**TFCS 21-03 (Chairs) Draft set of technical requirements for cyber security and software updates**

Introduction:

* The requirements have been drawn from Regulations R155 and R156 to identify enforcement neutral requirements. The ordering has been changed slightly to present a logical flow.
* Parenthetical references have been added pointing to corresponding section(s) in the corresponding regulation.
* Currently everything is in one document – Part 1 would be an explanatory section for the document; Part 2 would be the guidelines further divided into 3 sections: Section 1 = Management Systems, Section 2 = Vehicle Requirements, and Section 3 = a combined definition section. Annex 1 could be broken into separate documents if desired, but currently it is small enough that a single document was manageable.
* The colour coding is as follows:
  + Yellow = defined word from the Cyber security regulation
  + Green = defined word from the Software updates regulation
  + Blue = defined word from both regulations

**Recommendations for Automotive Cyber Security and Software Updates**

**Part I**

Individuals and organizations involved in the design, manufacturing, or assembly of a motor vehicle have a role to play with respect to vehicle cybersecurity

This document is provided as guidance for Contracting Parties to the 1998 Agreement when formulating national legislation on cyber security for automotive vehicles and/or legislation regarding software updates and the processes for updating vehicle’s software. The aim of the guidance is to enable a harmonized approach to the adoption of such legislation.

The document lists technical requirements for the vehicle and technical requirements for management systems. The technical requirements for the management systems list requirements that are external to the vehicle but need to be in place to effectively manage the cyber security of a vehicle over its lifetime and to ensure software updates will be sufficiently appraised and protected before they are sent to a vehicle.

It is recommended that, as a minimum, the technical requirements relating to the vehicle are adopted en mass when formulating national legislation. Where possible the requirements for the management system should also be adapted. Where it is not possible to adopt the management system requirements within legislation, it is suggested they are adopted as national guidance for manufacturers of automobiles to follow.

The document does not define acceptance criteria nor test criteria for these requirements.

**Part II**

1. MANAGEMENT SYSTEMS

1.1. Management System for Cyber security

1.1.1. The vehicle manufacturer shall have a system that manages cyber security throughout the following phases: (7.2.2.1)

(a) Development phase;

(b) Production phase; and

(c) Post-production phase.

1.1.2. The management system for cyber security shall include processes to: (7.2.2.2)

(a) manage cyber security at an organisational level;

(b) identify risks to vehicles, which shall include consideration of the threats in Annex 1, Part A, and other relevant threats;

(c) assess, categorise and treat identified risks;

(d) verify that risks identified are appropriately managed;

(e) test the cyber security of a vehicle;

(f) ensure that risk assessments are kept current;

(g) monitor for, detect and respond to cyber-attacks, cyber-threats and vulnerabilities on the vehicle;

(h) assess whether the cyber security measures implemented remain effective when new cyber threats or vulnerabilities are identified; and

(i) provide data to enable analysis of attempted or successful cyber-attacks.

1.1.3. The management system for cyber security shall ensure that cyber threats and vulnerabilities that are identified as requiring a response from the manufacturer shall be mitigated within a reasonable timeframe. (7.2.2.3)

1.1.4. The processes used in the management system for cyber security shall ensure that the monitoring specified in section 1.1.2(g) is continual and includes: (7.2.2.4)

(a) vehicles in the field; and

(b) the capability to analyse and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs. This capability shall respect the privacy rights of vehicle owners and drivers, particularly with respect to consent.

1.1.5. The management system for cyber security shall manage cyber security related dependencies that may exist with contracted suppliers, service providers or manufacturer’s sub-organizations. (7.2.2.5.)

1.2 Management System for Software Updates

1.2.1 The management system for software updates shall include processes to:

(a) document information relating to software updates (7.1.1.1)

(b) securely maintain the information documented in 1.2.1 part (a) (7.1.1.1)

(c) make the information documented in 1.2.1 part (a) available to appropriate authorities upon request (7.1.1.1)

(d) uniquely identify all initial and updated versions of software on systems of the vehicle specified in regulation or national legislation including integrity validation data, and relevant hardware components (7.1.1.2)

Chair suggested amendment

(e) access and update information regarding **any unique identifiers used to represent information about software on a vehicle**, ~~versions of the software of systems or functions specified in regulation or national legislation for a vehicle or vehicle system~~ before and after an update, which includes the ability to update information regarding the software versions and their integrity validation data of all ~~relevant~~ software **relevant to each unique identifier used** (7.1.1.3)

