La ciberseguridad aplicada a la automoción

Ana I. Ayerbe | Directora del Área de Negocio TRUSTECH de Tecnalia | @AnaAyerbe

Tema

Gran parte de nuestra economía depende de la movilidad y esta, de que se incluyan la ciberseguridad y la privacidad en el diseño de los vehículos y el de las infraestructuras.

Resumen

En los últimos años se ha producido una auténtica revolución en la industria de la automoción, en la que los vehículos han pasado de máquinas puramente mecánicas a auténticos ordenadores sobre ruedas. Los vehículos cuentan con sensores avanzados, gran capacidad de computación y miles de líneas de código para facilitar su conectividad y autonomía, pero precisan contar con sistemas fiables y robustos no sólo contra los riesgos de seguridad funcional, sino también contra las amenazas de ciberseguridad. Para competir en la era de la digitalización, el sector de la automoción debe concebir desde el diseño la ciberseguridad de los vehículos, de sus puntos de recarga, de las infraestructuras por las que transitarán y de la cadena de suministro.

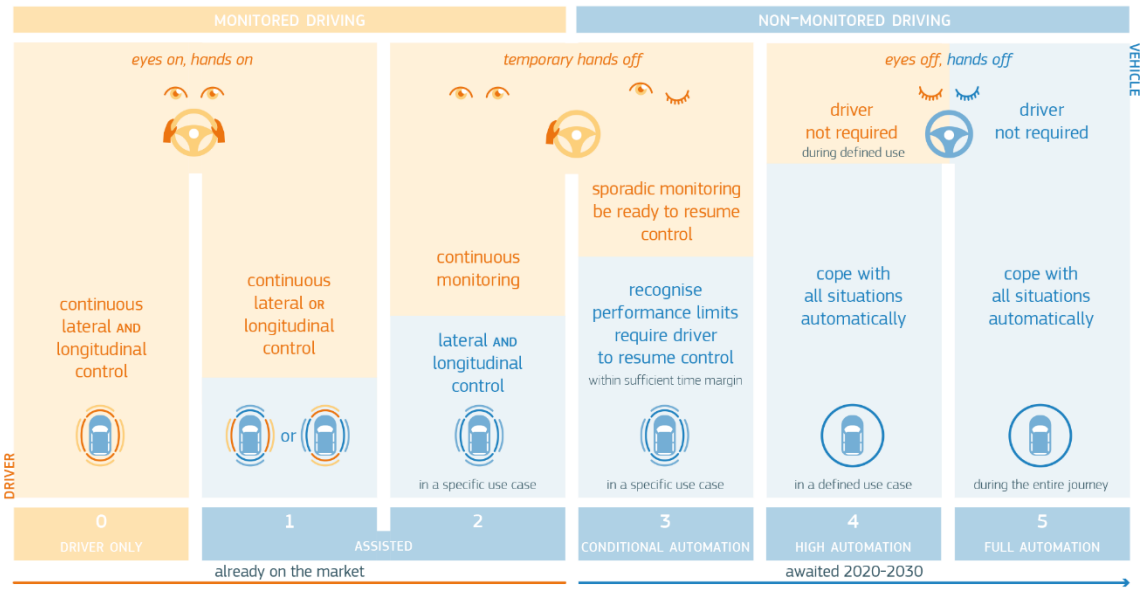
Análisis

Vivimos en un mundo globalizado que se fundamenta en una economía basada en la movilidad. No podemos imaginarnos nuestra economía y sociedad sin la movilidad sostenible de personas y mercancías de un lugar a otro utilizando diferentes tipos de vehículos y diferentes medios de transporte.

Actualmente todos los vehículos están ya conectados de una forma u otra. No tenemos más que pensar en la llamada de emergencia eCall, que se activa en caso de accidente; la geolocalización de los vehículos que disponen de GPS, o la capacidad de comunicación, por mencionar sólo algunos ejemplos. Esta conectividad será cada vez mayor en un futuro cuando se conecte con otros vehículos o con la infraestructura de transporte. Pero también podemos hablar de vehículos en los que algunas de las funciones de conducción se realizan de forma automática y de los vehículos totalmente autónomos que vendrían después.

