NOTA TÉCNICA

CIBERSEGURIDAD EN AUTOMOCIÓN

Por Óscar Ciordia

secpho
collaborate to innovate

Tel.: 937 833 664 | E: elisenda.lara@secpho.org | www.secpho.o
C/ Milà i Fontanals, 14-26, 1º 6ª 08012 Barcelona (Spain)

UNA INDUSTRIA DE AUTOMOCIÓN CIBERSEGURA PARA EL SIGLO XXI

ÓSCAR CIORDIA | Presidente del subcomité nacional para los componentes electrónicos del automóvil de UNE

Un grupo de trabajo de las Naciones Unidas está a punto de finalizar un nuevo reglamento que representa un cambio de paradigma para la industria automotriz mundial. En el futuro cercano la homologación de tipo en los vehículos para la UE será solo posible con la acreditación de un sistema de gestión de la ciberseguridad o CSMS por sus siglas en inglés (Cybersecurity Management System) por parte de las compañías de la cadena de valor. Es por esto que la ciberseguridad debería estar sobre la mesa de los consejos en empresas del sector en todo el mundo y en particular de España como uno de los principales suministradores y montadores de la industria.

La ciberseguridad de los vehículos en las noticias

La **exposición a los riesgos de ciberseguridad que presentan los vehículos** lleva siendo noticia desde que en el año 2015 una conocida marca de vehículos de alta gama tuvo que llamara a revisión a 1.4 millones de unidades en lo que fue el primer caso relevante de ataque cibernético valorado en casi 600 millones de dólares en pérdidas para la compañía. Ya en el año 2018 una empresa china de seguridad informática reveló más de 14 vulnerabilidades en los vehículos de una marca europea.

Los **vehículos actuales pueden llegar a montar 150 unidades electrónicas de control.** La predicción es que entorno a el **año 2030 el número de líneas de código** que estará corriendo en las unidades electrónicas vehiculares puede rondar los **300 millones** de líneas. Solo a modo de comparación, los vehículos actuales constan de cerca de 100 millones de líneas de código, **un avión de pasajeros alrededor de 15 millones**, un avión de caza no llega a 25 millones y el sistema operativo de ordenadores personales más conocido unos 40 millones.

Las cifras anteriores revelan cómo existe una **amplia variedad de posibilidades que exponen a los vehículos actuales y futuros a ciberataques** no solo dirigidos contra el propio vehículo sino contra toda la cadena de valor. Por todo ello, la industria y los gobiernos llevan años trabajando en normas que permitan minimizar los riesgos que las nuevas arquitecturas y cadenas de valor puedan presentar frente a ciberataques.

Normas sobre ciberseguridad: UNE, ISO y SAE

El **foro mundial de las Naciones Unidas** que se encarga de armonizar las regulaciones sobre los vehículos, conocido como el **WP.29**, está a punto de finalizar un **nuevo reglamento que habrá de incluirse en la homologación de tipo en el futuro cercano**. El subgrupo encargado de elaborar la nueva reglamentación conocido por sus siglas **TF-CS/OTA** se ha basado en dos requerimientos básicos: La existencia y funcionamiento de un sistema de gestión de la ciberseguridad (CSMS) en las empresas fabricantes y suministradores y la aplicación de este sistema al tipo de vehículo en el momento de su aprobación. Como ya viene siendo habitual la UE adoptará el reglamento durante la primera mitad del 2022 lo cual deja escasos dos años para que el sector ponga en marcha las medidas necesarias.

En paralelo con la TF-CS/OTA, la industria automotriz está trabajando en la **norma ISO/SAE 21434** para la seguridad de los vehículos. De manera análoga al CSMS definido en el WP.29, la norma ISO/SAE se enfoca en especificar la organización y los procesos que durante todo el ciclo de vida de los vehículos garantizan su protección contra ciberataques. Ambas normas son complementarias, así, la regulación de las Naciones Unidas hace referencia constante a la futura norma ISO para la implementación del CSMS.

