G A _ P

Gómez-Acebo & Pombo

# Primeros reglamentos de ciberseguridad y sobre actualizaciones de *software* de vehículos de motor armonizados internacionalmente y vinculantes

**Ainara Rentería Tazo**
Responsable del Sector de Automoción
*Counsel* de Gómez-Acebo & Pombo

*Se analiza para el sector la regulación aprobada por las Naciones Unidas relativa a la ciberseguridad y a las actualizaciones de* software *en los vehículos.*

El pasado 24 de junio del 2020, el Foro Mundial de Naciones Unidas para la Armonización de la Reglamentación de Vehículos aprobó los primeros reglamentos armonizados internacionalmente y vinculantes para los países miembros en materia de ciberseguridad de vehículos y actualizaciones de *software*.

Esta nueva regulación será vinculante para los cincuenta y cuatro países que forman parte del foro, entre los que se encuentran la Unión Europea y todos sus países miembros, Rusia, Japón y Corea del Sur, entre otros. Entrarán en vigor en enero del 2021 y serán incorporados paulatinamente por los respectivos países.

Los reglamentos establecen medidas en materia de ciberseguridad y actualizaciones de *software* obligatorias para las fabricantes de equipamiento original u OEM (*original equipment manufacturers)* para proteger de ciberataques a los vehículos; son de necesario cumplimiento para obtener la homologación de tipo de los vehículos y que éstos se puedan comercializar. En resumen, se obliga a las citadas fabricantes a contar con un sistema de gestión de ciberseguridad y a documentar las evaluaciones de riesgos, los test y los procesos en las fases de diseño, producción y postproducción. Esto supone que las fabricantes de equipamiento original tendrán que trabajar con las empresas



*N. de la C.*: En las citas literales se ha rectificado en lo posible —sin afectar al sentido— la grafía de ciertos elementos (acentos, mayúsculas, símbolos, abreviaturas, cursivas...) para adecuarlos a las normas tipográficas utilizadas en el resto del texto.

proveedoras de componentes que también quedarán vinculadas por estos nuevos reglamentos en la medida en que dichas fabricantes deban acreditar para la homologación de los vehículos la gestión de los riesgos de los componentes de automoción incorporados a ellos. De igual modo, se obliga a las fabricantes a contar con un sistema de gestión de actualización del *software* antes de la comercialización de los vehículos y de su aplicación en los vehículos en circulación, así como a proteger el proceso de actualización y garantizar la integridad y la autenticidad.

- **Reglamento de las Naciones Unidas sobre la ciberseguridad y los sistemas de gestión de ciberseguridad**

  El reglamento de ciberseguridad aprobado incorpora en su anexo 1 la documentación que sobre control de ciberseguridad deberá aportar el solicitante de la homologación. La fabricante de equipamiento original deberá presentar una declaración responsable de cumplimiento acompañada de la documentación que se especifica. El anexo 5 del reglamento enumera los riesgos de ciberseguridad que deberán valorar las fabricantes de equipamiento original en el estado actual de la ciencia *(state of the art)* y los mecanismos de mitigación de riesgo que se deberán tomar en consideración. Véase la imagen 1 (tabla del anexo 5 del reglamento en su versión original).

  Entre las medidas de control de ciberseguridad que introduce el reglamento de ciberseguridad cabe destacar las siguientes:

  — La obligación del fabricante de gestionar documentalmente los riesgos de ciberseguridad de los vehículos en el momento del diseño, producción y postproducción. A tales efectos, los fabricantes de automóviles deberán recopilar y verificar la información que se especifica en el reglamento en la cadena de suministro, de forma que se acredite el control de los riesgos de ciberseguridad de los componentes incorporados al vehículo.

  — La obligación de los fabricantes de llevar a cabo evaluaciones de riesgos de ciberseguridad desde la fase de diseño y desarrollo, así como distintos test y documentación de las medidas de mitigación desarrolladas en consecuencia. Se deberán actualizar y adaptar a cada momento las evaluaciones de riesgo efectuadas en un principio.

  — La obligación del fabricante de diseñar los vehículos de forma que quede mitigado el riesgo de ataques de ciberseguridad a lo largo de la cadena de valor.

  — La obligación del fabricante de contar con detectores de ciberataques que permitan el análisis forense de ellos de forma histórica y el adecuado registro de cada uno de los ataques, incluidos los meros intentos. Los fabricantes deberán tener la capacidad de responder adecuadamente a cualquier incidente de seguridad en cualquier momento del proceso.

