Submitted by the experts from European Commission

Informal document **GRVA-02-37**
2nd GRVA session, 28 January – 1 February 2019
Agenda item 5(b)

Comments on ECE/TRANS/WP29/GVA/2019/2

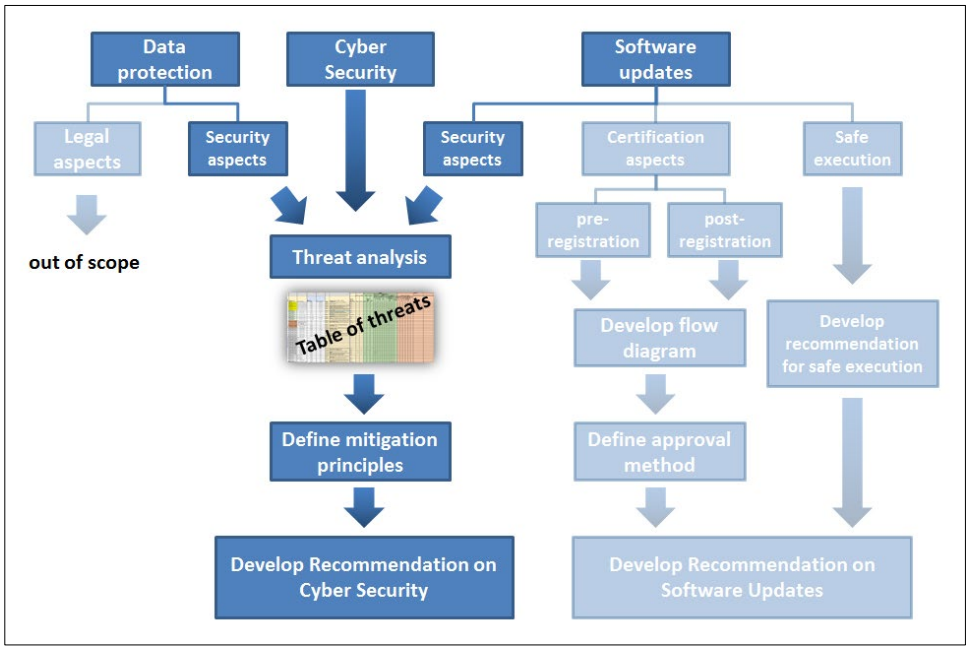
The Commission intends to regulate vehicle cybersecurity and therefore welcomes in principle this recommendation and the proposed test phase. The document has been subject to a first review internally, which is however not final. . It is in particular intended to check that this proposal is not in contradiction with the EU legislation on access to vehicle data by independent operators. The Commission would like to submit the initial comments/questions hereafter to be reviewed by the task force. Comments/questions are shown in balloons (track change mode).

A. Preamble

1.1. A Task Force was established as a subgroup of the Informal Working Group on Intelligent Transport Systems / Automated Driving (IWG on ITS/AD) of WP.29 to address Cyber Security and Over-the-air issues. The task force consisted of members of representatives from contracting parties and non-governmental organizations, e.g. the European Association of Automotive Suppliers (CLEPA), the International Motor Vehicle Inspection Committee (CITA), la Fédération Internationale de l'Automobile (FIA), the International Telecommunication Union (ITU) and the International Organization of Motor Vehicle Manufacturers (OICA).

1.2. The scope of what is covered in this recommendation is illustrated by figure 1. It is noted that there are commonalities between data protection, cyber security and software updates. Software updates have security aspects, certification aspects and aspects for safe execution that need to be considered. The Task Force determined that Cyber Security and Over-the-air issues were distinct topics to be assessed separately. This is the output of the Cyber Security considerations, including the security of software updates. A separate paper, named "Recommendation on Over-the-air issues of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 IWG ITS/AD", considers managing software updates and type approval processes.

Figure 1.
Task Force activities and deliverables



1.3. The work of the Task Force took into account the document ECE/TRANS/WP.29/2017/46 titled "Guideline on cybersecurity and data protection", developed by the IWG on ITS/AD and other relevant standards, practice(s), directives and regulations concerning cyber security. This includes some that are under development, as well as existing standards that are applicable to the automotive industry. These are referenced in Annex D.

1.4. This paper reflects the state-of-the-art approaches at the time of developing the paper. Therefore, the recommendations herein need to be reviewed periodically to ensure they address new and emerging threats and mitigations, and are updated where necessary. GRVA needs to oversee and initiate the reviews.

B. Scope

1.5. This paper defines principles to address key cyber threats and vulnerabilities identified in order to assure vehicle safety in case of cyber-attacks. It further defines detailed guidance or measures for how to meet these principles. This includes examples of processes and technical approaches. Finally it considers what assessments or evidence may be required to demonstrate compliance or certification with any requirements identified.

