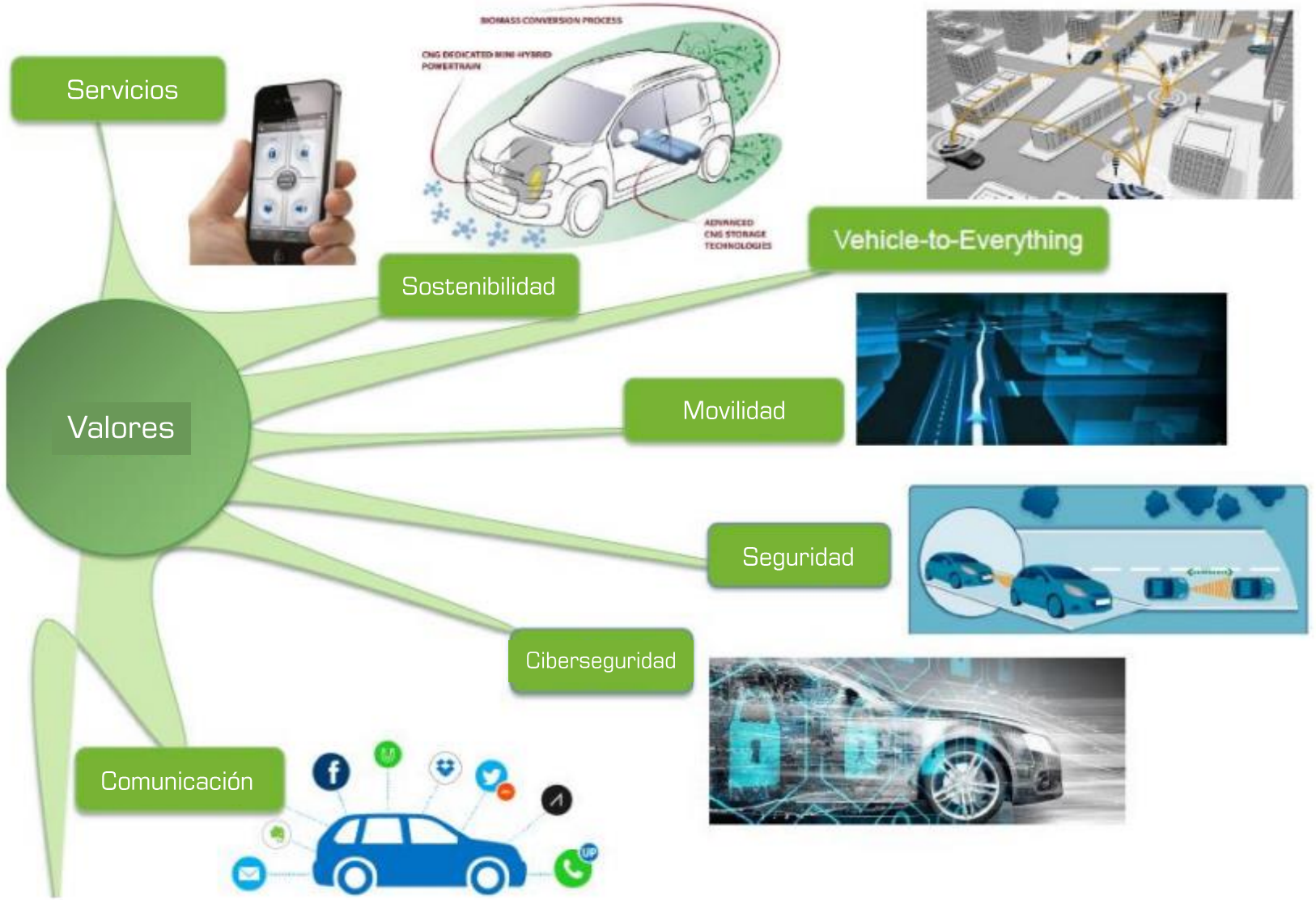
Perspectivas de la Ciberseguridad y la Movilidad Inteligente

