CIBERSEGURIDAD
en los vehículos

Por **Enrique Zapico Alonso**
RESPONSABLE DE MOBILITY LAB
ezapico@cesvimap.com

Los vehículos actuales cada vez se parecen más a un ordenador con ruedas. Y aunque esto lleva aparejado como ventaja la mayor ***conectividad*** *con el exterior y funciones avanzadas de automatización, también, una* ***exposición a los riesgos cibernéticos*** *de igual magnitud a un ordenador personal o un móvil. La diferencia fundamental es que puede poner en peligro la vida de los ocupantes del vehículo o de otros usuarios de la vía…*

El problema de la ciberseguridad de los vehículos es que alguien puede controlar, de forma remota, su dirección eléctrica, frenos o acelerador electrónico... Por eso se hizo necesario establecer alguna normativa que garantizase que los componentes electrónicos eran fiables. También que, en caso de fallo de algún componente, el vehículo continuase siendo seguro. La norma **ISO 26262** es el estándar internacional para la **seguridad funcional en la industria automóvil**. Se aplica a los sistemas eléctricos y electrónicos con componentes de hardware y software en vehículos. Define qué requisitos deben cumplir las funciones relevantes de segu-

ridad del sistema, así como los procesos, métodos y herramientas que se utilizan. No obstante, esta norma no contempla la ciberseguridad. Para cubrir este vacío, en 2016, **SAE** (*Society of Automotive Engineers*) publicó el documento **J3061** "Guía de ciberseguridad para sistemas ciber-físicos de vehículos". Esta práctica recomendada establece principios para la ciberseguridad en los sistemas electrónicos de los vehículos:

- Su ciclo de vida completo que se pueda adaptar y utilizar en los procesos para incorporar la ciberseguridad en los sistemas electrónicos de los vehículos desde la fase de concepto hasta la producción, operación, servicio y desmantelamiento;
- Información sobre las herramientas y métodos comunes existentes al diseñar, verificar y validar estos sistemas electrónicos;
- Principios rectores básicos sobre ciberseguridad para sistemas de vehículos;
- Bases para desarrollo de estándares futuros en ciberseguridad de vehículos.

Paralelamente, diversos organismos públicos y privados del mundo fueron publicando guías y recomendaciones sobre buenas prácticas en el diseño de los sistemas electrónicos de los vehículos para limitar las consecuencias de un ciberataque.

Ciberseguridad por ley

La Unión Europea conoce que la conectividad y la automatización de los vehículos aumentan la posibilidad de acceso remoto no autorizado a sus datos y de modificación ilegal de software por vía inalámbrica. Así, establece la aplicación obligatoria de los reglamentos de Naciones Unidas en ciberseguridad. El **Reglamento (UE) 2019/2144** establece como **requisito para la homologación de tipo** de vehículos de motor el cumplimiento de dichos reglamentos. Las fechas claves para su aplicación son:

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

Los reglamentos de Naciones Unidas son:

- **Reglamento nº 155** de la Comisión Económica para Europa (CEPE) de las Naciones Unidas — Disposiciones uniformes relativas a la homologación de los vehículos de motor en la ciberseguridad y su gestión.
- **Reglamento nº 156** de las Comisión Económica para Europa (CEPE) de las Naciones Unidas — Disposiciones uniformes relativas a la homologación de vehículos en lo que respecta a las actualizaciones de software y al sistema de gestión de actualizaciones de software.

Ambos han entrado en vigor este 22 de enero de 2021.

Reglamento UN 155

Este reglamento de homologación establece los requisitos que deben cumplir tanto el fabricante como los modelos concretos de vehículos sometidos a homologación de tipo.

En lo que respecta al fabricante, exige que disponga de un **sistema de gestión de la ciberseguridad** (**CSMS** - *Cyber Security Management System*), certificado por tercera parte (la autoridad de homologación o el servicio técnico designado por esta), que establezca procesos para:

- Identificar y gestionar riesgos de ciberseguridad en el diseño del vehículo;
- Verificar que se gestionan los riesgos;
- Asegurarse de que la evaluación de riesgos está actualizada;
- Monitorear los ataques cibernéticos;
- Evaluar si las medidas siguen siendo efectivas ante nuevas amenazas o vulnerabilidades;
- Responder a los ataques;
- Apoyar el análisis de ataques exitosos o intentados.

Verificado mediante auditoría que el fabricante dispone de un sistema eficaz de gestión de la ciberseguridad, la autoridad de homologación emitirá un certificado de conformidad del sistema de gestión de la ciberseguridad. Tendrá una validez máxima de 3 años y es el paso previo para que el fabricante pueda presentar un vehículo a la homologación de tipo en esta materia.