— La obligación del fabricante de reportar periódicamente, al menos una vez al año, a la autoridad nacional competente el resultado de su actividad de control, en especial en lo referente a nuevos ciberataques. Asimismo, se ha de aportar una valoración sobre la eficiencia de las acciones de mitigación implementadas.

Las autoridades de homologación de vehículos que analicen la documentación suministrada deberán inspeccionar y auditar por sí mismos o mediante técnicos especializados el cumplimiento de lo anterior antes de otorgar la homologación. El cumplimiento se acreditará mediante la emisión de un certificado de cumplimiento en materia de ciberseguridad y la marcación correspondiente en el vehículo. Cualquier incumplimiento posterior por parte del fabricante de las obligaciones de reporte o la constatación de incumplimientos por parte de las autoridades competentes supondrá la retirada de la homologación de tipo del vehículo.

- **Reglamento de las Naciones Unidas sobre las actualizaciones de *software* y los sistemas de gestión de actualizaciones de *software***

  Este reglamento incorpora la base legal para actualizar el *software* del vehículo de forma segura, con especial referencia a las actualizaciones de *software* O. T. A. *(over the air)*. Una actualización O. T. A. es la forma más sencilla de efectuar actualizaciones en cualquier dispositivo y, en este caso, también en un vehículo. El realizador sólo tendría que configurar la actualización y se lanzaría un aviso que llegaría a la pantalla del vehículo, con lo que el usuario sólo tendría que aceptar la actualización y ésta se llevaría a cabo en pocos pasos.

  Para garantizar las medidas de seguridad adecuadas para la actualización de *software* en el caso de los vehículos de motor, el reglamento establece las siguientes obligaciones para las fabricantes de equipamiento original:

  — Evaluar la seguridad e interconectividad de los *softwares* que se incorporen a los vehículos, realizando y documentando las evaluaciones de riesgo correspondientes.

  — Llevar un registro de las versiones de *hardware* y *software* relevantes que se correspondan con el tipo de vehículo.

  — Detectar interdependencias con las funcionalidades del vehículo, especialmente en lo concerniente a la actualización del *software*.

  — Implantación de procesos para poder identificar de forma ágil y segura los vehículos que se verán afectados por una actualización.

  — Determinar si una actualización de *software* afecta a la aprobación de tipo ya obtenida.

— La obligación del fabricante, que deberá trasladar contractualmente a sus proveedores de componentes, de proporcionar actualizaciones de *software* seguras para el *software* integrado en el vehículo, de forma que no sólo se proteja al consumidor de los ciberataques, sino también que se asegure que recibirá actualizaciones adecuadas a lo largo de la vida del producto sin que se produzca la obsolescencia de éste por nuevas versiones.

— El deber de informar a los titulares de los vehículos de las actualizaciones de *software*. El reglamento establece la información que se les deberá proporcionar a tales efectos. La fabricante de equipamiento original deberá especificar claramente al usuario si la actualización se realiza por motivo de alguna campaña de seguridad o si puede afectar a la seguridad. Deberá asimismo explicar al usuario los cambios que pudieran darse en las especificaciones del vehículo a causa de la actualización y las funcionalidades del vehículo que podrían no estar operativas durante el proceso de actualización.

— Los fabricantes deberán tener documentado todo lo anterior de forma que se pueda evidenciar frente a las autoridades competentes de homologación su cumplimiento.

— Los usuarios deberán ser informados con posterioridad a la actualización si ésta se ha podido completar correctamente y de cualquier cambio de funcionalidad y actualizaciones de los manuales con motivo de la actualización efectuada.

— La obligación del fabricante de reportar periódicamente a la autoridad nacional competente del resultado de su actividad de control o de cualquier modificación llevada a cabo.

En relación con las actualizaciones de *software over the air*, el fabricante deberá evaluar y especificar debidamente si la actualización se podrá llevar a cabo durante la conducción del vehículo y, en caso de que esto no fuera posible, tendrá que acreditar debidamente cómo garantizará que el vehículo no se pueda poner en uso durante la actualización ni que se vaya a utilizar ninguna funcionalidad del vehículo que pueda poner en riesgo la actualización.

Las autoridades de homologación de vehículos que analicen la documentación suministrada deberán inspeccionar y auditar por sí mismos o mediante técnicos especializados el cumplimiento de lo anterior antes de otorgar la homologación. El cumplimiento se acreditará mediante la emisión de un certificado de cumplimiento en materia de gestión de actualizaciones de *software* y el correspondiente marcado en el vehículo. Cualquier incumplimiento posterior por parte del fabricante de las obligaciones de reporte o la constatación de incumplimientos por parte de las autoridades competentes supondrá la retirada de la homologación del tipo.