Los vehículos que asisten al conductor (*Advanced Driving Assistance Systems*, ADAS) ya están disponibles en el mercado de la UE (niveles 1 y 2) y los vehículos autónomos que pueden conducir en un número limitado de situaciones de conducción (niveles 3 y 4) ya están probándose en situaciones reales, así como las pruebas del nivel 5, tal y como anuncian WAYMO, previamente conocido como el proyecto de Google de autoconducción, o Tesla, que va más allá hablando de las pruebas de flotas de vehículos sin conductor.

Figura 1. Niveles del SAE J3016 de conducción automatizada para vehículos de carretera.



Fuente: "The Future of Road Transport"[1], p. 21.

Tal y como señalaba Erik Jonnaert, secretario general de la Asociación de Fabricantes Europeos del Automóvil (ACEA), el mundo digital ofrece oportunidades sin precedentes y, sin embargo, las oportunidades llegan con riesgo, y uno de estos riesgos es la amenaza de un ciberataque directo a un vehículo o a una flota de vehículos. Por este motivo, es de crucial importancia considerar los riesgos de ciberseguridad en los vehículos conectados.

¿Cuál es la superficie de ciberataque de un vehículo?

Los vehículos presentan vulnerabilidades que se pueden explotar mediante ciberataques, como las descritas en el informe publicado por BMW en 2018[2] que afectaban a las unidades principales de sus vehículos, especialmente a la unidad de control telemático y al módulo de pasarela central. Las arquitecturas de los vehículos suelen organizarse por dominios interconectados mediante una puerta de enlace central. Los dominios más comunes son los de control de info-entretenimiento, control de la carrocería, sistemas de diagnóstico y mantenimiento, control de comunicaciones, control del tren motriz y control del chasis. Con el objetivo de minimizar riesgos, todos los componentes que pertenecen a un determinado dominio deben estar adecuadamente protegidos.

Aunque la arquitectura, sus subredes y los diferentes protocolos pueden variar de un vehículo a otro, la red de área del controlador (red de área de campus o red CAN) es normalmente el tipo de protocolo utilizado para el dominio del tren motriz. Dado que la

[1] "The Future of Road Transport. Implications of automated, connected, low-carbon and shared mobility", Joint Research Centre, Comisión Europea, abril de 2019.

[2] Keen Security Labs, "Experimental Security Assessment of BMW cars: A Summary Report", 2018.

red CAN se caracteriza por ser particularmente vulnerable, se generan muchos riesgos debido a su falta de seguridad, aunque únicamente parece atacable si previamente existe un acceso físico, y es aquí donde debemos pensar en las amenazas internas provenientes de los talleres que realizan el mantenimiento de los vehículos o los lugares donde se realicen sus recargas.

En el caso de la unidad de control telemático, conectada directamente a una puerta de enlace, esto conlleva que las vulnerabilidades en esta unidad de control puedan ser explotadas por un atacante a través de varias interfaces del vehículo con el exterior (sistemas de diagnóstico a bordo, memoria USB o la red celular), lo que podría proporcionar acceso a toda la red del vehículo, pudiendo manipular funciones tan críticas como la dirección o el freno.

Puede decirse que, a medida que el conductor va perdiendo importancia en la conducción del vehículo, la complejidad del diseño y de las pruebas que realizar sobre el mismo aumentan. Este tipo de vehículos exigen un alto grado de fiabilidad y robustez, ya que ciertas funciones, como la dirección o el freno, no pueden simplemente desactivarse ante fallos o ataques, sino que deben mantenerse activas para no perder el control del vehículo. Por lo tanto, a medida que se avanza en los niveles de conducción, aumenta la potencial superficie de ataque de los vehículos y de las infraestructuras al encontrarnos con sistemas de sistemas interactuando entre sí. Las posibles vulnerabilidades de estos sistemas deben evaluarse durante su diseño, desarrollo, pruebas, mantenimiento y fin de vida útil para evitar situaciones que puedan llegar a ser peligrosas.