Respecto a la auditoría del sistema de gestión de la ciberseguridad, aunque el Reglamento UN 155 no obliga a realizarla conforme a ninguna norma concreta, indica como apropiada,

En enero entró en vigor el Reglamento nº 155 para la homologación de los vehículos en lo que respecta a la ciberseguridad

entre otras, la **ISO/SAE 21434:2021** -Vehículos de carretera – Ingeniería de ciberseguridad, publicada en agosto de 2021. Este documento especifica los requisitos de ingeniería para la gestión de riesgos de ciberseguridad respecto al concepto, desarrollo de productos, producción, operación, mantenimiento y desmantelamiento de sistemas eléctricos y electrónicos en vehículos de carretera, incluidos sus componentes e interfaces. El cumplimiento de sus requisitos por parte del fabricante aseguraría el cumplimiento del Reglamento UN 155.

Para evaluar la ciberseguridad de un vehículo, el fabricante deberá justificar que ha realizado un completo análisis de posibles amenazas y vulnerabilidades de ciberseguridad, implementando las medidas de mitigación oportunas. Esta evaluación por parte de la autoridad de homologación o del servicio técnico designado, en una primera fase, se hará mediante control documental.

¿Qué vulnerabilidades o amenazas han de tenerse en cuenta según el este Reglamento UN 155?

- Amenazas relativas a los **servidores back-end** en relación con vehículos sobre el terreno;
- Amenazas a vehículos por lo que respecta a sus **canales de comunicación**;
- Amenazas a vehículos con respecto a sus **procedimientos de actualización**;
- Amenazas a vehículos con respecto a acciones humanas involuntarias que faciliten un ciberataque;
- Amenazas a vehículos con respecto a su **conectividad externa** y sus conexiones externas;
- Amenazas a los datos o código del vehículo;
- Posibles vulnerabilidades que podrían explotarse si no se protegen o se refuerzan de forma suficiente.

En España, en 2021, la autoridad de homologación (Ministerio de Industria, Comercio y Turismo) ha designado como servicio técnico para los Reglamentos UN 155 y UN 156 a **IDIADA** AUTOMOTIVE TECHNOLOGY, S.A. Es, hasta la fecha, el único servicio técnico designado.

El análisis de amenazas y vulnerabilidades que realiza el fabricante del vehículo debe extenderse a lo largo de toda su cadena de suministro para constatar que se detectan y gestionan los riesgos relacionados con los proveedores.

El fabricante está obligado a notificar a la autoridad de homologación o servicio técnico, al menos anualmente, la información sobre nuevos ciberataques. También habrá de notificar y confirmar que las medidas de mitigación aplicadas a sus vehículos para esta materia siguen siendo eficaces, así como las adicionales adoptadas.

Reglamento UN 156

De manera simultánea al Reglamento UN 155 se ha publicado el Reglamento UN 156 - *Disposiciones uniformes relativas a la homologación*

de vehículos en lo que respecta a las actualizaciones de software y al sistema de gestión de actualizaciones de software.

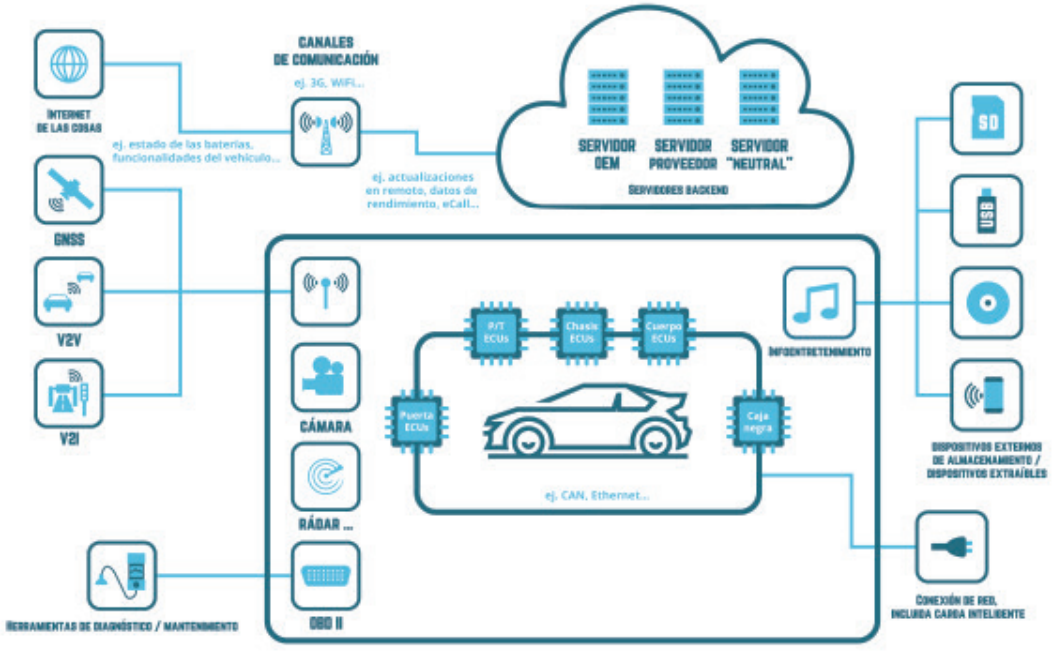
Dado que los vehículos actuales disponen de conectividad, muchas de las actualizaciones de software se realizan de forma remota (OTA – *Over The Air*). Este reglamento pretende asegurar que se hacen de manera efectiva y sin riesgos de fallos de funcionamiento posteriores ni durante la ejecución de la actualización. Exige, al igual que el UN 155, que el fabricante disponga de un **sistema de gestión para la actualización del software** (**SUMS** - *Software Update Management System*). No obstante, el reglamento aplica a todo tipo de actualizaciones del software, incluidas las efectuadas mediante cable u otra conexión local.