1.6. Vehicles process a range of different types of data. The paper defines principles to be achieved to protect this data from unauthorized access, amendment or deletion both when it is stored and when it is transmitted.

C. Approach

1.7. An assessment was made to identify key threats and vulnerabilities to vehicles, and then identified the key mitigations that are required to reduce or minimise them. It is by intent that the outcome does not prescribe specific technical solutions (although they may be cited as examples). The key mitigations were then presented as principles.

1.8. A threat analysis was undertaken according the state-of-the-art. A list of threats was identified from multiple sources (refer to Annex B). The resulting list is not to be considered exhaustive but is highly illustrative of possible cyber threats posed to vehicles. It considers how these threats may be manifested and specific examples of how they might affect a vehicle.

1.9. The threats were clustered based on sharing similar characteristics, and for the clusters a list of mitigations were identified. These provide one or more ways that the threat examples identified could be mitigated. A number of reference documents were used to identify these mitigations (refer to Annex C). The mitigations were defined as principles that need to be achieved; in some cases specific solutions are provided as examples of how the principles might be achieved but there is no intention these should be incorporated into regulation.

II. Definitions

2. For the purpose of this recommendation the following definitions shall apply:

2.1 "*Aftermarket*" means the secondary market of the automotive industry, concerned with the manufacturing, remanufacturing, distribution, retailing, and installation of all vehicle parts, software, services, chemicals, equipment, and accessories, after the sale of the automobile by the vehicle manufacturer to the customer.

2.2. "*Authentication*" means a provision of assurance that a claimed characteristic of an entity is correct.

2.3. "*Access*" means obtaining the use of a resource.

2.4. "*Automotive industry*" means vehicle manufacturers, suppliers, maintenance providers and providers of systems and services that interact with the vehicles.

2.5. "*Cyber Security*" means the condition in which road vehicles and their functions are protected against threats to electrical or electronic components.

2.6. "*Cyber Security Management System (CSMS)*" means a systematic risk-based approach defining organisational processes, responsibilities and governance to mitigate cyber threats and protect vehicles from cyber-attacks.

2.7. "*Data protection*" means the implementation of appropriate administrative, technical or physical means to guard against unauthorized intentional or accidental disclosure, modification, or destruction of data.

2.8. "*Defence-in-depth*" means a system with multiple levels of protection that maintains a total protection level even in the event of failure or penetration of a single protection level.

2.9. "*Lifecycle*" means the span of a vehicle's existence from its initial development through the period of marketing and active use to eventual obsolescence.

2.10. "*Lifetime*" means the lifetime of a vehicle with regard to cyber security is the period from 1st registration of the vehicle until it is decommissioned.

2.11. "*Mitigation*" means a measure that is modifying risk.

2.12. "*Organisation*" means a person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives.

2.13. "*Over-The-Air update*" means any method of making data transfers wirelessly instead of using a cable or other local connection.

2.14. "*Risk*" means the effect of uncertainty on security objectives.

2.15. "*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).

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

2.17. "*System*" means a set of components or sub-systems that implements a feature.

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

2.19. "*Vulnerability*" means a weakness of an asset or control that can be exploited by one or more threats.

III. Cyber security principles

3.1. Cyber security principles can be used to demonstrate how organisations should implement cyber security over the lifecycle of the vehicle. They can be used by vehicle manufacturers, sub-contractors, suppliers and service providers.

3.2. Demonstration of how these principles can be met is not explicitly defined in this paper. Instead it is recommended that through the use of relevant standards (such as ISO/SAE 21434), processes and implementing appropriate mitigations organisations should be able to evidence how they are meeting the principles corresponding to requests from authorities.

3.3. The cyber security principles are:

3.3.1. Organisational security should be owned, governed and promoted at the highest organizational level;

3.3.2. Security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain;

3.3.3. Organizations should implement cyber security monitoring and incident response to ensure systems are secure over their lifetime;

3.3.4. All organisations, including sub-contractors, suppliers and potential 3rd parties, should work together to enhance the security of the system;

3.3.5. The vehicle should be designed using a defence-in-depth approach. The vehicle manufacturer should design the vehicle architecture to reduce the likelihood that compromise of assets within one architectural element would result in propagation of the attack to other architectural elements;

3.3.6. The security of software should be managed throughout the lifetime of the vehicle;

3.3.7. The storage and transmission of data should be secure and should be controlled;

3.3.8. The vehicle manufacturer should assess security functions with testing procedures;

3.3.9. The vehicle should be designed to be resilient to cyber attacks;

3.3.10. The vehicle should be designed with the capability to detect cyber attacks and respond appropriately;

3.3.11. Access to vehicle services and functions should be controlled and available only to authorized parties;

3.3.12. Access to personal data of drivers and passengers should be controlled and available only to authorized parties;

3.3.13. Vehicles should log relevant data, which can be used for post incident analysis and forensics.

IV. Threats to vehicles

4.1. The threats identified in this paper may be used by parties engaged in introducing, designing or modifying products or services which are part of or interact with vehicles. The threats listed represent the state of the art when written but will need to be re-evaluated for completeness when used. They should be used as a basis for ensuring risks are adequately mitigated. They can be used to help determine vulnerabilities to potential cyber threats and ensure that appropriate measures are in place how to mitigate these risks.