3 de junio 2021

www.anfac.com

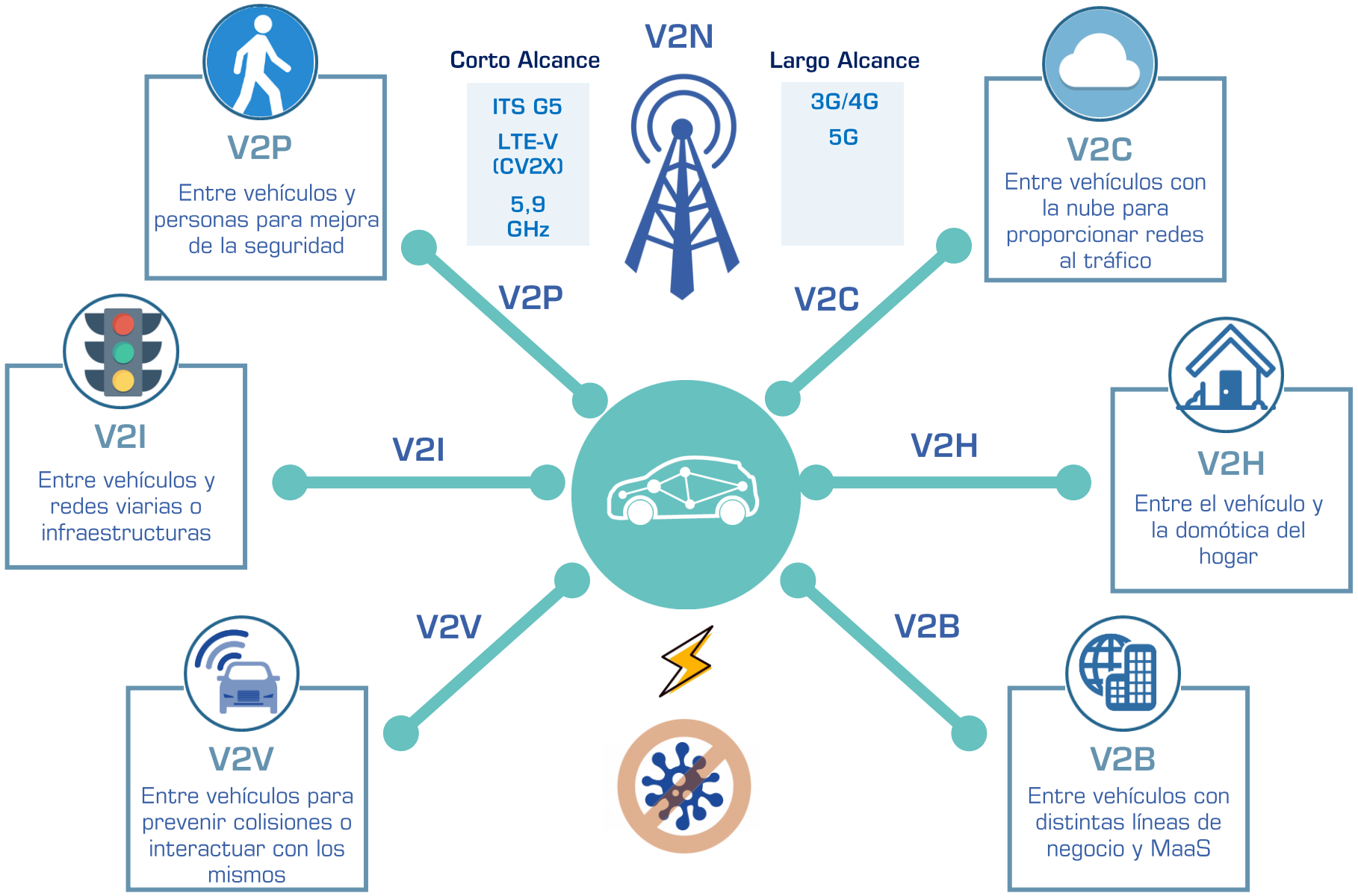
El vehículo como Centro de la Conectividad en el Transporte por Carretera



Hoy en día los vehículos cada vez están más **CONECTADOS V2X**, prácticamente en cualquier vehículo existe un intercambio inalámbrico de datos con servidores, infraestructura (V2I), otros vehículos (V2V) y peatones (V2P).