Chair Suggested Amendment

(f) verify that, **where unique identifiers are used to represent information about software on a vehicle,** the version(s) of the software present on a **relevant** component of **the vehicle** ~~a system or function specified in regulation or national legislation for a vehicle or vehicle system~~ are consistent with **those defined by the relevant unique identifier** ~~information stored by the manufacturer according to 1.2.1 part (e)~~ (7.1.1.4)

(g) identify interdependencies of the updated system with other system(s) (7.1.1.5)

(h) identify target vehicles for a software update (7.1.1.6)

(i) confirm the compatibility of a software update with the target vehicle(s)'s configuration before the software update is issued, including an assessment of compatibility between the last known software/hardware configuration of the target vehicle(s) and the software update to be issued (7.1.1.7)

(j) determine whether a software update will affect any system that is subject to regulation or national legislation, including whether the update will impact or alter any of the parameters used to define the systems the update affects, or whether it changes any parameters that are subject to regulation or national legislation (7.1.1.8)

(k) determine whether a software update will add, alter or enable any function(s) that were not present, or enabled, when the vehicle was certified according to regulation or national legislation, or whether an update will alter or disable any other parameters or functions that are subject to regulation or national legislation, including consideration of whether:

(1) regulated information (according to regulation or national legislation) regarding the vehicle will need to be modified

(2) results of previous tests conducted according to regulation or national legislation will no longer cover the vehicle after modification

(3) any modifications to functions on the vehicle will affect the vehicle’s certification according to regulation or national legislation (7.1.1.9)

(l) determine whether a software update will affect any other system required for the safe and continued operation of the vehicle, or if the update will add or alter functionality of the vehicle compared to when it was certified. (7.1.1.10)

(m) enable the vehicle user to be informed about a software update (7.1.1.11).

1.2.2. The vehicle manufacturer shall record and store the following information for each update: (7.1.2)

(a) Documentation describing the processes used by the vehicle manufacturer for software updates and any relevant standards followed. (7.1.2.1)

(b) Documentation describing the configuration of any systems, that are regulated by regulation or national legislation, before and after an update. This shall include unique identification for the system’s hardware and software (including software versions) and any relevant vehicle or system parameters. (7.1.2.2)

Chair suggested amendment

(c) **If unique identifiers are used to represent information about software of Electronic Control Systems contributing to systems or functions on a vehicle that are specified in regulation or national legislation**, an auditable register describing **information about** all the software relevant to each unique identifier ~~relevant to all the systems or functions on a vehicle that are regulated according to national legislation or regulation~~ before and after an update. This shall include information of the software versions and their integrity validation data for all relevant software. (7.1.2.3)

(d) Documentation listing target vehicles for the update and confirmation of the compatibility of the last known configuration of those vehicles with the update. (7.1.2.4)

(e) Documentation for all software updates describing: (7.1.2.5)

(1) the purpose of the update

(2) what systems or functions of the vehicle the update may affect

(3) which (if any) of the systems or functions listed in part b) are required by regulation or national legislation (if any)

(4) if applicable, whether the software update affects the fulfilment of the requirements of any relevant regulation or national legislation identified in part 3)

(5) whether the software update affects any parameter specified in regulation or national legislation for a vehicle or vehicle system

(6) if applicable, whether an approval for the update was requested from the relevant national authority

(7) how the software update may be executed and under what conditions

(8) confirmation that the software update will be conducted safely and securely

(9) confirmation that the software update has undergone and successfully passed verification and validation procedures

1.2.3 The information specified in 1.2.2.3 and 1.2.2.4 shall be available from the vehicle manufacturer to relevant national authorities. (7.1.1.12)

1.2.4. With regards to security for software updates, the vehicle manufacturer shall implement and maintain processes to: (7.1.3)

(a) ensure software updates are protected to reasonably prevent manipulation before the update process is initiated; (7.1.3.1)

(b) ensure software update processes used are protected to reasonably prevent their compromise, including the development of the software update delivery system; and (7.1.3.2)

(c) verify and validate software functionality and code for the software used in the vehicle are appropriate. (7.1.3.3)

1.2.5. For vehicles that support over the air updates, the vehicle manufacturer shall implement and maintain processes to: (7.1.4)

(a) assess over the air updates to ensure they will not impact safety, if conducted during driving; and (7.1.4.1)

(b) ensure over the air updates that require a specific skilled or complex action (for example recalibration of a sensor post-programming in order to complete an update process) can only proceed when a person skilled to do that action is present or is in control of the process. (7.1.4.2)

2. VEHICLE REQUIREMENTS

2.1. Requirements for Cyber Security

2.1.1. The manufacturer shall identify the critical elements of the vehicle and perform an exhaustive risk assessment for the vehicle and shall treat/manage the identified risks appropriately. (7.3.3)

2.1.1.1. The risk assessment shall consider the individual elements of the vehicle and their interactions.

2.1.1.2. The risk assessment shall consider interactions with external systems.

2.1.1.3. While assessing the risks, the vehicle manufacturer shall consider the risks related to all the threats referred to in Annex 1, part A, as well as any other relevant risk.