- **Nuevos puestos y funciones en el sector de la automoción**

  Estos avances y obligaciones en materia de ciberseguridad harán necesaria previsiblemente la creación de nuevos puestos de trabajo para gestionar la ciberseguridad, preparar los protocolos correspondientes, coordinar los test y hacer las evaluaciones de riesgo que serán necesarias tanto entre los fabricantes como en las empresas del sector que compongan la cadena de valor. Por otro lado, estas nuevas materias y obligaciones deberán tenerse en consideración dentro de las funciones de cumplimiento normativo *(compliance)* existentes en las compañías automovilísticas y, por lo tanto, será necesario prever la coordinación o los procesos de comprobación oportunos.

- **Desarrollo**

  Está previsto que el Grupo de Trabajo sobre Vehículos Autónomos y Conectados de la Comisión Económica para Europa de las Naciones Unidas se reúna en las próximas semanas y delibere con objeto de redactar una lista de requerimientos técnicos —que se publicará más adelante— con el fin de crear un marco de referencia para fabricantes de automóviles en cuanto a ciberseguridad, actualizaciones de *software* y modo de realización de inspecciones para vehículos autónomos de nivel 3. Esta lista será presentada ante el Foro Mundial sobre Armonización de Regulaciones de Vehículos para su aprobación e incluirá estrictos requerimientos para que los fabricantes aseguren que tanto el diseño como las actualizaciones y las pruebas de seguridad incorporen los requerimientos de ciberseguridad pertinentes y que toda actualización de *software* o fallo que derive de ella pueda ser encontrado y solucionado rápidamente en cualquier vehículo.

  Estos dos reglamentos son sólo el comienzo de una regulación sobre la ciberseguridad en los vehículos que será debatida en los próximos foros de armonización de las Naciones Unidas sobre la materia, que será aplicable directamente en un gran número de productores y exportadores y que podrá constituir una referencia para los países no miembros.

**Tabla (*Img 1)**
**List of vulnerability or attack method related to the threats**

| **High level and sub-level descriptions of vulnerability/fear** | | | **Example of vulnerability or attack method** | |
|---|---|---|---|---|
| 4.3.1. Threats regarding back-end servers related to vehicles in the field | 1 | Back-end servers used as a means to attack a vehicle or extract data. | 1.1 | Abuse of privileges by staff **(insider attack)**. |
| | | | 1.2 | **Unauthorized internet access** to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means). |
| | | | 1.3 | **Unauthorized physical access** to the server (conducted by for example USB sticks or other media connecting to the server). |
| | 2 | Services from back-end server being disrupted, affecting the operation of a vehicle. | 2.1 | **Attack on back-end server stops it functioning**, for example it prevents it from interacting with vehicles and providing services they rely on. |
| | 3 | Vehicle related data held on back-end servers being lost or compromised ("data breach"). | 3.1 | Abuse of privileges by staff **(insider attack)**. |
| | | | 3.2 | **Loss of information in the cloud**. Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers. |
| | | | 3.3 | **Unauthorized internet access to the server** (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means). |
| | | | 3.4 | **Unauthorized physical access to the server** (conducted for example by USB sticks or other media connecting to the server). |

| High level and sub-level descriptions of vulnerability/fear | | | Example of vulnerability or attack method | |
|---|---|---|---|---|
| | | | 3.5 | **Information breach** by unintended sharing of data (e.g. admin errors) |
| 4.3.2. Threats to vehicles regarding their communication channels | 4 | Spoofing of messages or data received by the vehicle. | 4.1 | **Spoofing of messages** by impersonation (e.g. 802.11p V2X during platooning, GNSS messages, etc.). |
| | | | 4.2 | **Sybil attack** (in order to spoof other vehicles as if there are many vehicles on the road). |
| | 5 | Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle held code/data. | 5.1 | Communications channels permit **code injection**, for example tampered software binary might be injected into the communication stream. |
| | | | 5.2 | Communications channels permit **manipulate** of vehicle held data/code. |
| | | | 5.3 | Communications channels permit **overwrite** of vehicle held data/code. |
| | | | 5.4 | Communications channels permit **erasure** of vehicle held data/code. |
| | | | 5.5 | Communications channels permit introduction of data/code to the vehicle (write data code). |
| | 6 | Communication channels permit untrusted/unreliable messages to be accepted or are vulnerable to session hijacking/replay attacks. | 6.1 | Accepting information from an **unreliable or untrusted source**. |
| | | | 6.2 | **Man in the middle** attack/ session hijacking. |
| | | | 6.3 | **Replay attack**, for example an attack against a communication gateway allows the attacker to downgrade software of an ECU or firmware of the gateway. |