El sistema de gestión para la actualización del software debe establecer requisitos para:

- Control de la configuración (hardware/software);
- Datos de validación de integridad para el software;
- Identificación de software (*RX Software Identification Number – RXSWIN*);
- Verificación de que el software instalado es el debido;
- Identificación de interdependencias (relevante para actualizaciones de software);
- Identificación de vehículos objetivo y verificación de compatibilidad;
- Proceso para verificar si una actualización afecta una homologación de tipo;
- Proceso para evaluar si la actualización afecta a la seguridad y a la conducción segura;
- Informar al propietario de las actualizaciones;
- Documentación de todo lo anterior;
- Garantizar la ciberseguridad de la actualización de software antes del envío.

¿Qué **requisitos específicos de las actualizaciones OTA** debe cumplir el fabricante?

- El vehículo puede restaurar los sistemas a su versión anterior si una actualización falla o se interrumpe;
- Las actualizaciones de software solo puedan ejecutarse cuando el vehículo tenga energía suficiente para completar el proceso de actualización;
- Si una actualización puede afectar a la seguridad del vehículo, se asegurará de que se realiza de forma segura;
- Demostrará que puede informar al usuario del vehículo de una actualización antes de que se ejecute;
- Si la actualización no es segura durante la conducción, garantizará que el vehículo no pueda conducirse mientras se actualiza y que el conductor no pueda utilizar ninguna función del vehículo que



afecte a la seguridad del vehículo o a la ejecución satisfactoria de la actualización;
- Tras la actualización, informará al conductor del éxito (o fracaso) de la misma y si necesita acudir a un taller.

Consecuencias

La entrada en vigor y aplicación de esta nueva normativa en un plazo tan breve (año y medio para nuevas homologaciones y poco más de 3 años para nuevas matriculaciones) acarreará a los **fabricantes cambios drásticos** en su concepción de la electrónica de los vehículos. Hasta ahora, la ciberseguridad no había sido una de las prioridades de los constructores. Ahora, habrá de ser tenida en cuenta desde la concepción del producto hasta el final de su vida. Todos los fabricantes deben contar con ingenieros especializados en ciberseguridad o recurrir a consultoras especializadas que les gestionen estos procesos. También será una revolución respecto a la forma de evaluar la conformidad durante la homologación de tipo. Para estos reglamentos no existirán pruebas objetivas a las que someter a los vehículos. La evaluación se basará en comprobar que el fabricante ha realizado una correcta y completa evaluación de amenazas y vulnerabilidades, categorizándolas en función de su probabilidad y de los posibles efectos de los ataques e implementando medidas de mitigación.

¿Qué efectos puede tener un ataque?

a. Afecta al funcionamiento seguro del vehículo;
b. Interrumpe el funcionamiento de las funciones del vehículo;
c. Modifica el software y/o altera su rendimiento;
d. Altera el software, pero sin efectos en el funcionamiento;
e. Viola la integridad de los datos;
f. Viola la confidencialidad de los datos;
g. Pierde la disponibilidad de los datos;
h. Otros, incluida la delincuencia.

Además de la evaluación documental, el servicio técnico realizará test de ataque sobre algunas de las vulnerabilidades detectadas, para verificar la eficacia de las medidas de mitigación. Desde el punto de vista de los clientes y del mercado en general, cabe esperar que los vehículos que se homologuen conforme a estos nuevos reglamentos sean realmente más ciberseguros. No hay que olvidar que los que existen y se comercializan hoy día no cumplen ninguno de los requisitos -o, al menos, los fabricantes no pueden acreditarlo-. Es de prever que los robos de los vehículos mediante medios electrónico disminuyan, que no sea posible realizar modificaciones ilegales en su software ("dieselgate") y, lo más importante, que en caso de producirse alguno de estos ataques, el fabricante tiene la obligación de implementar una solución ("parche") durante toda la vida del vehículo ●

Para saber más:

› Reglamento (UE) 2019/2144
› Reglamento UN nº 155
› Reglamento UN nº 156
› ISO/SAE 21434:2021. Road vehicles — Cybersecurity engineering