Compartiendo una terminología y métricas comunes, ambas **normas proporcionarán una base** sobre la cual toda la industria, fabricantes de vehículos y componentes, concesionarios y talleres, podrán construir interfaces, compartir responsabilidades y procesos seguros frente a posibles ciberamenazas. La **norma ISO ya ha sido publicada en la primera mitad del 2020 y está comenzando a ser exigida por los principales fabricantes mundiales de vehículos.**

ISMS y CSMS: Seguridad de la información vs. Ciberseguridad

Previo al concepto de CSMS la industria se adhería al **ISMS** o sistema de gestión de la seguridad de la información, por sus siglas en inglés (Information Security Management System), concepto definido en la serie de normas ISO/IEC 27000 de seguridad industrial. El ISMS describe cómo la seguridad de la información ha de definirse, implementarse, analizarse y mejorarse continuamente en una empresa tomando como base para ello el riesgo asociado.

Con el nuevo reglamento UNECE WP.29 y la norma ISO/SAE 21434, sin embargo, **el término ISMS se ve reemplazo en la industria automotriz por el CSMS,** o lo que es lo mismo, **el perímetro de seguridad se amplía desde el ámbito de la Información hasta el más global de Ciberseguridad.** El CSMS define lo que es un nivel mínimo aceptable de seguridad y operación de un producto y como lograrlo, certificarlo y mantenerlo mejorando continuamente.

Mientras que el ISMS incluye la protección de la información en la empresa y evita los posibles ataques contra ella (foco interno), **el CSMS tiene un foco hacia el exterior especialmente en lo referente a la detección y defensa frente a posibles ciberataques** que se puedan dirigir contra el producto y su entorno de operación. Este cambio requiere de la adaptación de muchos procesos debido especialmente a las implicaciones que estas amenazas presentan para la seguridad funcional o la protección frente al robo. **La nueva aproximación, centrada en el producto, implica también un cambio de perspectiva en la estrategia empresarial** puesto que en contraste con los factores de coste que refleja el ISMS, el CSMS se convierte en un componente adicional

de la misión de la compañía en el entorno estratégico del producto.

Estrategia de defensa frente a ciberataques

Las nuevas normas y reglamentos promueven una **estrategia de defensa frente a ciberataques basada en el uso de múltiples capas de seguridad**. De esta forma, si se sufre un ataque es posible reducir el impacto que puede tener sobre el vehículo o la cadena de valor, así como establecer contramedidas adecuadas.

El concepto militar de defensa en profundidad es un buen modelo para la nueva propuesta normativa, puesto que ésta incluye recomendaciones como son:

• **Interfaces seguros con el mundo exterior** como por ejemplo en actualizaciones de software inalámbricas, aplicaciones de ayuda al conductor, interfaz OBD o enlaces Bluetooth. Todos estos enlaces no son sino invitaciones explícitas a penetrar los sistemas vehiculares basándose en sus vulnerabilidades. Todos estos interfaces deben ser prioritarios en el análisis y diseño de la estrategia de defensa.
• **Arquitecturas de red intra-vehiculares con segregación física y aislamiento de unidades electrónicas** con implicaciones en la seguridad vehicular. Para esto es fundamental el uso de pasarelas, buses de comunicación y protocolos a distintos niveles OSI que sean seguros.
• Uso de **módulos de seguridad hardware** (HSM por su acrónimo en inglés) para proporcionar unos fundamentos sólidos para el software al que apoyan por ejemplo en arranques seguros, generación o almacenamiento de claves y protección activa de memoria en microcontroladores. Los HSM ayudan a la implementación de servicios de seguridad como son los entornos de ejecución confiable (TEE por su acrónimo en inglés) o la aceleración de computaciones criptográficas.

• **Aseguración de la cadena de valor,** especialmente larga y compleja en los nuevos vehículos conectados. Todos los actores de la cadena han de ser conscientes de los riesgos de ciberseguridad y de que estos han de minimizarse y gestionarse activamente mediante las correspondientes directrices y mejores prácticas.
• La **estrategia ha de ser extremo a extremo** mediante la protección de la cadena de confianza desde la arquitectura vehicular a los servidores y la nube.