| High level and sub-level descriptions of vulnerability/fear | | | Example of vulnerability or attack method | |
|---|---|---|---|---|
| | 7 | Information can be readily disclosed. For example, through eavesdropping on communications or through allowing unauthorized access to sensitive files or folders. | 7.1 | **Interception of information** / interfering radiations / monitoring communications. |
| | | | 7.2 | Gaining **unauthorized access** to files or data. |
| | 8 | Denial of service attacks via communication channels to disrupt vehicle functions. | 8.1 | **Sending** a large number of garbage **data** to vehicle information system, **so that it is unable to provide services** in the normal manner. |
| | | | 8.2 | **Black hole attack**, in order to disrupt communication between vehicles the attacker is able to block messages between the vehicles. |
| | 9 | An unprivileged user is able to gain privileged access to vehicle systems. | 9.1 | An unprivileged user is able to **gain privileged access**, for example root access. |
| | 10 | Viruses embedded in communication media are able to infect vehicle systems. | 10.1 | **Virus** embedded in communication media infects vehicle systems. |
| | 11 | Messages received by the vehicle (for example X2V or diagnostic messages), or transmitted within it, contain malicious content. | 11.1 | Malicious **internal** (e.g. CAN) **messages**. |
| | | | 11.2 | Malicious **V2X messages,** e.g. infrastructure to vehicle or vehicle-vehicle messages (e.g. CAM, DENM). |
| | | | 11.3 | Malicious diagnostic messages. |

| High level and sub-level descriptions of vulnerability/fear | | | Example of vulnerability or attack method | |
|---|---|---|---|---|
| | | | 11.4 | Malicious **proprietary messages** (e.g. those normally sent from OEM or component/system/function supplier). |
| 4.3.3. Threats to vehicles regarding their update procedures | 12 | Misuse or compromise of update procedures. | 12.1 | Compromise of **over the air software update procedures**. This includes fabricating the system update program or firmware. |
| | | | 12.2 | Compromise of **local/physical software update procedures**. This includes fabricating the system update program or firmware. |
| | | | 12.3 | The **software** is **manipulated before the update process** (and is therefore corrupted), although the update process is intact. |
| | | | 12.4 | **Compromise** of cryptographic keys of the software provider **to allow invalid update**. |
| | 13 | It is possible to deny legitimate updates. | 13.1 | Denial of Service attack against update server or network to **prevent rollout of critical software updates** and/or unlock of customer specific features. |
| 4.3.4. Threats to vehicles regarding unintended human actions facilitating a cyber attack | 15 | Legitimate actors are able to take actions that would unwittingly facilitate a cyber-attack. | 15.1 | Innocent victim (e.g. owner, operator or maintenance engineer) being **tricked into taking an action** to unintentionally load malware or enable an attack. |
| | | | 15.2 | **Defined security procedures** are not followed. |
| 4.3.5. Threats to vehicles regarding their external | 16 | Manipulation of the connectivity of vehicle functions enables a cyber- | 16.1 | Manipulation of **functions designed to remotely operate systems**, such as remote key, immobilizer and charging pile. |

| High level and sub-level descriptions of vulnerability/fear | | | Example of vulnerability or attack method | |
|---|---|---|---|---|
| connectivity and connections | | attack, this can include telematics; systems that permit remote operations; and systems using short range wireless communications. | 16.2 | **Manipulation of vehicle telematics** (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors). |
| | | | 16.3 | Interference with **short range wireless systems** or sensors. |
| | 17 | Hosted 3rd party software, e.g. entertainment applications, used as a means to attack vehicle systems. | 17.1 | **Corrupted applications**, or those with poor software security, used as a method to attack vehicle systems. |
| | 18 | Devices connected to external interfaces e.g. USB ports, OBD port, used as a means to attack vehicle systems. | 18.1 | **External interfaces** such as USB or other ports used as a point of attack, for example through code injection. |
| | | | 18.2 | Media infected with a **virus** connected to a vehicle system. |
| | | | 18.3 | **Diagnostic access (e.g. dongles in OBD port)** used to facilitate an attack, e.g. manipulate vehicle parameters (directly or indirectly). |
| 4.3.6. Threats to vehicle data/code | 19 | Extraction of vehicle data/code. | 19.1 | Extraction of copyright or proprietary software from vehicle systems (product **piracy**). |
| | | | 19.2 | Unauthorized access to the **owner's privacy information** such as personal identity, payment account information, address book information, location information, vehicle's electronic ID, etc. |
| | | | 19.3 | Extraction of cryptographic keys. |
| | 20 | Manipulation of vehicle data/code. | 20.1 | Illegal/unauthorized changes to **vehicle's electronic ID**. |