En la resolución de estas y otras vulnerabilidades están trabajando activamente los fabricantes del sector de la automoción, complementando la seguridad funcional con la ciberseguridad, ayudados por buenas prácticas y normas en proceso de definición en algunos casos. En este sentido, la práctica recomendada SAE J3061 intenta minimizar el riesgo producido por posibles ciberataques y debe señalarse que ya está camino de convertirse en una norma bajo el nombre de " Road Vehicles Cybersecurity Engineering" (ISO/SAE CD 21434) actualmente en proceso de definición.

Motivos para un ciberataque

Cuando se habla de ciberseguridad en la automoción, una de las mayores preocupaciones suele ser que un *hacker* explote vulnerabilidades en los sistemas electrónicos del vehículo para generar incidentes e incluso asumir su control, lo que podría afectar a la seguridad de sus ocupantes, a otros vehículos en la carretera o a la propia infraestructura del transporte en caso de colisión. Realmente, es un escenario posible, pero podríamos decir que poco probable, a no ser que nos encontremos con un acto de ciberterrorismo. Mucho más probable es pensar en ataques asociados al cibercrimen. En realidad, el ciberterrorismo y el cibercrimen son dos de las amenazas que se ciernen sobre el sector de la automoción y, sobre todo en el caso del cibercrimen, pueden llegar a afectar a un gran número de usuarios en la medida en la que los cibercriminales vean medios de extorsionar a los conductores explotando vulnerabilidades de los vehículos para lograr beneficios económicos. Por ejemplo, acceder a los datos en tiempo real de un vehículo como su localización, navegación,

información de sus alrededores e incluso información de su conductor y pasajeros sería de valor para los cibercriminales, que si ven una oportunidad en su explotación lo harán.

Desde el punto de vista de la privacidad, no debemos olvidar que los vehículos pueden acabar procesando una gran cantidad de datos personales, desde la mera localización y la identificación del que llama a información sobre el estado de fatiga del conductor, estilo de conducción o información de la tarjeta de crédito. Para cumplir con el Reglamento General de Protección de Datos, los controladores de los datos personales deben implementar medidas técnicas y organizativas apropiadas para evitar que esos datos sean expuestos. Si por la existencia de vulnerabilidades de los sistemas o por fallos de privacidad esos datos caen en manos de cibercriminales, tienen un valor, ya sea por la propia venta de los datos, para perpetrar otro tipo de actos criminales en el mundo físico o para realizar un *ransomware* de alguna de las funcionalidades del vehículo y que no podamos utilizar esa funcionalidad mientras no paguemos un rescate.

Iniciativas en marcha para la seguridad del vehículo autónomo

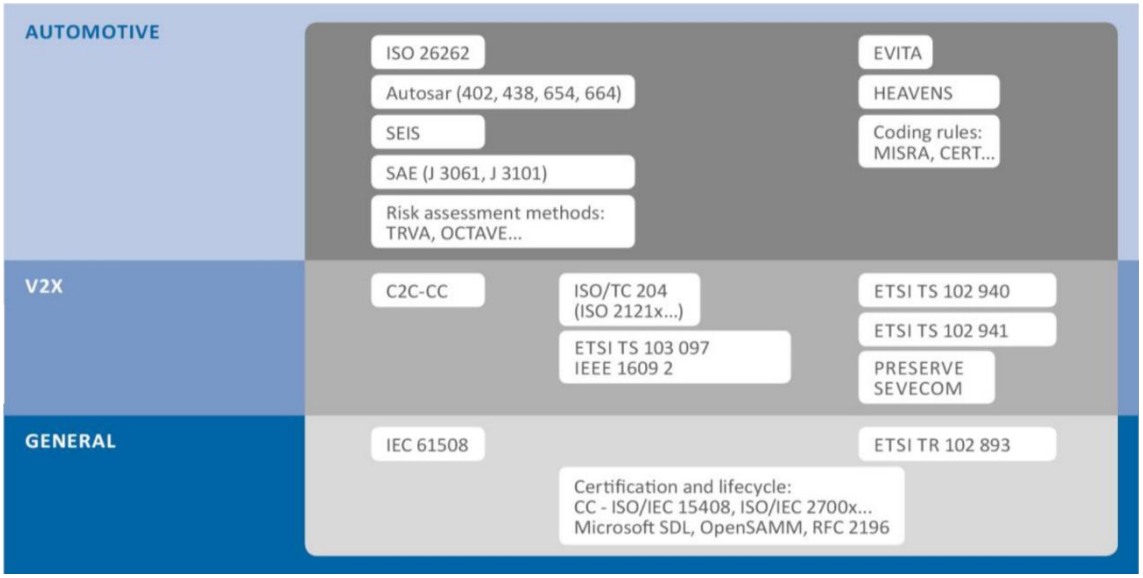
La Agencia Europea de Seguridad de las Redes y la Información (ENISA) ha identificado los retos de ciberseguridad, así como realizado un repaso a las diferentes iniciativas en marcha para acabar sugiriendo una serie de recomendaciones en forma de buenas prácticas para la ciberseguridad y resiliencia de los vehículos inteligentes. Estas pasan por la protección holística de todos los sistemas involucrados, incluyendo el proceso posventa del vehículo, incidiendo en la idea de disponer de vehículos seguros hoy para poder disponer en el futuro de vehículos autónomos seguros.