"*Connectivity Potential*". Fuente: ACEA

El vehículo como Centro de la Conectividad en el Transporte por Carretera



"El ecosistema de la conectividad vehicular". Fuente: UNE (Elaboración ANFAC)

¿Cómo será el vehículo del mañana?

Éstos serán **AUTOMATIZADOS**, capaces de detectar su entorno y tomar decisiones sin intervención humana. La conectividad, a su vez, aumentará la comodidad y la experiencia de los usuarios, mejorarán los productos y **SERVICIOS** y contribuirán a mejorar la **SEGURIDAD VIAL**, reducir el consumo de combustible y facilitar la gestión del tráfico y el estacionamiento.

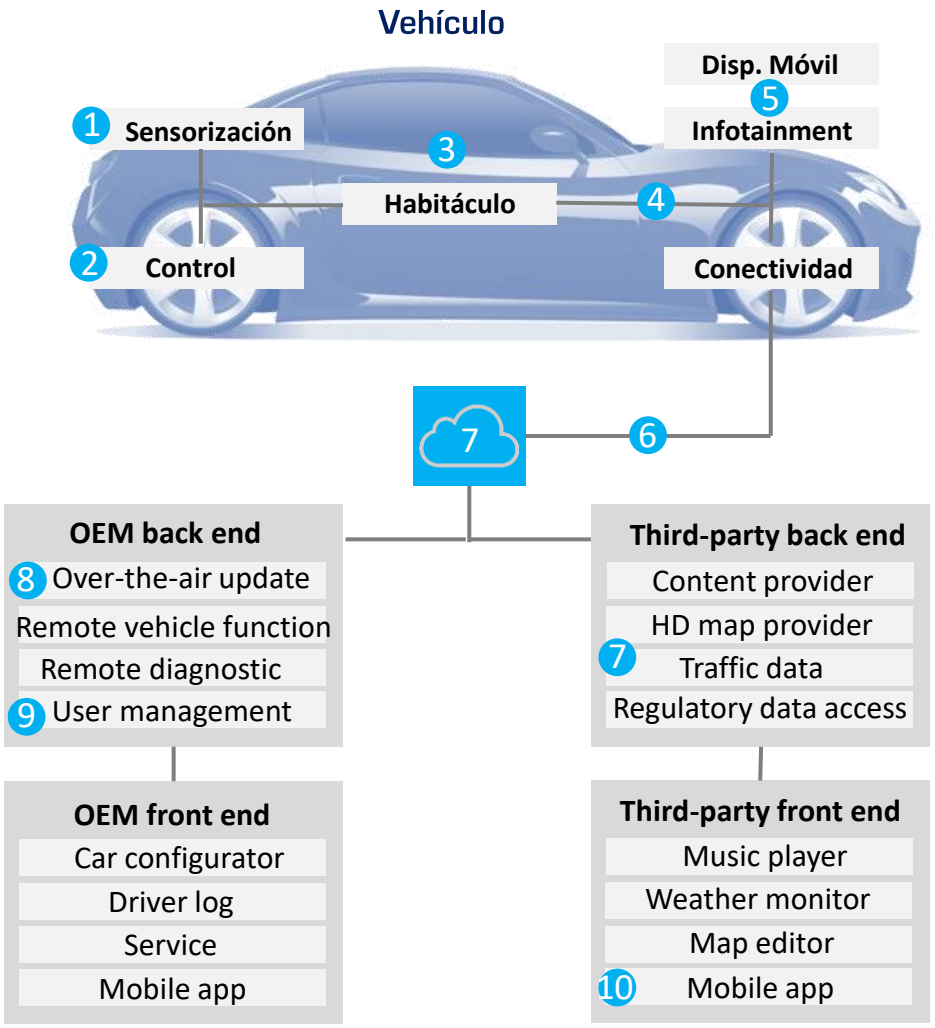
¿Cómo se va ha lograr esta transformación?