| High level and sub-level descriptions of vulnerability/fear | | | Example of vulnerability or attack method | |
|---|---|---|---|---|
| | | | 20.2 | **Identity fraud.** For example, if a user wants to display another identity when communicating with toll systems, manufacturer backend. |
| | | | 20.3 | Action to **circumvent monitoring systems (**e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs). |
| | | | 20.4 | Data manipulation to **falsify vehicle's driving data (**e.g. mileage, driving speed, driving directions, etc.). |
| | | | 20.5 | Unauthorized changes to **system diagnostic data**. |
| | 21 | Erasure of data/code. | 21.1 | Unauthorized deletion/manipulation of **system event logs**. |
| | 22 | Introduction of malware | 22.1 | Introduce **malicious software** or malicious software activity. |
| | 23 | Introduction of new software or overwrite existing software. | 23.1 | **Fabrication of software** of the vehicle control system or information system. |
| | 24 | Disruption of systems or operations. | 24.1 | **Denial of service**, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a high rate of messaging. |
| | 25 | Manipulation of vehicle parameters. | 25.1 | Unauthorized access of **falsify the configuration parameters** of vehicle's key functions, such as brake data, airbag deployed threshold, etc. |
| | | | 25.2 | Unauthorized access of **falsify the charging parameters**, such as |

| High level and sub-level descriptions of vulnerability/fear | | | Example of vulnerability or attack method | |
|---|---|---|---|---|
| | | | | charging voltage, charging power, battery temperature, etc. |
| 4.3.7. Potential vulnerabilities that could be exploited if not sufficiently protected or hardened | 26 | Cryptographic technologies can be compromised or are insufficiently applied. | 26.1 | Combination of short **encryption keys** and long period of validity enables attacker to break encryption. |
| | | | 26.2 | Insufficient use of cryptographic algorithms to protect sensitive systems. |
| | | | 26.3 | Using already or soon to be deprecated **cryptographic algorithms**. |
| | 27 | Parts or supplies could be compromised to permit vehicles to be attacked. | 27.1 | **Hardware or software, engineered to enable an attack** or fails to meet design criteria to stop an attack. |
| | 28 | Software or hardware development permits vulnerabilities. | 28.1 | **Software bugs**. The presence of software bugs can be a basis for potential exploitable vulnerabilities. This is particularly true if software has not been tested to verify that known bad code/bugs is not present and reduce the risk of unknown bad code/bugs being present. |
| | | | 28.2 | **Using remainders** from development (e.g. debug ports, JTAG ports, microprocessors, development certificates, developer passwords…) can permit access to ECUs or permit attackers to gain higher privileges. |
| | 29 | Network design introduces vulnerabilities. | 29.1 | **Superfluous internet ports left open**, providing access to network systems. |

| High level and sub-level descriptions of vulnerability/fear | | | Example of vulnerability or attack method | |
|---|---|---|---|---|
| | | | 29.2 | Circumvent **network separation** to gain control. Specific example is the use of unprotected gateways, or access points (such as truck-trailer gateways), to circumvent protections and gain access to other network segments to perform malicious acts, such as sending arbitrary CAN bus messages. |
| | 31 | Unintended transfer of data can occur. | 31.1 | Information breach. Personal data may be leaked when the **car changes user** (e.g. is sold or is used as hire vehicle with new hirers). |
| | 32 | Physical manipulation of systems can enable an attack. | 32.1 | **Manipulation of electronic hardware**, e.g. unauthorized electronic hardware added to a vehicle to enable "man-in-the-middle" attack.<br>**Replacement of authorized electronic hardware** (e.g., sensors) with unauthorized electronic hardware.<br>**Manipulation of the information** collected by a sensor (for example, using a magnet to tamper with the Hall effect sensor connected to the gearbox). |