Figura 2. Buenas prácticas para la ciberseguridad y resiliencia de los vehículos inteligentes

Fuente: "Cyber Security and Resilience of smart cars"[3], p. 51.

[3] ENISA, "Cyber Security and Resilience of smart cars", diciembre de 2016.

Figura 3. Iniciativas de seguridad y ciberseguridad



Fuente: "Cyber Security and Resilience of smart cars", p. 47.

Aunque guías como la de ENISA, mencionada anteriormente, o los Principios de Ciberseguridad en la Automación de la Asociación Europea de Fabricantes de Automóviles (ACEA) [4], proporcionan una base nada desdeñable, es necesario desarrollar una estrategia propia de ciberseguridad en los fabricantes de vehículos conectados y autónomos para asegurar una conducción segura.

En la UE, el camino para el desarrollo de tecnología de conducción automatizada se inició con la Declaración de Ámsterdam sobre la cooperación en el campo de la conducción conectada y autónoma"[5], en la que los ministros responsables plantearon la necesidad de establecer modelos de confianza y políticas de certificación para evitar riesgos y apoyar la ciberseguridad al mismo tiempo que asegurar el despliegue de una tecnología conectada e interoperable. Este esfuerzo ha continuado identificando las siguientes acciones para el desarrollo y despliegue de vehículos conectados y automatizados:

- Definición de una metodología basada en riesgos para identificar y priorizar los principales riesgos de los vehículos conectados y automatizados.

- Privacidad y seguridad desde el diseño de los vehículos conectados y automatizados.

- Establecer una estructura de gobernanza para la definición, puesta en marcha y refuerzo de los procesos a nivel europeo.

[4] "ACEA Principles of Automobile Cybersecurity", septiembre 2017, https://www.acea.be/uploads/publications/ACEA_Principles_of_Automobile_Cybersecurity.pdf

[5] Comisión Europea, "Cooperation in the field of connected and automated driving", 14 de abril de 2016, https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_17_3272.

- Promover un esfuerzo internacional coordinado para apoyar aproximaciones armonizadas a nivel mundial.

Todo esto ha quedado complementado por el Reglamento Delegado de marzo de 2019 que establece los requisitos mínimos legales para una interoperabilidad segura entre estaciones sistemas de transporte inteligentes cooperativos (STI-C) —vehículos y carreteras—, que les permita intercambiar mensajes de forma segura dentro de una red STI-C abierta y de confianza bajo la Directiva 2010/40/EU[6].

Por otro lado, el Reino Unido aprobó en julio de 2018 la Ley sobre Vehículos Eléctricos y Autónomos (Automated and Electric Vehicles Act) que fija las responsabilidades cuando un vehículo funciona en modo automático. Entre ellas, cabe mencionar que considera imputable no instalar actualizaciones en un vehículo autónomo. En el caso de Estados Unidos, está en discusión la ley sobre "The American Vision for Safer Transportation through Advancement of Revolutionary Technologies" (AV START Act), para que los fabricantes de vehículos autónomos desarrollen y ejecuten un plan para reducir las cibervulnerabilidades. También la ley sobre "Safely Ensuring Lives Future Deployment and Research in Vehicle Evolution Act" (Self Drive Act), que exigiría que los fabricantes de vehículos autónomos desarrollen planes de ciberseguridad antes de que se les permita vender los vehículos.

