Attachment 96 Cyber security and cyber security management system

Refer to: R155 00 Series

96.1 Effective date and Scope

96.1.1 Effective date from 2028/1/1, new vehicle types of category M and N, and from 2030/1/1, all vehicle types of category M and N, shall complied with this regulation.

96.1.2 Effective date from 2028/1/1, new vehicle types of category O, and from 2030/1/1, all vehicle types of category O, if fitted with at least one electronic control unit, shall complied with this regulation.

96.1.3 This Regulation is without prejudice to other attachment of this regulation, regional or national legislations governing the access by authorized parties to the vehicle, its data, functions and resources, and conditions of such access. It is also without prejudice to the application of national and regional legislation on privacy and the protection of natural persons with regard to the processing of their personal data.

96.1.4 This Regulation is without prejudice to other attachment of this regulation, national or regional legislation governing the development and installation/system integration of replacement parts and components, physical and digital, with regards to cybersecurity.

96.1.5 Except for large passenger vehicles and child-only vehicles, the vehicle that the applicant applying for low volume safety type approval may be exempt from this attachment.

96.1.6 The vehicle that the applicant applying for vehicle-by-vehicle low volume safety type approval, may be exempt from this attachment.

96.1.7 Technical Service can carry out test according to UN Regulations that this direction harmonized with: UN R155 00 Series of amendments and following amendments of above-mentioned regulations.

96.2 Definitions

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

components.

96.2.2 "Cyber Security Management System (CSMS)" means a systematic risk-based approach defining organisational processes, responsibilities and governance to treat risk associated with cyber threats to vehicles and protect them from cyber-attacks.

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

96.2.4 "Development phase" means the period before a vehicle type is type approved.

96.2.5 "Production phase" refers to the duration of production of a vehicle type.

96.2.6 "Post-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.

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

96.2.8 "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.

96.2.9 "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).

96.2.10 "Risk Management" means coordinated activities to direct and control an organization with regard to risk.

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

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

96.3 The principles of applicable type and scope of Cyber security and cyber security management system shall be as follows:

96.3.1 Same vehicle brand.

96.3.2 Same essential aspects of the electric/electronic architecture and external interfaces with respect to cyber security

96.4 Certificate of Compliance for Cyber Security Management System

96.4.1 Applicants shall provide undermentioned documents with specific context in triplicate to apply to certification institution for “certificate of compliance for cyber security management system”, certification institution would issue “Certificate of Compliance for Cyber Security Management System” after evaluation of applicant :

96.4.1.1 Documents describing the Cyber Security Management System.

96.4.1.2 A signed declaration of compliance for Cyber Security Management System.

96.4.2 In the context of the assessment, the applicant shall provide declaration and demonstrate to the satisfaction of the certification institution or technical service that they have the necessary processes to comply with all the requirements for cyber security according to this Regulation.

96.4.3 When this assessment has been satisfactorily completed and in receipt of a signed declaration from the applicant, a certificate named Certificate of Compliance for CSMS (hereinafter the Certificate of Compliance for CSMS) shall be granted to the applicant.

96.4.4 The certification institution or technical service shall use the model set out in this Regulation for the Certificate of Compliance for CSMS.

96.4.5 The Certificate of Compliance for CSMS shall remain valid for a maximum of three years from the date of deliverance of the certificate unless it is withdrawn.

96.4.6 The certification institution which has granted the Certificate of Compliance for CSMS may at any time verify that the requirements for it continue to be met. The certification institution shall withdraw the Certificate of Compliance for CSMS if the requirements laid down in this Regulation are no longer met.

96.4.7 The applicant shall inform the certification institution or technical service of any change that will affect the relevance of the Certificate of Compliance for CSMS. After consultation with the applicant, the certification institution or technical service shall decide whether new

checks are necessary.

96.4.8 In due time, permitting the certification institution to complete its assessment before the end of the period of validity of the Certificate of Compliance for CSMS, the applicant shall apply for a new or for the extension of the existing Certificate of Compliance for CSMS. The certification institution shall, subject to a positive assessment, issue a new Certificate of Compliance for CSMS or extend its validity for a further period of three years. The certification institution shall verify that the CSMS continue to comply with the requirements of this Regulation. The certification institution shall issue a new certificate in cases where changes have been brought to the attention of the certification institution or technical service and the changes have been positively re-assessed.

96.4.9 The expiry or withdrawal of the applicant's Certificate of Compliance for CSMS shall be considered, with regard to the vehicle types to which the CSMS concerned was relevant, as modification of approval, which may include the withdrawal of the approval if the conditions for granting the approval are not met anymore.