**Table B1**

**Mitigation to the threats which are related to "vehicle communication channels"**

| Table A1 Reference | Threats to "vehicle communication channels" | Ref. | Mitigation |
|---|---|---|---|
| 4.1 | Spoofing of messages (e.g. 802.11p V2X during platooning, GNSS messages, etc.) by impersonation. | M10 | The vehicle shall verify the authenticity and integrity of messages it receives. |
| 4.2 | Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road). | M11 | Security controls shall be implemented for storing cryptographic keys (e.g., use of Hardware Security Modules). |
| 5.1 | Communication channels permit code injection into vehicle held data/code, for example tampered software binary might be injected into the communication stream. | M10<br><br>M6 | The vehicle shall verify the authenticity and integrity of messages it receives.<br>Systems shall implement security by design to minimize risks. |
| 5.2 | Communication channels permit manipulation of vehicle held data/code. | M7 | Access control techniques and designs shall be applied to protect system data/code. |
| 5.3 | Communication channels permit overwrite of vehicle held data/code. | | |
| 5.4<br>21.1 | Communication channels permit erasure of vehicle held data/code. | | |
| 5.5 | Communication channels permit introduction of data/code to vehicle systems (write data code). | | |

| Table A1 Reference | Threats to "vehicle communication channels" | Ref. | Mitigation |
|---|---|---|---|
| 6.1 | Accepting information from an unreliable or untrusted source. | M10 | The vehicle shall verify the authenticity and integrity of messages it receives. |
| 6.2 | Man in the middle attack / session hijacking. | M10 | The vehicle shall verify the authenticity and integrity of messages it receives. |
| 6.3 | Replay attack, for example an attack against a communication gateway allows the attacker to downgrade software of an ECU or firmware of the gateway. | | |
| 7.1 | Interception of information / interfering radiations / monitoring communications. | M12 | Confidential data transmitted to or from the vehicle shall be protected. |
| 7.2 | Gaining unauthorized access to files or data. | M8 | Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data. Example of Security Controls can be found in OWASP. |
| 8.1 | Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner. | M13 | Measures to detect and recover from a denial of service attack shall be employed. |
| 8.2 | Black hole attack, disruption of communication between vehicles by blocking the transfer of messages to other vehicles. | M13 | Measures to detect and recover from a denial of service attack shall be employed. |

| Table A1 Reference | Threats to "vehicle communication channels" | Ref. | Mitigation |
|---|---|---|---|
| 9.1 | An unprivileged user is able to gain privileged access, for example root access. | M9 | Measures to prevent and detect unauthorized access shall be employed. |
| 10.1 | Virus embedded in communication media infects vehicle systems. | M14 | Measures to protect systems against embedded viruses/malware should be considered. |
| 11.1 | Malicious internal (e.g. CAN) messages. | M15 | Measures to detect malicious internal messages or activity should be considered. |
| 11.2 | Malicious V2X messages, e.g. infrastructure to vehicle or vehicle-vehicle messages (e.g. CAM, DENM). | M10 | The vehicle shall verify the authenticity and integrity of messages it receives. |
| 11.3 | Malicious diagnostic messages. | | |
| 11.4 | Malicious proprietary messages (e.g. those normally sent from OEM or component/system/function supplier). | | |

**Table B2**

**Mitigations to the threats which are related to "update process"**

| Table A1 Reference | Threats to "update process" | Ref. | Mitigation |
|---|---|---|---|
| 12.1 | Compromise of over the air software update.procedures. This includes fabricating thesystem update program or firmware. | M16 | Secure software update procedures shall be employed. |
| 12.2 | Compromise of local/physical software update procedures. This includes fabricating the system update program or firmware. | | |
| 12.3 | The software is manipulated before the update process (and is therefore corrupted), although the update process is intact. | | |
| 12.4 | Compromise of cryptographic keys of the software provider to allow invalid update. | M11 | Security controls shall be implemented for storing cryptographic keys. |
| 13.1 | Denial of Service attack against update server or network to prevent rollout of critical software updates and/or unlock of customer specific features. | M3 | Security Controls shall be applied to back-end systems. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage. Example Security Controls can be found in OWASP. |

**Table B3**

**Mitigations to the threats which are related to "unintended human actions facilitating a cyber attack"**

| Table A1 Reference | Threats relating to "unintended human actions" | Ref. | Mitigation |
|---|---|---|---|
| 15.1 | Innocent victim (e.g. owner, operator or maintenance engineer) is tricked into taking an action to unintentionally load malware or enable an attack. | M18 | Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege. |
| 15.2 | Defined security procedures are not followed. | M19 | Organizations shall ensure security procedures are defined and followed including logging of actions and access related to the management of the security functions. |