¿Nos preocupa a los consumidores la ciberseguridad de nuestros vehículos?

Hoy por hoy, no parece que exista una demanda real por parte de los consumidores de conocer el estado de ciberseguridad de sus vehículos, aunque esto irá cambiando poco a poco a medida que tomen conciencia de los riesgos, como ha ido sucediendo en otros ámbitos, como en el de los ordenadores o los móviles. De todas formas, empiezan a aparecer algunas iniciativas que se preocupan por la protección de los consumidores frente a amenazas de ciberseguridad, como es el caso de Estados Unidos con su reciente propuesta —en discusión— sobre "Security and Privacy in Your Car Act of 2019" (SPY Car Act de 2019). Presentada en el Senado de Estados Unidos el 18 de julio de 2019, la propuesta plantea una serie de medidas para proteger a los consumidores frente a amenazas de seguridad y privacidad de sus vehículos en aspectos relacionados con:

- Protección contra ciberataques. Todos los puntos de entrada a sistemas electrónicos de cada vehículo puesto a la venta en Estados Unidos tendrían que estar equipados con medidas razonables que lo protejan contra ciberataques, incluidas medidas de aislamiento para separar los sistemas críticos de *software* de los sistemas no críticos y la necesidad de evaluarlo frente a vulnerabilidades de ciberseguridad incluyendo la aplicación de pruebas de penetración.

- Seguridad de la información recogida. Asegurar los datos recogidos por los sistemas electrónicos del vehículo para evitar accesos no autorizados mientras los datos están almacenados en el vehículo, mientras se transfieren desde el

[6] Reglamento Delegado C(2019) 1789 de 13 de marzo que complementa la Directiva STI 2010/40 de 7 de julio sobre la implantación de sistemas de transporte.

vehículo a otro lugar y en cualquier almacenamiento o utilización de los datos fuera del vehículo. Si un propietario o persona que haya alquilado el vehículo opta por que no se recojan y guarden datos de su conducción, debería seguir teniendo acceso, en la medida en la que sea técnicamente posible, a herramientas de navegación u otras funcionalidades, salvo excepciones contempladas.

- Detección, informe y respuesta a ciberataques. Cualquier vehículo fabricado para su venta en los Estados Unidos que presente puntos de entrada tendría que estar equipado con capacidades para detectar, informar y responder inmediatamente a cualquier intento de interceptar los datos de conducción y control del vehículo.

- Panel de ciberseguridad. Obligatoriamente incorporado en cada vehículo, debería informar a los consumidores a través de un gráfico estándar y fácil de entender del nivel en el que se protege la ciberseguridad y privacidad de los propietarios del vehículo, personas que puedan alquilarlo, conductores y pasajeros.

La ley va más allá y plantea la necesidad de disponer de herramientas de ciberseguridad y de un coordinador de ciberseguridad específico para el sector de la automoción que ayude a las autoridades de transporte a identificar, detectar, proteger, responder y recuperarse ante ciberincidentes, mejorando la ciberseguridad de esta infraestructura crítica. Todas estas propuestas obligan a seguir de cerca la evolución de la SPY Car Act de 2019 para ver si es aprobada por el Senado y pasa a las siguientes fases.

A nivel español, existen iniciativas pioneras, como la de la empresa Eurocybcar, que promueve la realización de una serie de pruebas para medir la ciberseguridad de un determinado vehículo.

La ciberseguridad como reto para las empresas del sector. Necesidad de talento

La introducción de la ciberseguridad plantea retos en diferentes ámbitos y para diferentes actores de la cadena de suministro: fabricantes, proveedores, concesionarios y talleres posventa, fabricantes y gestores de puntos de recarga, propietarios de infraestructuras de transporte, transportistas y conductores, entre otros.