96.5 Specifications

96.5.1 General specifications

96.5.1.1 The requirements of this attachment shall not restrict provisions or requirements of other attachment in this Regulation.

96.5.2 Requirements for the Cyber Security Management System

96.5.2.1 For the assessment the certification institution or technical service shall verify that the applicant has a Cyber Security Management System in place and shall verify its compliance with this Regulation.

96.5.2.2 The Cyber Security Management System shall cover the following aspects:

96.5.2.2.1 The applicant shall demonstrate to an certification institution or technical service that their Cyber Security Management System applies to the following phases:

(a) Development phase;

(b) Production phase;

(c) Post-production phase.

96.5.2.2.2 The applicant shall demonstrate that the processes used within their Cyber Security Management System ensure security is adequately considered, including risks and mitigations listed in paragraph 96.6. This shall include:

(a) The processes used within the applicant's organization to manage cyber security;

(b) The processes used for the identification of risks to vehicle types. Within these processes, the threats in paragraph 96.6, Part A, and other relevant threats shall be considered;

(c) The processes used for the assessment, categorization and treatment of the risks identified;

(d) The processes in place to verify that the risks identified are appropriately managed;

(e) The processes used for testing the cyber security of a vehicle type;

(f) The processes used for ensuring that the risk assessment is kept current;

(g) The processes used to monitor for, detect and respond to cyber-attacks, cyber threats and vulnerabilities on vehicle types and the processes used to assess whether the cyber security measures implemented are still effective in the light of new cyber threats and vulnerabilities that have been identified.

(h) The processes used to provide relevant data to support analysis of attempted or successful cyber-attacks.

96.5.2.2.3 The applicant shall demonstrate that the processes used within their Cyber Security Management System will ensure that, based on categorization referred to in paragraph 96.5.2.2.2 (c) and 96.5.2.2.2 (g), cyber threats and vulnerabilities which require a response from the applicant shall be mitigated within a reasonable timeframe.

96.5.2.2.4 The applicant shall demonstrate that the processes used within their Cyber Security Management System will ensure that the monitoring referred to in paragraph 96.5.2.2.2 (g) shall be continual. This shall:

(a) Include vehicles after first registration in the monitoring;

(b) Include the capability to analyse and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs. This capability shall respect paragraph 96.1.3. and the privacy rights of car owners or drivers, particularly with respect to consent.

96.5.2.2.5 The applicant shall be required to demonstrate how their Cyber Security Management System will manage dependencies that may exist with contracted suppliers, service providers or applicant's sub-organizations in regards of the requirements of paragraph 96.5.2.2.2.

96.5.3 Requirements for vehicle types

96.5.3.1 The applicant shall have a valid Certificate of Compliance for the Cyber Security Management System relevant to the vehicle type being approved.

96.5.3.2 The applicant shall identify and manage, for the vehicle type being approved, supplier-related risks.

96.5.3.3 The applicant shall identify the critical elements of the vehicle type and perform an exhaustive risk assessment for the vehicle type and shall treat/manage the identified risks appropriately. The risk assessment shall consider the individual elements of the vehicle type and their interactions. The risk assessment shall further consider interactions with any external systems. While assessing the risks, the applicant shall consider the risks related to all the threats referred to in paragraph 96.6, Part A, as well as any other relevant risk.

96.5.3.4 The applicant shall protect the vehicle type against risks identified in the applicant's risk assessment. Proportionate mitigations shall be implemented to protect the vehicle type. The mitigations implemented shall include all mitigations referred to in paragraph 96.6, Part B and C which are relevant for the risks identified. However, if a mitigation referred to in paragraph 96.6, Part B or C, is not relevant or not sufficient for the risk identified, the applicant shall ensure that another appropriate mitigation is implemented.

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

96.5.3.6 The applicant shall perform, prior to type approval, appropriate and sufficient testing to verify the effectiveness of the security measures implemented.

96.5.3.7 The applicant shall implement measures for the vehicle type to:

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

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

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

96.5.3.8 Cryptographic modules used for the purpose of this attachment shall be in line with consensus standards. If the cryptographic modules used are not in line with consensus standards, then the applicant shall justify their use.

96.5.4 Reporting provisions

96.5.4.1 The applicant shall report at least once a year, or more frequently if relevant, to the certification institution or the technical service the outcome of their monitoring activities, as defined in paragraph 96.5.2.2.2.(g)), this shall include relevant information on new cyber-attacks. The applicant shall also report and confirm to the certification institution or the technical service that the cyber security mitigations implemented for their vehicle types are still effective and any additional actions taken.

96.5.4.2 The certification institution or the technical service shall verify the provided information and, if necessary, require the applicant to remedy any detected ineffectiveness.