2.1.1.4. The risk assessment shall consider all supplier-related risks. (7.3.2)

2.1.2. The manufacturer shall protect the vehicle against risks identified in the risk assessment. (7.3.4)

2.1.2.1. Relevant and proportionate mitigations shall be implemented to protect the vehicle.

2.1.2.2. The mitigations implemented shall include all mitigations referred to in Annex 1, Part B and C which are relevant for the risks identified. However, if a mitigation referred to in Annex 1, Part B or C, is not relevant or not sufficient for the risk identified, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented.

2.1.2.3. The vehicle manufacturer shall perform appropriate and sufficient testing to verify the effectiveness of the security measures implemented. (7.3.6)

2.1.3. The vehicle manufacturer shall put in place appropriate and proportionate measures to secure dedicated environments on the vehicle (if provided) for the storage and execution of aftermarket software, services, applications or data. (7.3.5)

2.1.4. The vehicle manufacturer shall implement measures for the vehicle to: (7.3.7)

(a) Detect and prevent cyber-attacks against the vehicle;

(b) Support the monitoring capability of the vehicle manufacturer with regards to detecting threats, vulnerabilities and cyber-attacks relevant to the vehicle;

(c) Provide data forensic capability to enable analysis of attempted or successful cyber-attacks.

2.1.5. Cryptographic modules shall be in line with consensus standards. If the cryptographic modules used are not in line with consensus standards, then the vehicle manufacturer shall justify their use. (7.3.8)

2.2. Requirements for Software Updates

2.2.1. The authenticity and integrity of software updates shall be protected to reasonably prevent their compromise and reasonably prevent invalid updates. (7.2.1.1)

Chair suggested insertion

**2.2.x If unique identifiers are used to represent information about software of Electronic Control Systems contributing to systems or functions on a vehicle that are specified in regulation or national legislation, each identifier shall be uniquely identifiable. When relevant software is modified by the vehicle manufacturer, the unique identifier shall be updated if it affects the certification of the vehicle or its systems (7.2.1.2.1)**

**Chair suggested amendment**

2.2.2 **The versions of the software on Electronic Control Systems contributing to systems or functions on a vehicle that are specified in regulation or national legislation, or unique identifiers used to represent information about that software,** ~~Information to identify the configuration of the software on a vehicle~~ shall be easily readable in a standardized way via the use of an electronic communication interface on the vehicle. (7.2.1.2.2)

2.2.3. Information regarding the configuration of the software on a vehicle shall be protected against unauthorized modification. (7.2.1.2.3)

2.2.4. Additional Requirements for Over-the-Air (OTA) Updates (7.2.2)

2.2.4.1. The vehicle shall restore systems to their previous version in case of a failed or interrupted update or that the vehicle shall be placed into a safe state after a failed or interrupted update.

2.2.4.2. Software updates shall only be executed when the vehicle has enough power to complete the update process (including that needed for a possible recovery to the previous version or for the vehicle to be placed into a safe state).

2.2.4.3. When the execution of an update may affect the safety of the vehicle, the vehicle shall be in a state where it can be executed safely.

2.2.4.4. The vehicle user shall be able to be informed about an update before the update is executed. The information made available shall contain:

(a) The purpose of the update. This could include the criticality of the update and if the update is for recall, safety and/or security purposes;

(b) Any changes implemented by the update on vehicle functions;

(c) The expected time to complete execution of the update;

(d) Any vehicle functionalities which may not be available during the execution of the update;

(e) Any instructions that may help the vehicle user safely execute the update;

In case of groups of updates with a similar content one information may cover a group.

2.2.4.5. In the situation where the execution of an update while driving may not be safe, the vehicle shall either:

(a) Be incapable of being driven during the execution of the update; or,

(b) Be in a state ensuring that the driver is not able to use any functionality of the vehicle that would affect the safety of the vehicle or the successful execution of the update.

2.2.4.6. After the execution of an update:

(a) The vehicle user shall be able to be informed of the success (or failure) of the update;

(b) The vehicle user shall be able to be informed about the changes implemented and any related updates to the user manual (if applicable).