Centrándonos en los fabricantes, ya sólo las pruebas de seguridad tienen desafíos únicos en comparación con las pruebas tradicionales. Por ejemplo, las pruebas de seguridad difieren de una manera crucial de aquellas con las que los ingenieros están familiarizados. Mientras que las pruebas relacionadas con la seguridad buscan fallos que ocurren en operaciones y cargas típicas, ahora pueden ocurrir debido a un ataque de un adversario malicioso. Por lo tanto, la naturaleza de este descubrimiento de vulnerabilidad no es determinista ni está programada, sino que es exploratoria y exige que el probador de seguridad piense “fuera de la caja”. Estos complejos sistemas bajo análisis requieren pruebas automatizadas a gran escala, lo que permite descubrir

sucesos raros que ocurren solo en circunstancias extrañas, por lo que las pruebas de penetración se presentan como elementos necesarios. Además, la reproducción de los resultados de la vulnerabilidad de seguridad meses o años después de su notificación también es problemática. Durante ese tiempo, podrían haber cambiado algunos parámetros, como el entorno o el *software* del sistema que debería actualizarse.

Si hablamos de desarrollar ciberseguridad y privacidad desde el diseño, los ingenieros de desarrollo deben saber cómo gestionar requisitos de ciberseguridad relacionados con las diferentes comunicaciones que pueden tener lugar y con el intercambio y compartición de datos. Necesitan disponer de metodologías, estándares y regulaciones claros para el ciclo de vida del desarrollo que estén llevando a cabo (requisitos, diseño, pruebas, validación, verificación y mantenimiento posterior), así como poder realizar una gestión segura de la cadena de suministro exigiendo ciberseguridad a los dispositivos internos y productos de terceros que puedan utilizarse en un momento dado.

Una vez vendido el vehículo, debemos poder tratar con problemas de seguridad cuando se produzcan, pudiendo realizar actualizaciones de *software* que resuelvan vulnerabilidades cuando sean necesarias y, en caso de ciberataques, disponer de mecanismos que permitan reconfigurar y deshabilitar aplicaciones para garantizar que las funciones importantes del vehículo siguen activas[7] y no suponen riesgos para los ocupantes del vehículo o del entorno.

Todo esto requiere una especialización en ciberseguridad en la industria de la automoción, que, al igual que otras industrias, sufre de una falta de ingenieros cualificados en ciberseguridad. Pero también carece de organizaciones sensibles hacia la ciberseguridad con procesos de seguridad bien definidos.

Conclusiones

Hablar de la ciberseguridad del sector de la automoción implica considerar la ciberseguridad y privacidad del vehículo desde su diseño, así como de todos los elementos con los que posteriormente interactuará, como los sistemas de recarga, las carreteras por las que circule o los sistemas de gestión del tráfico. Todo esto sin olvidarnos de la cadena de suministro del vehículo y de las responsabilidades subyacentes en caso de que algo falle algo falle.

Para integrar la ciberseguridad y privacidad desde el diseño, se debe fomentar una cultura de la ciberseguridad en las organizaciones, de forma que puedan definir y gestionar políticas de ciberseguridad, capacitar a las personas, adoptar ciclos de vida ciberseguros para el desarrollo de los vehículos y pensar en las respuestas ante posibles incidentes. La concienciación de los usuarios pasa por conocer el estado de ciberseguridad de sus vehículos y clarificar las responsabilidades en caso de fallos de ciberseguridad.

[7] EARPA Position Paper, “Cross-cutting activity Task Forces. The Role of Cybersecurity R&D in European Road Transport and ICT”, octubre de 2016.

El camino hacia los vehículos autónomos es imparable. Estaremos hablando de sistemas de sistemas interactivos entre sí y con las personas haciendo uso de múltiples tecnologías, como inteligencia artificial o *blockchain*. Por ello, es necesario que los diferentes avances tecnológicos en el sector de la automoción vayan de la mano de la ciberseguridad. No concibamos proyectos de I+D en el vehículo conectado sin que la ciberseguridad sea una parte importante de ello.