Para lograr todo esto, la **DIGITALIZACIÓN** será una pieza clave para alcanzar estos objetivos.

Sin embargo, la digitalización conlleva riesgos asociados a **CIBERSEGURIDAD**, por lo que requiere de desarrollos en la prevención de ciberataques a vehículos.

La Ciberseguridad y el Ecosistema de la Movilidad Conectada

El avance de la arquitectura E/E y la digitalización de los ecosistemas del automóvil son una pieza clave, puesto que ofrece una oportunidad sin precedentes para la mejora de los servicios. Sin embargo, ESTA DIGITALIZACIÓN CONLLEVA RIESGOS, aumenta la lista de vulnerabilidades y posibles ciberataques a vehículos y/o a flotas de vehículos.



Lista de vulnerabilidades o métodos de ataque

1. **Sensor spoofing:** Acceso a funciones de conducción automatizada, motor, airbags, frenos a través de vulnerabilidad de sensores.
2. **Control del vehículo:** Control de las unidades críticas de seguridad como las funciones del motor, el frenado o el kilometraje.
3. **Espionaje:** Grabación no autorizada de conversaciones voz mediante módulos de reconocimiento de voz.
4. **Acceso físico:** Acceso a datos de diagnóstico a bordo para manipulación de datos de consumo, características del motor, alertas, etc.
5. **Contenido Entretenimiento:** Acceso a datos de sistemas Bluetooth, USB, WiFi, etc.
6. **Telemática:** Bloqueo de pasarelas de pago en remoto a través de vulnerabilidad con los módulos de conectividad externos.
7. **Negación del servicio**: Detener vehículos que confían en el back end de los servidores para proveer datos.
8. **Over-the-air**: Acceso al software del vehículo a través de actualizaciones de software
9. **Acceso no autorizado**: Acceso a los servicios y datos del usuario
10. **Robo de datos**: Acceso a información privada a través de apps de terceros.

150 ECUs

Los vehículos de hoy tienen un elevado nº de unidades de control electrónico

Es muy importante cultivar una cultura de ciberseguridad y adoptar un ciclo de vida de ciberseguridad para el desarrollo de vehículos con el objetivo de mejorar la protección de los vehículos contra los ciberataques.

100M líneas código de software/vh.

Se espera que en 2030 los vehículos alcancen las 300M de líneas de código

Un avión de pasajeros tiene 15M de líneas de código

"The race for cybersecurity: Protecting the connected car in the era of new regulation". Fuente: McKinsey

La Ciberseguridad y el Ecosistema de la Movilidad Conectada

Principios de la ciberseguridad para los fabricantes de automóviles

Los fabricantes de automóviles están comprometidos a mitigar estos riesgos.

Para hacerlo, han identificado un conjunto de **SEIS PRINCIPIOS CLAVE** para mejorar la protección de los vehículos conectados y automatizados contra las amenazas de la ciberseguridad.

1 FOMENTAR UNA CULTURA DE LA CIBERSEGURIDAD

Incluir equipos humanos de ciberseguridad para garantizar el EXPERTISE para que la cultura de la ciberseguridad impregne toda la organización para fortalecer la conciencia general de la empresa.

2 ADOPTAR UN CICLO DE VIDA DE LA CIBERSEGURIDAD EN EL DESARROLLO DE LOS VEHÍCULOS

Reducción amenazas ciberseguridad en arquitectura E/E del vehículo: Desarrollo de ECUs con HW y SW específicos para la ciberseguridad y todas las subredes con suficiente ANCHO DE BANDA para implementar métodos de autenticación y CRIPTOGRAFÍA.

3 EVALUAR LAS FUNCIONES DE SEGURIDAD A TRAVÉS DE FASES DE PRUEBA: AUTO AUDITORÍAS Y ENSAYOS

Los ensayos deben ser realizados por PERSONAL CUALIFICADO que no haya formado parte de la fase de desarrollo. Pruebas de seguridad AUTOMATIZADAS para vulnerabilidades conocidas. Pruebas de seguridad FUNCIONAL para evaluar funciones de seguridad.