4.2. This section provides details of threats and vulnerabilities that may exist. A more detailed list of possible threat examples that could be used are provided in Annex B.

4.3. The following provides a level description of possible threats and vulnerabilities which shall be considered in the design of a new or modified product or service. The numbers provided for each bullet provide a cross-reference to how they are referred to in Annex B:

4.3.1. Threats regarding back-end servers:

(a) Back-end servers used as a means to attack a vehicle or extract data (1.);

(b) Services from back-end server being disrupted, affecting the operation of a vehicle (2.);

(c) Data held on back-end servers being lost or compromised ("data breach") (3.).

4.3.2. Threats to vehicles regarding their communication channels:

(a) Spoofing of messages or data received by the vehicle (4.);

(b) Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle held code/data (5.);

(c) Communication channels permit untrusted/unreliable messages to be accepted or are vulnerable to session hijacking/replay attacks (6.);

(d) Information can be readily disclosed. For example through eavesdropping on communications or through allowing unauthorized access to sensitive files or folders (7.);

(e) Denial of service attacks via communication channels to disrupt vehicle functions (8.);

(f) An unprivileged user is able to gain privileged access to vehicle systems (9.);

(g) Viruses embedded in communication media are able to infect vehicle systems (10.);

(h) Messages received by the vehicle (for example X2V or diagnostic messages), or transmitted within it, contain malicious content (11.).

4.3.3. Threats to vehicles regarding their update procedures:

(a) Misuse or compromise of update procedures (12.);

(b) It is possible to deny legitimate updates (13.).

4.3.4. Threats to vehicles regarding unintended human actions:

(a) Misconfiguration of equipment or systems by legitimate actor, e.g. owner or maintenance community (14.);

(b) Legitimate actors are able to take actions that would unwittingly facilitate a cyber-attack (15.).

4.3.5. Threats to vehicles regarding their external connectivity and connections:

(a) 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.);

(b) Hosted third party software, e.g. entertainment applications, used as a means to attack vehicle systems (17.);

(c) Devices connected to external interfaces e.g. USB ports, OBD port, used as a means to attack vehicle systems (18.).

4.3.6. Potential targets of, or motivations for, an attack:

(a) Extraction of vehicle data/code (19.);

(b) Manipulation of vehicle data/code (20.);

(c) Erasure of data/code (21.);

(d) Introduction of malware (22.);

(e) Introduction of new software or overwrite of existing software (23.);

(f) Disruption of systems or operations (24.);

(g) Manipulation of vehicle parameters (25.).

4.3.7. Potential vulnerabilities that could be exploited if not sufficiently protected or hardened:

(a) Cryptographic technologies can be compromised or are insufficiently applied (26.);

(b) Component parts or supplies could be compromised to permit vehicles to be attacked (27.);

(c) Software or hardware development permits vulnerabilities (28.);

(d) Network design introduces vulnerabilities (29.);

(e) Physical loss of data can occur (30.);

(f) Unintended transfer of data can occur (31.);

(g) Physical manipulation of systems can enable an attack (32.).

4.3.8. The threat analysis shall also consider possible attack outcomes. These may help ascertain the severity of a risk and identify additional risks. Possible attack outcomes 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.

4.4. More detailed examples of vulnerabilities or attack methodologies are given against each entry in table 1 of Annex B. This may be used to further understand the entries above. It is anticipated that new and unforeseen examples of vulnerability and attack methodologies will emerge over time. Therefore, neither the list above nor the examples should be considered to be an exhaustive list.

V. Mitigations

5.1. This section provides a list of measures which shall be considered in the design of a new or modified product or service in order to mitigate identified threats and risks. Within this list there are entries described as "shall" which are mandatory considerations whereas those described as "should" will be considered if applicable.

5.1.1. Security controls shall be applied to back-end systems to minimize the risk of insider attack

5.1.2. Security controls shall be applied to back-end systems to minimize unauthorized access

5.1.3. Where back-end servers are critical to the provision of services there shall be recovery measures in case of system outage

