación y cumplimiento normativo.