4 GESTIONAR POLÍTICAS DE ACTUALIZACIÓN PARA LA SEGURIDAD

Informar al usuario final si expira el soporte o reparación para un vehículo. Cuando las actualizaciones EN REMOTO no están disponibles, se debe considerar un plan de ACTUALIZACIONES CRÍTICAS o heredadas.

5 PROPORCIONAR UNA RESPUESTA Y RECUPERACIÓN ANTE INCIDENTES

Realizar un análisis de la CAUSA RAÍZ. Identificar dónde se originó el incidente. Determinar el riesgo de un impacto más amplio en otros vehículos de un mismo OEM. Contener el incidente para eliminar o REDUCIR SU GRAVEDAD. Elaborar un método apropiado para remediar las consecuencias del incidente, etc…

6 MEJORAR EL INTERCAMBIO DE INFORMACIÓN ENTRE STAKEHOLDERS

Generar CONFIANZA entre stakeholders. Contribuir a la elaboración de ESTÁNDARES para toda la industria. Mejorar la INTEGRACIÓN mediante prácticas comúnmente aceptadas, etc…

La Ciberseguridad y el Ecosistema de la Movilidad Conectada

Certificación y requisitos de ciberseguridad para la homologación de vehículos

Dentro del Foro Mundial para la Armonización de la Reglamentación sobre Vehículos (UNECE WP.29), el grupo de trabajo GRVA "Working Party on Automated/Autonomous and Connected Vehicles" desarrolló, aprobó y publicó en junio de 2020 dos reglamentos que contienen requisitos de ciberseguridad para el vehículo conectado:

Regulación UNECE

Reglamento UNECE n.º 155 - Cybersecurity requirements for vehicle type approval

Desarrolla en el marco de la WVTA los requisitos de ciberseguridad del vehículo (producto) y de los procesos de ingeniería asociados (desarrollo, producción, operación, mantenimiento y retirada del servicio).

Reglamento UNECE n.º 156 – Software update and software update management system

Desarrolla en el marco de la WVTA los requisitos mínimos de los procesos de actualización de software vía OTA, para la homologación de vehículos y entre ellos se consideran requisitos específicos de ciberseguridad.

Marco de Estandarización

ISO 21434
Road vehicles. Cybersecurity engineering

Define un sistema de gestión de la ciberseguridad en los procesos de ingeniería de vehículo conectado, cubriendo todas las fases del ciclo de vida del vehículo.