DEFINITIONS

3.1. "Cyber security" means the condition in which road vehicles and their functions are protected from cyber threats to electrical or electronic components.

3.2. "Execution", in the context of software updates, means the process of installing and activating an update that has been downloaded.

3.x “Configuration information” is data that provides an understanding of the software versions present on the vehicle. Such data may be detailed or provided by an identifier for a set configuration (i.e., RXSWIN)

3.x. “Integrity Validation Data” means a representation of digital data, against which comparisons can be made to detect errors or changes in the data. This may include checksums and hash values.

3.3. "Mitigation" means a measure that is reducing risk.

3.4. "Over-the-Air (OTA) " means any method of making data transfers wirelessly instead of using a cable or other local connection.

~~Blackberry original suggestion~~

~~3.x. "Development phase" means the period before a vehicle type is type approved~~ **~~enters series production~~**

~~Blackberry suggestion alternative assuming affected requirement relates to (logical) vehicle models:~~

~~3.x "Development phase" means the period before a vehicle type is type approved~~ **~~model goes into series production~~**

~~Blackberry suggestion alternative assuming affected requirement relates to (actual) physical vehicles:~~

~~3.x "Development phase" means the period before a vehicle enters series production type is type approved.~~

~~Blackberry suggestion alternative assuming affected requirement relates to (logical) vehicle models:~~

~~3.x. "Production phase" refers to the duration of production of a vehicle type~~ **~~model~~**~~.~~

~~Blackberry suggestion alternative assuming affected requirement relates to (actual) physical vehicles:~~

~~3.x "Production phase" refers to the~~ **~~period~~** ~~duration of production of a vehicle type.~~

~~Blackberry original suggestion~~

~~3.x. "Post-production phase"~~ **~~"Ceased-production phase"~~** ~~refers to the period in which a vehicle type is no longer produced until the end-of-life of all vehicles under the vehicle type. Vehicles incorporating a specific vehicle type will be operational during this phase but will no longer be produced. The phase ends when there are no longer any operational vehicles of a specific vehicle type.~~

~~Blackberry suggestion alternative assuming affected requirement relates to (logical) vehicle models:~~

~~3.x "Post-production phase" refers to the period in which a vehicle type~~ **~~model~~** ~~is no longer produced,~~ **~~up~~** ~~until the end-of-life of all vehicles under~~ **~~of~~** ~~the vehicle type~~ **~~model~~**~~. Vehicles incorporating~~ **~~of~~** ~~a specific vehicle~~ **~~model~~** ~~type will~~ **~~can~~** ~~be operational during this phase but~~ **~~new vehicles of that model~~** ~~will no longer be produced. The~~ **~~This~~** ~~phase ends when there are no longer any operational vehicles of a specific vehicle type~~ **~~model~~**~~.~~

~~Blackberry suggestion alternative assuming affected requirement relates to (actual) physical vehicles:~~

~~3.x "Post-production phase" refers to the period in which~~ **~~after~~** ~~a vehicle type is no longer~~ **~~has been~~** ~~produced,~~ **~~up~~** ~~until the~~ **~~vehicle's~~** ~~end-of-life. of all vehicles under the vehicle type. Vehicles incorporating a specific vehicle type will be operational during this phase but will no longer be produced. The phase ends when there are no longer any operational vehicles of a specific vehicle type.~~

3.5. "Risk" means the potential that a given threat will exploit vulnerabilities of a vehicle and thereby cause harm to the organization or to an individual.

3.6. "Risk Assessment" means the overall process of finding, recognizing and describing risks (risk identification), to comprehend the nature of risk and to determine the level of risk (risk analysis), and of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable (risk evaluation).

3.7. "Safe state" means an operating mode in case of a failure of an item without an unreasonable level of risk.

3.8. "Software" means the part of an Electronic Control System that consists of digital data and instruction.

3.9. "Software update" means a package used to upgrade software to a new version including a change of the configuration parameters.

3.10. "System" means a set of components and/or sub-systems that implement a function of functions.

3.11. "Threat" means a potential cause of an unwanted incident, which may result in harm to a system, organization or individual.

3.12. "Vehicle user" means a person operating or driving the vehicle, a vehicle owner, an authorised representative or employee of a fleet manager, an authorised representative or employee of the vehicle manufacturer, or an authorized technician.

3.13. "Vulnerability" means a weakness of an asset or mitigation that can be exploited by one or more threats.