Implicaciones para la industria automotriz

Dado los tiempos de desarrollo manejados en la industria automotriz, **los fabricantes y proveedores deben afrontar desde ya los nuevos requerimientos de ciberseguridad para lograr las aprobaciones de tipo de sus próximos productos**. Para ello deben adoptar una **aproximación basada en el riesgo identificado y lograr y mantenerlo a un nivel apropiado a lo largo de toda la línea homologada bajo el mismo tipo**, sus interfaces externos y subsistemas. Éste último aspecto incluye en particular la consideración de las dependencias e información proveniente de los proveedores de componentes, proveedores de servicios, así como de terceras partes, siempre desde una perspectiva de ciberseguridad.

Con la llegada de los **nuevos vehículos autónomos y conectados** la industria afronta una batalla dura y larga en la cual parte con desventaja. Teniendo en cuenta el **cambio continuo de las ciberamenazas** frente a los dilatados tiempos de vida de los vehículos, el CSMS tiene un foco prioritario en la fase una vez comenzada la producción del modelo, gestionando el riesgo durante la operación del vehículo. Por ello, es necesario la **adopción de medidas de seguridad orientadas a los procesos hasta ahora no presente en la industria automotriz**.
Aunque ya se tienen unos años de experiencia con los estándares de seguridad funcional a través de la norma ISO27000, el **principal reto en el diseño de un CSMS es tener en cuenta las especificidades propias de la industria**. A todo lo anterior hay que añadir la complejidad del producto y la cadena de valor, las interacciones con la seguridad funcional vehicular, el cumplimiento de las regulaciones medioambientales y la protección antirrobo.

Con el **nuevo reglamento de Naciones Unidas la ciberseguridad** cambiará de consideración y pasará de ser un ítem no obligatorio a ser un **prerrequisito para poder realizar negocios y ser competitivo en el mercado de fabricantes y proveedores del automóvil.** En el contexto de cambio continuo y acelerado de la era digital, no solo es necesario cumplir con la regulación sino hacerlo con la mayor efectividad en relación a la estrategia corporativa y sus planes de producto. En caso contrario la pérdida de competitividad de la industria se verá duramente afectada.

Por todo lo anterior, **las compañías han de implementar medidas organizativas holísticas a la vez que medidas técnicas que permitan definir permanentemente, controlar, gestionar y mejorar la ciberseguridad a todo lo largo de la cadena de valor y del ciclo de vida del producto.**
Ya existe un movimiento de la industria a través de sus compañías más competitivas y con mejor visión de futuro en esta dirección donde el análisis de riesgos, que determina el estado de implementación de un CSMS, es el primer paso del cual se deben derivar los planes de mejora.

Análisis de riesgos de ciberseguridad

Los puntos esenciales que componen el análisis de los riesgos de ciberseguridad recomendados por el nuevo reglamente y que, como mínimo ha de afrontar una organización y su producto son:

- **Identificación de los activos y de los daños potenciales** que resultarían de una brecha en las funcionalidades de seguridad
- **Identificación y análisis de las posibles amenazas**, ataques y vulnerabilidades
- **Determinación de niveles de riesgo basados en escenarios de daños** y en la probabilidad de ataques exitosos
- Establecer las **contramedidas** hasta que el riesgo remanente sea aceptable
- Documentación de los pasos relevantes y resultados del análisis de riesgo como son las listas de activos, escenarios de daños, informes de ataques e informes de riesgos.

El aspecto más debatido en las reglamentaciones de ciberseguridad es el relacionado con el análisis e identificación de las posibles amenazas puesto que al ser un tema fundamentalmente tecnológico está sujeto a una evolución continua. **Cualquier lista o flujograma que pretenda ayudar al proceso en este punto queda obsoleto inmediatamente a su publicación**. Sin embargo, el acuerdo final de los expertos ha sido establecer una **lista base de protecciones que marcan el mínimo** a partir del cual cada empresa ha de completar conforme a su experiencia y en colaboración con los otros eslabones de la cadena de valor. Las protecciones en el reglamento se han segmentado en dos áreas: **Protecciones intra-vehiculares y protecciones a los sistemas externos al vehículo** y de ellas se derivan las listas que contienen los escenarios a considerar.

El **análisis de riesgo** cuya estructura se ha esbozado no es sino el último escalón que ha de ser necesariamente **precedido de un planteamiento de la arquitectura eléctrica y electrónica del vehículo que permita minimizar las amenazas** y, en la medida de lo posible aislarlas si se produjeran evitando que afecten a la seguridad vehicular o integridad de sus ocupantes.