5.1.4. Security controls shall be applied to minimize risks associated with cloud computing

5.1.5. Security controls shall be applied to back-end systems to prevent data breaches

5.1.6. The principle of security by design shall be adopted to minimise the impact of an attack on the vehicle

5.1.7. Access control techniques and designs shall be applied to protect system data/code

5.1.8. Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data

5.1.9. Measures to prevent and detect unauthorized access shall be employed

5.1.10. The vehicle shall verify the authenticity and integrity of messages it receives

5.1.11 Security controls shall be implemented for storing cryptographic keys

5.1.12. Confidential data transmitted to or from the vehicle shall be protected

5.1.13. Measures to detect and recover from a denial of service attack should be considered

5.1.14. Measures to protect systems against embedded viruses/malware should be considered

5.1.15. Measures to detect malicious internal messages or activity should be considered

5.1.16. Secure software update procedures shall be employed

5.1.17. Measures shall be implemented for defining and controlling maintenance procedures

5.1.18. Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege

5.1.19. Organizations shall ensure security procedures are defined and followed

5.1.20. Security controls shall be applied to systems that have remote access

5.1.21. Software shall be security assessed, authenticated and integrity protected

5.1.22. Security controls shall be applied to external interfaces

5.1.23. Cybersecurity best practices for software and hardware development shall be followed

5.1.24. Data protection best practices shall be followed for storing private and sensitive data

5.1.25. Systems should be designed to respond appropriately if an attack on a vehicle is detected.

5.1.25. The systems should log relevant information, which can be used for post-incident analysis.

5.2. Annex B and C provide examples of mitigations that may be used. These are not exhaustive and may not be applicable for the specific implementation of a given product or service.

5.3. To help identify specific mitigations, each threat example may be assessed by means of the "Extended CIA". During this assessment it should be considered how an attack relating to the threat or vulnerability could be initiated and propagated through a vehicle's networks. The extended CIA identifies seven objectives:

(a) Confidentiality;

(b) Integrity;

(c) Availability;

(d) Non-repudiation;

(e) Authenticity;

(f) Accountability;

(g) Authorization.

VI. Requirements for cyber security processes and how to evidence their application

6.1. This section describes how a vehicle manufacturer shall evidence to an authority how they have considered the threats, mitigations and principles applicable to their products in order for the authority to certify compliance.

6.2. The section does not specify how the vehicle manufacturer should gather the necessary information. It may be internal to the organisation, or require interaction between different organisations in a supply chain (for example manufacturer and supplier).

6.3. Cyber Security Management System certification

6.3.1. A Cyber Security Management System shall be implemented by the vehicle manufacturer.

6.3.2. Suppliers and service providers shall implement a Cyber Security Management System.

6.3.3. Suppliers and service providers shall be able to provide evidence about the implementation of their Cyber Security Management System to a vehicle manufacturer.

6.3.4. The vehicle manufacturer shall demonstrate to an authority that their Cyber Security Management System considers the following phases:

6.3.4.1 Development phase;

6.3.4.2. Production phase;

6.3.4.3. Post-production phase.

6.3.5. The vehicle manufacturer shall demonstrate to an authority how their Cyber Security Management System will manage dependencies that may exist with contracted suppliers and service providers.

6.3.6. The vehicle manufacturer shall have processes for monitoring risks and threats to the vehicle and incident response processes defined within their Cyber Security Management System.

6.4. Requirements for post vehicle production:

6.4.1. Cyber security measures shall be integrated into the lifecycle of a vehicle.

6.4.2. The vehicle manufacturer shall demonstrate how they plan to maintain adequate protection and adherence to the cyber security principles outlined in this document over the lifecycle of vehicles. This capability is required so that they can demonstrate that the safety and availability of their vehicle and system functions will be maintained in the face of changing cyber threats. This is particularly important for safety critical systems, including type approved systems.

6.4.3. Organizations within the automotive industry shall have the capability to identify how threats and vulnerabilities to vehicles or systems change over time and to identify threats that were not identified or accounted for in the development stage.

6.4.4. Organizations within the automotive industry shall have the capability to assess whether the security measures implemented are still effective in the light of new cyber threats or vulnerabilities that they have identified. This should consider whether the safety or availability of the vehicle, or its functions, are affected.

6.4.5. Organizations within the automotive industry shall have incident response processes.

6.5. Approval of vehicle type:

6.5.1. Approval of vehicle type shall only take place if the vehicle manufacturers Cyber Security Management System has a current CSMS Certificate of Compliance.

6.5.2. The vehicle manufacturer shall demonstrate that a risk assessment has been performed for the vehicle type in terms of the vehicle systems, the interactions of the different vehicle systems and the entire vehicle.

6.5.3. The vehicle manufacturer shall ensure the design of critical elements of the vehicle to mitigate the risks identified in the vehicle manufacturer's risk assessment. Proportionate mitigations measures shall be implemented to protect such elements and related assets.

6.5.4. The vehicle manufacturer shall implement appropriate and proportionate measures to protect dedicated environments (if provided) for the storage and execution of aftermarket software, services, applications or data.