**Annex 1**

**List of threats and corresponding mitigations**

1. This annex consists of three parts. Part A of this annex describes the baseline for threats, vulnerabilities and attack methods. Part B of this annex describes mitigations to the threats which are intended for vehicle types. Part C describes mitigations to the threats which are intended for areas outside of vehicles, e.g. on IT backends.

2. Part A, Part B, and Part C shall be considered for risk assessment and mitigations to be implemented by vehicle manufacturers.

3. The high-level vulnerability and its corresponding examples have been indexed in Part A. The same indexing has been referenced in the tables in Parts B and C to link each of the attack/vulnerability with a list of corresponding mitigation measures.

4. The threat analysis shall also consider possible attack impacts. These may help ascertain the severity of a risk and identify additional risks. Possible attack impacts may include:

(a) Safe operation of vehicle affected;

(b) Vehicle functions stop working;

(c) Software modified, performance altered;

(d) Software altered but no operational effects;

(e) Data integrity breach;

(f) Data confidentiality breach;

(g) Loss of data availability;

(h) Other, including criminality.

**Part A. Vulnerability or attack method related to the threats**

1. High level descriptions of threats and relating vulnerability or attack method are listed in Table A1.

Table A1

**List of vulnerability or attack method related to the threats**

| *High level and sub-level descriptions of vulnerability/ threat* | | | *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) |
| 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 introductionof 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 |
| 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 |
| 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** tounintentionally load malware or enable an attack |
| 15.2 | **Defined security procedures** are not followed |
| 4.3.5 Threats to vehicles regarding their external connectivity and connections | 16 | Manipulation of the connectivity of vehicle functions enables a cyber-attack, this can include telematics; systems that permit remote operations; and systems using short range wireless communications | 16.1 | Manipulation of **functions designed to remotely operate systems**, such as remote key, immobilizer, and charging pile |
| 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** |
| 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 | 22.2 | 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 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 |
| 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  **Replacement of authorized electronic hardware** (e.g., sensors) with unauthorized electronic hardware  **Manipulation of the information** collected by a sensor (for example, using a magnet to tamper with the Hall effect sensor connected to the gearbox) |

**Part B. Mitigations to the threats intended for vehicles**

1. Mitigations for "Vehicle communication channels"

Mitigations to the threats which are related to "Vehicle communication channels" are listed in Table B1.

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  M6 | The vehicle shall verify the authenticity and integrity of messages it receives  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  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) |
| 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 |
| 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) |

2. Mitigations for "Update process"

Mitigations to the threats which are related to "Update process" are listed in Table B2.

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 the system 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 |

3. Mitigations for "Unintended human actions facilitating a cyber attack"

Mitigations to the threats which are related to "Unintended human actions facilitating a cyber attack" are listed in Table B3.

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 |

4. Mitigations for "External connectivity and connections"

Mitigations to the threats which are related to "external connectivity and connections" are listed in Table B4.

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.  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 |

5. Mitigations for "Potential targets of, or motivations for, an attack "

Mitigations to the threats which are related to "Potential targets of, or motivations for, an attack " are listed in Table B5.

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 ofSecurity 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.  Data manipulation attacks on sensors or transmitted data could be mitigated by correlating the data from different sources of information |
| 20.4 | Data manipulation to falsify vehicle’s driving data (e.g. mileage, driving speed, driving directions, etc.) |
| 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 |
| 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 | M13 | 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. | M7 | 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. |

6. Mitigations for "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened"

Mitigations to the threats which are related to "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened" are listed in Table B6.

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.  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 |
| 29.1 | Superfluous internet ports left open, providing access to network systems |
| 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.  Cybersecurity best practices for system design and system integration shall be followed |

7. Mitigations for "Data loss / data breach from vehicle"

Mitigations to the threats which are related to "Data loss / data breach from vehicle" are listed in Table B7.

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. |

8. Mitigations for "Physical manipulation of systems to enable an attack"

Mitigation to the threats which are related to "Physical manipulation of systems to enable an attack" are listed in Table B8.

Table B8   
**Mitigations to the threats which are related to "Physical manipulation of systems to enable an attack"**

|  |  |  |  |
| --- | --- | --- | --- |
| *Table A1 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 |

**Part C. Mitigations to the threats outside of vehicles**

1. Mitigations for "Back-end servers"

Mitigations to the threats which are related to "Back-end servers" are listed in Table C1.

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 Security Controls can be found in OWASP |

2. Mitigations for "Unintended human actions"

Mitigations to the threats which are related to "Unintended human actions" are listed in Table C2.

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 |