El CSMS, en la base de todo el sistema de ciberseguridad; es el **pilar que garantiza que los procesos de las empresas que diseñan y fabrican los componentes y vehículos finales lo hagan de una forma coherente** en relación a la garantía de ciberseguridad que exigen los usuarios y gobiernos.

Referencias bibliográficas

Task Force on Cyber Security and [OTA] software updates [CS/OTA). UNECE.
Recuperado de https://wiki.unece.org/pages/viewpage.action?pageId=40829521

Automotive cybersecurity. IEEE.
Recuperado de https://site.ieee.org/ocs-cssig/?page_id=736

SAE J3061TM "CYBERSECURITY GUIDEBOOK FOR CYBER-PHYSICAL VEHICLE SYSTEMS". SAE.
Recuperado de https://interact.gsa.gov/sites/default/files/J3061%20JP%20presentation.pdf

Conclusión

El cambio de paradigma en relación a la ciberseguridad que tendrá lugar cuando los nuevos reglamento y normas se publiquen **requerirán de fuertes inversiones en sistemas y capital humano altamente cualificado** en todas las empresas de la cadena de suministro del automóvil **desde los fabricantes de componentes hasta las fábricas de montaje y acabando en la comercialización y servicio de los vehículos a lo largo de su vida útil.**

La **competitividad futura de la industria mundial en general y española en particular dependerá grandemente de su capacidad para adaptarse a los nuevos requerimientos de ciberseguridad** en consonancia con las nuevas arquitecturas vehiculares y modelos de movilidad segura y autónoma.

España, con una fuerte industria de componentes y montaje de vehículos tiene una gran oportunidad tecnológica para poder hacer **uso del talento existente en las áreas de software y TIC** en un contexto nuevo como es el de la industria de automoción.

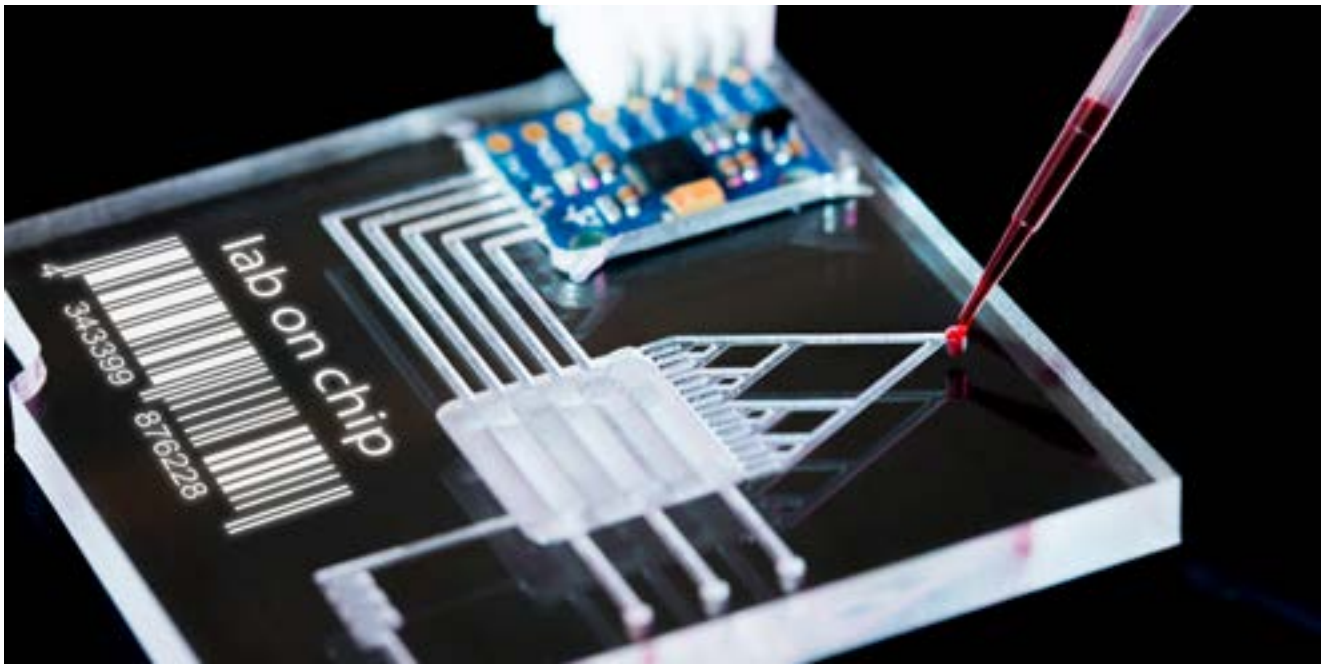
Como parte de esa adaptación, la **Asociación Española por la Normalización (UNE)** ha comenzado a apoyar al sector mediante la **creación de un nuevo grupo de trabajo en ciberseguridad** dentro del comité técnico de normalización del automóvil en su subcomité de aspectos eléctricos y electrónicos. El nuevo grupo, c**on miembros relevantes** en los aspectos de ciberseguridad del automóvil como son las empresas RENAULT, GMV, KDPOF o SEAT, los centros tecnológicos CTAG y APPLUS+ y los laboratorios de certificación IDIADA o DEKRA, participa en las reuniones de ISO en representación de España lo que garantiza una mejor y más rápida adopción de las normas a su entrada en vigor en nuestro país.