6.5.5. The evidence required for vehicle approval shall include:

6.5.5.1. How the vehicle manufacturer has considered threats and vulnerabilities, including those detailed in Annex A, within their risk assessments;

6.5.5.1. What mitigations the vehicle manufacturer has implemented to minimise the risks to a level acceptable to the authority through describing:

(a) The vehicle architecture and systems;

(b) The significant components of the architecture and its (sub-)systems that are relevant to cyber security;

(c) The interactions of those architectures and systems with other vehicle architectures, systems and external interfaces;

(d) The risks posed to those architectures and systems that have been identified in the risk assessment;

(e) The mitigations that have been implemented on the systems listed and how they address the stated risks.

6.5.6. How the vehicle manufacturer has implemented the cyber security principles identified in this document may also be provided as an evidence for type approval.

VII. Conclusion and recommendation for further proceedings

7.1. The conclusion of this recommendation is that:

7.1.1. The assessment has drawn upon bodies of work and the knowledge and experience of stakeholders (see Annex D) to provide a recommendation on cyber security. The Task Force considers that it has fulfilled its Terms of Reference;

7.1.2. Specifying technical solutions would be inappropriate as these would not stand the test of time and would stifle innovation and competition. Therefore, this recommendation does not do so, instead it includes examples of processes, procedures and technologies that could be considered for cyber security;

7.1.3. Demonstration of how the requirements, given in this recommendation, can be met should not be explicitly defined. Instead it is recommended that through the use of relevant standards, processes and implementing appropriate mitigations vehicle manufacturer should be able to evidence how they are meeting the requirements to the approval authority;

7.1.4. The scope of this recommendation covers the lifecycle of the vehicle. How it is removed from operation and what happens to the vehicle after that point is out of scope of this recommendation.

7.2. In order to regulate the cyber security framework described in this document, the following would be needed:

7.2.1. A verification by an approval authority that the processes and procedures of a vehicle manufacturer (as described in its Cyber Security Management System) shall support the implementation of the recommendations of this document.

7.2.2. An approval by an approval authority that the risks identified to a specific vehicle type have been appropriately assessed and that the mitigations implemented to address those risks are suitable.

7.3. To aid the assessment of the Cyber Security Management System, the risk analysis undertaken and the implementation of the mitigations techniques, the recommendation includes:

7.3.1. Cyber security principles which can be used to demonstrate how organisations should implement cyber security over the lifetime of the vehicle;

7.3.2. Examples of threats, risks, vulnerabilities and attack outcomes that should be considered;

7.3.3. Examples of mitigations tecniques that should be considered.

7.4. It is anticipated that new and unforeseen examples of vulnerabilities and attack methodologies will emerge over time. Therefore, the examples provided should not be considered an exhaustive list nor a list that is applicable to every vehicle design, instead they will need to be evaluated for completeness and applicability when used.

7.5. The task force recommends that this paper is taken forward as two parts:

7.5.1. The main text (chapters 1 to 6) and Annexes B and C are taken forward as an official working document for WP.29. Furthermore, it could be used as a basis for

a Resolution on Cyber Security, but may need further revision to comply with the format required;

7.5.2. Annex A is taken forward as a UN Regulation, according to the 1958 Agreement, which addresses the recommendations made in paragraph 7.2. above. It includes requirements for:

7.5.2.1. A CSMS Certificate of Compliance for the Cyber Security Management System of the vehicle manufacturer.

7.5.2.2. Vehicle type approval with regard to cyber security.

7.5.3. Annex C may be useful for stakeholders as a reference document. It is not suitable for the UN Regulation as it is informative.

7.5.4. Annex D is not suitable for Regulation or Resolution. It is solely for this document.

7.5.5. The parent group should decide on next steps, e.g. on developing a GTR on Cyber Security. The task force notes that the development of a GTR will require further work.

7.5.6. For the regulatory annex categories L, O, R, S and T could be included but have had limited representation in the task force (in the case of category L) or no representation (in the other cases). It should therefore be considered whether the regulations should apply to these categories of vehicles.

7.5.7. The regulatory annex proposes that the length of time of duration of the CSMS Certificate of Compliance should be three years and the conformity of production checks should also be conducted every three years.

7.5.8. The task force recommends that provisions in the proposed Regulation (Annex A) should be checked to verify that they are legally permissible under the 1958 Agreement. In particular whether paragraphs 7.2.2.1 and 7.2.2.2 of Annex A would exceed the boundaries of what may be permitted under type approval legislation. It is the opinion of the task force that they should be permissible, but this should be verified.

7.6. Future developments that may be considered include:

7.6.1. Cyber Security threats can appear anytime during the lifetime of a vehicle. The task force specifies requirements in Annex A, paragraph 7. "Specifications" (and more specific in paragraph 7.2. "Requirements for the organization of the vehicle manufacturer"). These cyber security requirements may have relevance for the entire lifetime of a vehicle (design, production and post production). However, the task force acknowledges that the type approval does not need to be valid after the production is definitely discontinued (in accordance with the 1958 Agreement). A legal framework to improve embedding of the requirements in the post-production phase, other than already available from e.g. type approval requirements, should be considered further.