**Table B4**

**Mitigation to the threats which are related to "external connectivity and connections"**

| Table A1 Reference | Threats to “external connectivity and connections” | Ref. | Mitigation |
|---|---|---|---|
| 16.1 | Manipulation of functions designed to remotely operate vehicle systems, such as remote key, immobiliser, and charging pile. | M20 | Security controls shall be applied to systems that have remote access. |
| 16.2 | Manipulation of vehicle telematics (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors). | | |
| 16.3 | Interference with short range wireless systems or sensors. | | |
| 17.1 | Corrupted applications, or those with poor software security, used as a method to attack vehicle systems. | M21 | Software shall be security assessed, authenticated and integrity protected.<br>Security controls shall be applied to minimise the risk from third party software that is intended or foreseeable to be hosted on the vehicle. |
| 18.1 | External interfaces such as USB or other ports used as a point of attack, for example through code injection. | M22 | Security controls shall be applied to external interfaces. |
| 18.2 | Media infected with viruses connected to the vehicle. | | |
| 18.3 | Diagnostic access (e.g. dongles in OBD port) used to facilitate an attack, e.g. manipulate vehicle parameters (directly or indirectly). | M22 | Security controls shall be applied to external interfaces. |

**Table B5**

**Mitigations to the threats which are related to "potential targets of, or motivations for, an attack"**

| Table A1 Reference | Threats to "potential targets of, or motivations for, an attack" | Ref. | Mitigation |
|---|---|---|---|
| 19.1 | Extraction of copyright or proprietary software from vehicle systems (product piracy / stolen software). | M7 | Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP. |
| 19.2 | Unauthorized access to the owner's privacy information such as personal identity, payment account information, address book information, location information, vehicle's electronic ID, etc. | M8 | Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data. Examples of Security Controls can be found in OWASP. |
| 19.3 | Extraction of cryptographic keys. | M11 | Security controls shall be implemented for storing cryptographic keys e.g. Security Modules. |
| 20.1 | Illegal/unauthorised changes to vehicle's electronic ID. | M7 | Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP. |
| 20.2 | Identity fraud. For example, if a user wants to display another identity when communicating with toll systems, manufacturer backend. | | |
| 20.3 | Action to circumvent monitoring systems (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs). | M7 | Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP. |
| 20.4 | Data manipulation to falsify vehicle's driving data (e.g. mileage, | | |

| Table A1 Reference | Threats to "potential targets of, or motivations for, an attack" | Ref. | Mitigation |
|---|---|---|---|
| | driving speed, driving directions, etc.). | | Data manipulation attacks on sensors or transmitted data could be mitigated by correlating the data from different sources of information. |
| 20.5 | Unauthorised changes to system diagnostic data. | | |
| 21.1 | Unauthorized deletion/manipulation of system event logs. | M7 | Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP. |
| 22.2 | Introduce malicious software or malicious software activity. | M7 | Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP. |
| 23.1 | Fabrication of software of the vehicle control system or information system. | M7 | |
| 24.1 | Denial of service, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a high rate of messaging. | M7 | Measures to detect and recover from a denial of service attack shall be employed. |
| 25.1 | Unauthorized access to falsify configuration parameters of vehicle's key functions, such as brake data, airbag deployed threshold, etc. | M13 | Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP. |
| 25.2 | Unauthorized access to falsify charging parameters, such as charging voltage, charging power, battery temperature, etc. | M7 | |

**Table B6**

**Mitigations to the threats which are related to "potential vulnerabilities that could be exploited if not sufficiently protected or hardened"**

| Table A1 Reference | Threats to "potential vulnerabilities that could be exploited if not sufficiently protected or hardened" | Ref. | Mitigation |
|---|---|---|---|
| 26.1 | Combination of short encryption keys and long period of validity enables attacker to break encryption. | M23 | Cybersecurity best practices for software and hardware development shall be followed. |
| 26.2 | Insufficient use of cryptographic algorithms to protect sensitive systems. | | |
| 26.3 | Using deprecated cryptographic algorithms. | | |
| 27.1 | Hardware or software, engineered to enable an attack or fail to meet design criteria to stop an attack. | M23 | Cybersecurity best practices for software and hardware development shall be followed. |
| 28.1 | The presence of software bugs can be a basis for potential exploitable vulnerabilities. This is particularly true if software has not been tested to verify that known bad code/bugs is not present and reduce the risk of unknown bad code/bugs being present. | M23 | Cybersecurity best practices for software and hardware development shall be followed.<br><br>Cybersecurity testing with adequate coverage. |
| 28.2 | Using remainders from development (e.g. debug ports, JTAG ports, microprocessors, development certificates, developer passwords…) can permit an attacker to access ECUs or gain higher privileges. | | |