Cada vez más, aspectos informáticos de seguridad, electrónicos y telemáticos, ganarán relevancia dentro de los vehículos y con ello se abrirán oportunidades para los países y empresas dispuestos a afrontarlos, así como amenazas para aquellas que los desdeñen o decidan permanecer en sus ámbitos tradicionales de confort.

SOBRE EL AUTOR

ÓSCAR CIORDIA

Ingeniero de telecomunicaciones con Master en economía, Óscar Ciordia se ha especializado en el sector de la electrónica de consumo y la automoción. Compagina su cargo de Director de Desarrollo de Negocio y Marketing en KDPOF, que desarrolla microelectrónica de última generación para comunicaciones de alta velocidad a través de Fibra Óptica Plástica de gran núcleo (POF), con la docencia en la Universidad Rey Juan Carlos, donde forma parte del departamento de Teoría de la Señal y las Comunicaciones y Sistemas Telemáticos y Computación en calidad de profesor asociado.
Desde Junio de 2019 es presidente del subcomité técnico español para la normalización eléctrica y electrónica en automoción (CTN26/SC1)



¿Qué son las Deep Tech?

El término **Deep Tech**, que se traduciría como 'tecnologías profundas', se refiere a una nueva categoría de tecnologías transversales que están irrumpiendo de forma disruptiva en diversos ámbitos. Las principales **Deep Tech actualmente son: las tecnologías fotónicas, la inteligencia artificial, la biotecnología, el blockchain, los materiales avanzados, la computación cuántica, la robótica y la electrónica**

Son tecnologías generadas tras un descubrimiento científico y con un alto impacto en la sociedad. A diferencia de las "shallow tech" -como las apps o servicios de comercio electrónico-, las Deep Tech se refieren a tecnologías de hardware altamente sofisticadas y disruptivas.

Para ampliar información o concertar entrevistas, podéis contactar con:
Elisenda Lara
elisenda.lara@secpho.org
93 783 36 64

¿Qué es la fotónica?

La fotónica es la **ciencia que estudia la generación, control y detección de las ondas de luz y fotones**, que son partículas de luz. De ella se deriva una serie de **tecnologías, consideradas como Deep Tech**, entre las cuales encontramos los s**istemas láser, sensores ópticos, sistemas de escaneo e imagen, iluminación avanzada o las comunicaciones ópticas**, entre otras. Estas tecnologías altamente sofisticadas son clave en ámbitos tan diversos como la **Telemedicina, Industria 4.0, Internet de las Cosas, Smart Cities, Vehículo Autónomo, Ciberseguridad** o el desarrollo de **Nuevos Materiales**.

Acerca de secpho

secpho es un **clúster formado por 150 empresas**, c**entros tecnológicos y grupos de investigación** expertos en innovación tecnológica mediante la aplicación de tecnologías profundas (Deep Tech), principalmente tecnologías fotónicas, a todo tipo de sectores de nuestra economía. En este sentido, **secpho** es un **puente entre talento investigador y empresas innovadoras**, por una parte, y las oportunidades que aparecen en el mercado, por otra.