7.6.2. During the course of the threat analysis, risks were identified that were deemed to be outside the scope of this paper. However, these risks should not be overlooked, and it is therefore recommended that these should be passed onto the appropriate UN body for consideration.

7.6.3. It should be noted the domain of cyber security is highly dynamic. It is recommended that there is a need to periodically review this paper to ensure it

addresses new and emerging threats and mitigations, and is updated where necessary. There will be a need to oversee and initiate the reviews, re-establishing the Task Force as required.

7.6.4. At the time of completing this recommendation ISO and SAE were developing a new joint standard ISO/SAE 21434 Road Vehicles - Cybersecurity engineering. Once that is at a suitable stage this paper should be reviewed and updated where necessary.

7.6.5. It was noted that in future there would need to be dialogue between authorities to ensure a consistent approach to approvals and that WP.1 of UNECE could facilitate this.

7.7. Recommendations for implementation

7.7.1. The task force recommends that the proposed Regulation should consider a test phase before its full implementation. The aim of such a phase would be to validate and verify that the procedures envisaged for both, the vehicle manufacturers and Approval Authorities, work as intended and permit further revision of the Regulation, if needed. GRVA should consider what might be appropriate for such a test phase.

7.7.2. The task force recommends that time be given before the Regulation comes into force to permit vehicle manufacturers and Approval Authorities to adapt their processes so they can comply with this Regulation. GRVA should consider what might be an appropriate length of time and consider a phased introduction schedule. It is noted, that this will need to be balanced with the need to act in this area.

Annex A Draft proposal to introduce a Regulation on Cyber Security

Draft Regulation on Cyber Security

United Nations ECE/TRANS/WP.29/201x/xx

Economic and Social Council

Distr.: General
DD MM YYYY

Original: English

Economic Commission for Europe

Inland Transport Committee

World Forum for Harmonization of Vehicle Regulations

xxx session
Geneva, DD–DD MM YYYY
Item XXX of the provisional agenda
Draft new UN Regulation on software updates

Draft new UN Regulation on uniform provisions concerning the approval of cyber security

Submitted by the expert from xxx

The text reproduced below was prepared by the experts from xxx

I. Proposal

Draft new UN Regulation on uniform provisions concerning the approval of cyber security

Contents

1. Scope

1.1. This Regulation applies to vehicles of the categories [L], M, N, [O, R, S and T].

2. Definitions

For the purpose of this Regulation the following definitions shall apply:

2.1. "*Vehicle type*" means vehicles of a particular category which do not differ in at least the following essential respects:

(a) The manufacturer;

(b) The manufacturer's type designation;

(c) Essential aspects of vehicle design with respect to cyber security

2.2. "*Cyber security*" means the condition in which road vehicles and their functions are protected against threats to electrical or electronic components.

2.3. "*Cyber Security Management System (CSMS)*" means a systematic risk-based approach defining organisational processes, responsibilities and governance to mitigate cyber threats and protect vehicles from cyber-attacks.

3. Application for approval

3.1. The application for approval of a vehicle type with regard to cyber security shall be submitted by the vehicle manufacturer or by their duly accredited representative.

3.2. It shall be accompanied by the undermentioned documents in triplicate, and by the following particulars:

3.2.1. A description of the vehicle type with regard to the items specified in Annex 1 to this Regulation.

3.2.2. In cases where information is shown to be covered by intellectual property rights or to constitute specific know-how of the manufacturer or of their suppliers, the manufacturer or their suppliers shall make available sufficient information to enable the checks referred to in this Regulation to be made properly. Such information shall be treated on a confidential basis.

3.2.3. The CSMS Certificate of Compliance according to paragraph 6 of this Regulation.

4. Marking

4.1. There shall be affixed, conspicuously and in a readily accessible place specified on the approval form, to every vehicle conforming to a vehicle type approved under this Regulation an international approval mark consisting of:

4.1.1. A circle surrounding the Letter "E" followed by the distinguishing number of the country which has granted approval.

4.1.2. The number of this Regulation, followed by the letter "R", a dash and the approval number to the right of the circle described in paragraph 4.1.1. above.

4.2. If the vehicle conforms to a vehicle type approved under one or more other Regulations annexed to the Agreement in the country which has granted approval under this Regulation, the symbol prescribed in paragraph 4.1.1. above need not be repeated; in this case the Regulation and approval numbers and the additional symbols of all the Regulations under which approval has been granted in the country which has granted approval under this Regulation shall be placed in vertical columns to the right of the symbol prescribed in paragraph 4.1.1. above.

4.3. The approval mark shall be clearly legible and shall be indelible.

4.4. The approval mark shall be placed on or close to the vehicle data plate affixed by the Manufacturer.

4.5. Annex 3 to this Regulation gives examples of the arrangements of the approval mark.

5. Approval

5.1. Approval Authorities shall grant, as appropriate, type approval with regard to cyber security, only to such vehicle types that satisfy the requirements of this Regulation.