If the reporting or response is not sufficient the certification institution may decide to withdraw the CSMS in compliance with paragraph 96.4.6.

96.6 List of threats and corresponding Mitigations

96.6.1 This paragraph consists of three parts. Part A describes the baseline for threats, vulnerabilities and attack methods. Part B 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.

96.6.2 Part A, Part B, and Part C shall be considered for risk assessment and mitigations to be implemented by applicant.

96.6.3 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.

96.6.4 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.

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

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

Table 1 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	5.1	Communications channels permit **code injection**, for example tampered software binary might be injected into the communication stream

High level and sub-level descriptions of vulnerability/ threat			*Example of vulnerability or attack method*	
		unauthorized manipulation, deletion or other amendments to vehicle held code/data	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
	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

High level and sub-level descriptions of vulnerability/ threat			*Example of vulnerability or attack method*	
	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	15	Legitimate actors are able to take actions that would	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

High level and sub-level descriptions of vulnerability/ threat			*Example of vulnerability or attack method*	
unintended human actions facilitating a cyber attack		unwittingly facilitate a cyber-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)

High level and sub-level descriptions of vulnerability/ threat			*Example of vulnerability or attack method*	
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, applicant 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.

High level and sub-level descriptions of vulnerability/ threat			*Example of vulnerability or attack method*	
			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

High level and sub-level descriptions of vulnerability/ threat			*Example of vulnerability or attack method*	
	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)

96.6.6 Part B. Mitigations to the threats intended for vehicles

96.6.6.1 Mitigations for "Vehicle communication channels"

Mitigations to the threats which are related to "Vehicle communication channels" are listed in Table 2.

Table ~~2~~ Mitigation to the threats which are related to "Vehicle communication channels"

Table 1 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)

Table 1 reference	*Threats to "Vehicle communication channels"*	*Ref*	*Mitigation*
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

Table 1 reference	*Threats to "Vehicle communication channels"*	*Ref*	*Mitigation*
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

Table 1 reference	*Threats to "Vehicle communication channels"*	*Ref*	*Mitigation*
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)		

96.6.6.2 Mitigations for "Update process"

Mitigations to the threats which are related to "Update process" are listed in Table 3

Table 3 Mitigations to the threats which are related to "Update process"

Table 1 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

Table 1 reference	*Threats to "Update process"*	*Ref*	*Mitigation*
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

96.6.6.3 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 4.

Table 4 Mitigations to the threats which are related to "Unintended human actions facilitating a cyber attack"

Table 1 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

96.6.6.4 Mitigations for "External connectivity and connections"

Mitigations to the threats which are related to "external connectivity and connections" are listed in Table 5.

Table 5 Mitigation to the threats which are related to "external connectivity and connections"

Table 1 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		

Table 1 reference	*Threats to "External connectivity and connections"*	*Ref*	*Mitigation*
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

96.6.6.5 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 6.

Table 6 Mitigations to the threats which are related to "Potential targets of, or motivations for, an attack"

Table 1 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

Table 1 reference	*Threats to "Potential targets of, or motivations for, an attack"*	*Ref*	*Mitigation*
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, applicant 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.

Table 1 reference	*Threats to "Potential targets of, or motivations for, an attack"*	*Ref*	*Mitigation*
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.		

96.6.6.6 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 7.

Table 7 Mitigations to the threats which are related to "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened"

Table 1 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		

Table 1 reference	*Threats to "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened"*	*Ref*	*Mitigation*
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

96.6.6.7 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 8.

Table 8 Mitigations to the threats which are related to "Data loss / data breach from vehicle"

Table 1 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.

96.6.6.8 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 9.

Table 9 Mitigations to the threats which are related to "Physical manipulation of systems to enable an attack"

Table 1 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

96.6.7 Part C. Mitigations to the threats outside of vehicles

96.6.7.1 Mitigations for "Back-end servers"

Mitigations to the threats which are related to "Back-end servers" are listed in Table 10.

Table 10 Mitigations to the threats which are related to "Back-end servers"

Table 1 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

Table 1 reference	*Threats to "Back-end servers"*	*Ref*	*Mitigation*
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

96.6.7.2 Mitigations for "Unintended human actions"

Mitigations to the threats which are related to "Unintended human actions" are listed in Table 11.

Table 11 Mitigations to the threats which are related to "Unintended human actions"

Table 1 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

Table 1 reference	*Threats relating to "Unintended human actions"*	*Ref*	*Mitigation*
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

96.6.7.3 Mitigations for "Physical loss of data"

Mitigations to the threats which are related to "Physical loss of data" are listed in Table 12.

Table 12 Mitigations to the threats which are related to "Physical loss of data loss"

Table 1 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)		