| Table A1 Reference | Threats to "potential vulnerabilities that could be exploited if not sufficiently protected or hardened" | Ref. | Mitigation |
|---|---|---|---|
| 29.1 | Superfluous internet ports left open, providing access to network systems. | M23 | Cybersecurity best practices for software and hardware development shall be followed.<br><br>Cybersecurity testing with adequate coverage. |
| 29.2 | Circumvent network separation to gain control. Specific example is the use of unprotected gateways, or access points (such as truck-trailer gateways), to circumvent protections and gain access to other network segments to perform malicious acts, such as sending arbitrary CAN bus messages. | M23 | Cybersecurity best practices for software and hardware development shall be followed.<br>Cybersecurity best practices for system design and system integration shall be followed. |

**Table B7**

**Mitigations to the threats which are related to "data loss / data breach from vehicle"**

| Table A1 Reference | Threats of "data loss / data breach from vehicle" | Ref. | Mitigation |
|---|---|---|---|
| 31.1 | Information breach. Personal data may be breached when the car changes user (e.g. is sold or is used as hire vehicle with new hirers). | M24 | Best practices for the protection of data integrity and confidentiality shall be followed for storing personal data. |

**Table B8**

**Mitigations to the threats which are related to "physical manipulation of systems to enable an attack"**

| Reference | Threats to "physical manipulation of systems to enable an attack" | Ref. | Mitigation |
|---|---|---|---|
| 32.1 | Manipulation of OEM hardware, e.g. unauthorised hardware added to a vehicle to enable "man-in-the-middle" attack. | M9 | Measures to prevent and detect unauthorized access shall be employed. |

**Table C1**

**Mitigations to the threats which are related to "back-end servers"**

| Table A1 Reference | Threats to "back-end servers" | Ref. | Mitigation |
|---|---|---|---|
| 1.1 & 3.1 | Abuse of privileges by staff (insider attack). | M1 | Security Controls are applied to back-end systems to minimise the risk of insider attack. |
| 1.2 & 3.3 | Unauthorised internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means). | M2 | Security Controls are applied to back-end systems to minimise unauthorised access. Example Security Controls can be found in OWASP. |
| 1.3 & 3.4 | Unauthorised physical access to the server (conducted by for example USB sticks or other media connecting to the server). | M8 | Through system design and access control it should not be possible for unauthorised personnel to access personal or system critical data. |
| 2.1 | Attack on back-end server stops it functioning, for example it prevents it from interacting with vehicles and providing services they rely on. | M3 | Security Controls are applied to back-end systems. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage. Example Security Controls can be found in OWASP. |
| 3.2 | Loss of information in the cloud. Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers. | M4 | Security Controls are applied to minimise risks associated with cloud computing. Example Security Controls can be found in OWASP and NCSC cloud computing guidance. |
| 3.5 | Information breach by unintended sharing of data (e.g. admin errors, storing data in servers in garages). | M5 | Security Controls are applied to back-end systems to prevent data breaches. Example. |

**Table C2**

**Mitigations to the threats which are related to "Unintended human actions"**

| Table A1 Reference | Threats relating to "Unintended human actions" | Ref. | Mitigation |
|---|---|---|---|
| 15.1 | Innocent victim (e.g. owner, operator or maintenance engineer) is tricked into taking an action to unintentionally load malware or enable an attack. | M18 | Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege. |
| 15.2 | Defined security procedures are not followed. | M19 | Organizations shall ensure security procedures are defined and followed including logging of actions and access related to the management of the security functions. |

**Table C3**

**Mitigations to the threats which are related to "Physical loss of data loss"**

| Table A1 Reference | Threats of "Physical loss of data" | Ref. | Mitigation |
|---|---|---|---|
| 30.1 | Damage caused by a third party. Sensitive data may be lost or compromised due to physical damages in cases of traffic accident or theft. | M24 | Best practices for the protection of data integrity and confidentiality shall be followed for storing personal data. Example Security Controls can be found in ISO/SC27/WG5. |
| 30.2 | Loss from DRM (digital right management) conflicts. User data may be deleted due to DRM issues. | | |
| 30.3 | The (integrity of) sensitive data may be lost due to IT components wear and tear, causing potential cascading issues (in case of key alteration, for example). | | |