5.2. Notice of approval or of extension or refusal of approval of a vehicle type pursuant to this Regulation shall be communicated to the Parties to the 1958 Agreement which apply this Regulation, by means of a form conforming to the model in Annex 2 to this Regulation.

5.3. Approval Authorities shall not grant any type approval without ensuring that the manufacturer has put in place satisfactory arrangements and procedures to manage properly the cyber security aspects as covered by this Regulation.

5.4. For the purpose of paragraph 7.2. of this Regulation, the manufacturer shall ensure the cyber security aspects covered by this regulation are implemented.

6. Cyber Security Management System Certificate of Compliance

6.1. Contracting Parties shall appoint an Approval Authority or Technical Service to carry out the preliminary assessment of the manufacturer and to issue a CSMS Certificate of Compliance.

6.2. In the context of the preliminary assessment of the manufacturer, the Approval Authority or Technical Service shall ensure that the manufacturer has installed the necessary processes to comply with all legal requirements from this which are relevant for cyber security according to this Regulation.

6.3. When this preliminary assessment has been carried out, a certificate named CSMS Certificate of Compliance as described in Annex 4 to this Regulation (hereinafter the CSMS Certificate of Compliance) shall be granted to the manufacturer.

6.4. The Approval Authority or Technical Service shall use the model set out in Annex 4 to this Regulation for the CSMS Certificate of Compliance.

6.5. The CSMS Certificate of Compliance shall remain valid for three years from the date of deliverance of the certificate

6.6. The Approval Authority which has granted the CSMS Certificate of Compliance may at any time verify its continued validity. The CSMS Certificate of Compliance may be withdrawn if the requirements laid down in this Regulation are no longer met.

6.7. The manufacturer shall inform the Approval Authority or Technical Service of any significant change that could affect the relevance of the CSMS Certificate of Compliance. After consultation with the manufacturer, the Approval Authority or Technical Service shall decide whether new checks are necessary.

6.8. At the end of the period of validity of the CSMS Certificate of Compliance, the Approval Authority shall, as appropriate, issue a new CSMS Certificate of Compliance or extends its validity for a further period of three years. The Approval Authority shall issue a new certificate in cases where significant changes have been brought to the attention of the Approval Authority or Technical Service.

6.9. Existing vehicle type approvals shall not lose their validity due to the expiration of the manufacturer's CSMS Certificate of Compliance.

7. Specifications

7.1. General specifications

7.1.1. The requirements of this Regulation shall not restrict provisions or requirements of other UN Regulations.

7.1.2. The vehicle manufacturer may refer to [the Recommendation / Resolution on Cyber Security] in their assessment of cyber security risks and the mitigations, as well as when describing the processes employed.

7.2. Requirements for the Cyber Security Management System

7.2.1. For the preliminary assessment the Approval Authority or Technical Service shall verify that the vehicle manufacturer has a Cyber Security Management System in place and shall verify its compliance with this Regulation.

7.2.2. The Cyber Security Management System shall cover the following aspects:

7.2.2.1. The vehicle manufacturer shall demonstrate to an Approval Authority or Technical Service that their Cyber Security Management System considers the following phases:

- Development phase;

- Production phase;

- Post-production phase.

7.2.2.2. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System ensure security is adequately considered. This shall include:

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

(b) The processes used for the identification of risks to vehicle types;

(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 security of the system throughout its development and production phases;

(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 on vehicle types;

(h) The processes used to identify new and evolving cyber threats and vulnerabilities to vehicle types;

(i) The processes used to appropriately react to new and evolving cyber threats and vulnerabilities.

7.2.2.3. The vehicle manufacturer may refer to [the Recommendation / Resolution on cyber security] when describing the processes they have employed.

7.2.2.4. The vehicle manufacturer shall be required to demonstrate how their Cyber Security Management System will manage dependencies that may exist with contracted suppliers and service providers in regards of the requirements of paragraph 7.2.2.2.

7.3. Requirements for vehicle types

7.3.1. Before the assessment of a vehicle type for the purpose of type approval is carried out, the vehicle manufacturer shall demonstrate to the Approval Authority or Technical Service that their Cyber Security Management System has a valid CSMS Certificate of Compliance relevant to the vehicle type being approved.

7.3.2. The Approval Authority or Technical Service shall verify that the manufacturer has taken the necessary measures relevant for the vehicle type to:

(a) Collect and verify as appropriate information required under this regulation, through the full supply chain;

(b) Maintain appropriate design and test information;

(c) Implement appropriate security measures in the design of the vehicle and its systems;

7.3.3. The vehicle manufacturer shall demonstrate the risk assessment for the vehicle type in terms of the vehicle systems, the interactions of the different vehicle systems and the entire vehicle.