ISO 24089
Road vehicles. Software Update Engineering

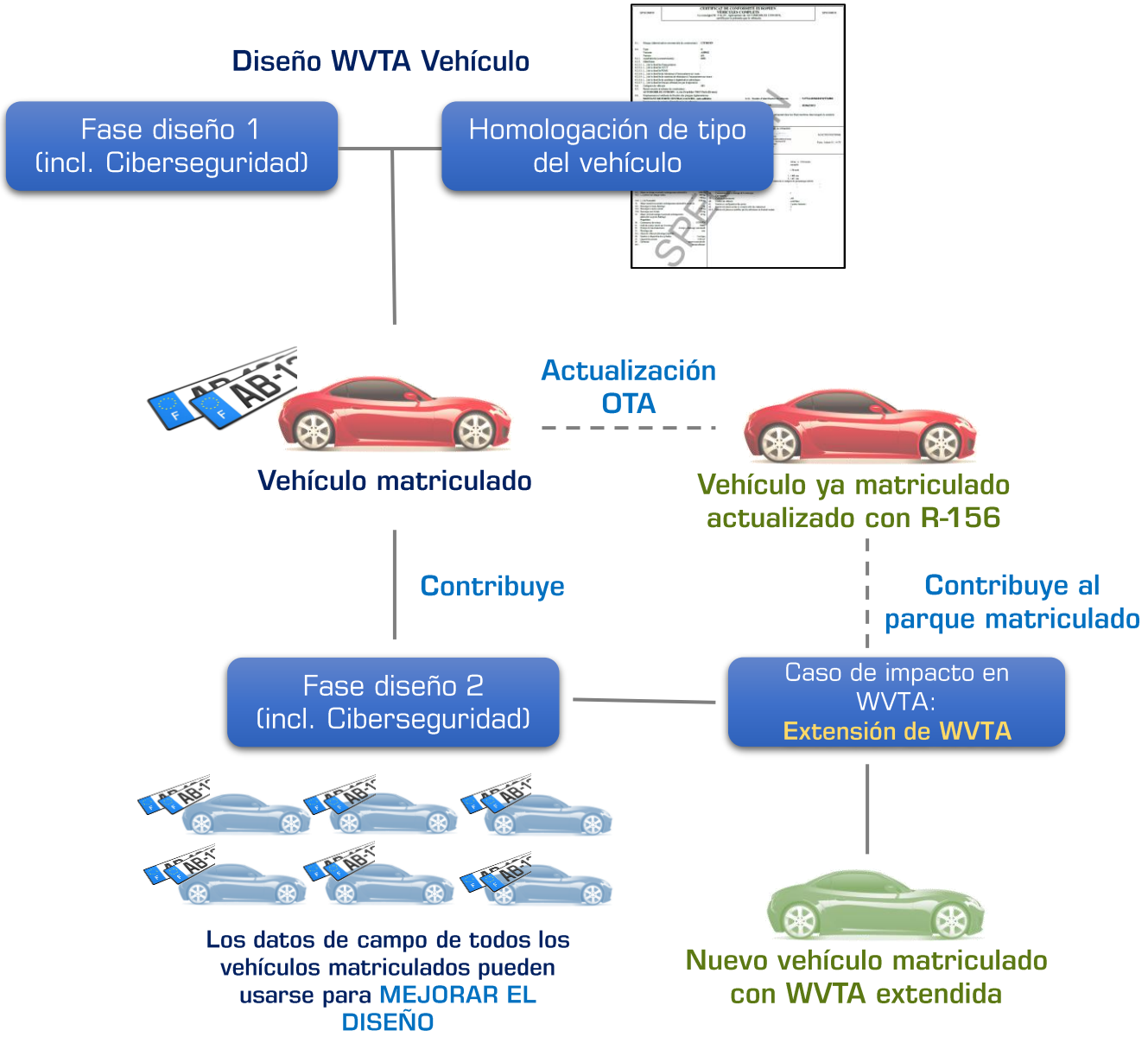
Ambos reglamentos entrarán a formar parte de los requisitos WVTA en Europa a partir de **julio de 2022** para **NT** y **julio de 2024** para **NM**. Será aplicable en **54 países** del WP.29, entre ellos los **26** estados europeos, Japón y Corea.

La Ciberseguridad y el Ecosistema de la Movilidad Conectada

Certificación y requisitos de ciberseguridad para la homologación de vehículos

¿QUÉ VENTAJAS OFRECE VINCULAR LOS AVANCES EN CIBERSEGURIDAD A LA HOMOLOGACIÓN DE TIPO y NORAMLIZACIÓN DEL VEHÍCULO?

- La homologación de tipo del vehículo es un **PRE-REQUISITO INDISPENSABLE** para todos los vehículos antes de su primera matriculación en países/regiones donde se aplica la WVTA.
- Para modificar las características de homologación de un vehículo matriculado es necesario la correspondiente extensión de la homologación o la **ACTUALIZACIÓN DEL SOFTWARE**.
- Las posibles actualizaciones de ciberseguridad quedan totalmente cubiertas por la homologación, con arreglo al **R-156** de actualización de software.
- La implementación del R-156 en el **REGLAMENTO MARCO EUROPEO UE 2018/858** se está discutiendo actualmente en el seno de la Comisión Europea (DG GROW).



"*Example of legal use of AI in vehicle design and update*". Fuente: STELLANTIS (Elaboración ANFAC)