7.3.4. The vehicle manufacturer shall demonstrate how the design of critical elements of the vehicle type are protected against risks identified in the vehicle manufacturer's

risk assessment. Proportionate mitigations shall be implemented to protect such elements.

7.3.5. The vehicle manufacturer shall demonstrate how they have implemented appropriate and proportionate measures to protect dedicated environments on the vehicle type (if provided) for the storage and execution of aftermarket software, services, applications or data.

7.3.6. The vehicle manufacturer shall describe what testing has been performed to verify the effectiveness of the security measures implemented and the outcome of those tests.

8. Modification and extension of the vehicle type

8.1. Every modification of the vehicle type shall be notified to the approval authority which granted the approval. The Approval Authority may then either:

8.1.1. Consider that the modifications made are unlikely to have an appreciable adverse effect and that in any case the vehicle still complies with the requirements; or

8.1.2. Require a further test report from the technical service responsible for conducting the tests.

8.1.3. Confirmation or extension or refusal of approval, specifying the alterations, shall be communicated by means of a communication form conforming to the model in Annex 2 to this Regulation. The Approval Authority issuing the extension of approval shall assign a series number for such an extension and inform there of the other Parties to the 1958 Agreement applying this Regulation by means of a communication form conforming to the model in Annex 2 to this Regulation.

9. Conformity of production

9.1. The Conformity of Production Procedures shall comply with those set out in the 1958 Agreement, Schedule 1 (E/ECE/TRANS/505/Rev.3) with the following requirements:

9.1.1. The holder of the approval shall ensure that results of the conformity of production tests are recorded and that the annexed documents remain available for a period determined in agreement with the Approval Authority or Technical Service. This period shall not exceed 10 years counted from the time when production is definitively discontinued;

9.1.2. The Approval Authority which has granted type approval may at any time verify the conformity control methods applied in each production facility. The normal frequency of these verifications shall be once every three years.

10. Penalties for non-conformity of production

10.1. The approval granted in respect of a vehicle type pursuant to this Regulation may be withdrawn if the requirements laid down in this Regulation are not complied with or if sample vehicles fail to comply with the requirements of this Regulation.

10.2. If an Approval Authority withdraws an approval it has previously granted, it shall forthwith so notify the Contracting Parties applying this Regulation, by means of a communication form conforming to the model in Annex 2 to this Regulation.

11. Names and addresses of Technical Services responsible for conducting approval test, and of type approval authorities

11.1. The Contracting Parties to the Agreement which apply this Regulation shall communicate to the United Nations Secretariat the names and addresses of the Technical Services responsible for conducting approval tests and of the Type Approval Authorities which grant approval and to which forms certifying approval or extension or refusal or withdrawal of approval, issued in other countries, are to be sent.

Annex 1

Information document

The following information, if applicable, shall be supplied in triplicate and include a list of contents. Any drawings shall be supplied in appropriate scale and in sufficient detail on size A4 or on a folder of A4 format. Photographs, if any, shall show sufficient detail.

0. General

0.1 Make (trade name of manufacturer):

0.2. Type:

0.2.0.1 Chassis:

0.2.1. Commercial name(s) (if available):

0.3. Means of identification of type, if marked on the vehicle (b):

0.3.1. Location of that marking:

0.4. Category of vehicle (c):

0.8. Name(s) and address(es) of assembly plant(s):

0.9. Name and address of the manufacturer's representative (if any):

12. MISCELLANEOUS

12.8. Cyber Security

12.8.1. General construction characteristics of the vehicle type

12.8.1.1. Schematic representation of the vehicle type:

12.8.1.2. Documents for the vehicle type to be approved describing:

(a) The outcome of the risk assessment for the vehicle type;

(b) The vehicle systems (both type approved and non-type approved) which are relevant to the cyber security of the vehicle type;

(c) The components of those systems that are relevant to cyber security;

(d) The interactions of those systems with other systems within the vehicle type and external interfaces;

(e) The risks posed to those systems that have been identified in the vehicle type's risk assessment;

(f) The mitigations that have been implemented on the systems listed, or to the vehicle type, and how they address the stated risks;

(g) What tests have been used to verify the cyber security of the vehicle type and its systems and the outcome of those tests.

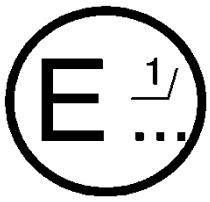
12.8.2. The number of the CSMS Certificate of Compliance

Annex 2

Communication form

COMMUNICATION

(Maximum format: A4 (210 x 297 mm))



issued by : Name of administration:

.....

.....

concerning: 2/ APPROVAL GRANTED

APPROVAL EXTENDED

APPROVAL REFUSED

APPROVAL WITHDRAWN

PRODUCTION DEFINITELY DISCONTINUED

of a vehicle type with regard to xxx equipment pursuant to Regulation No. **X**

Approval No. ……..

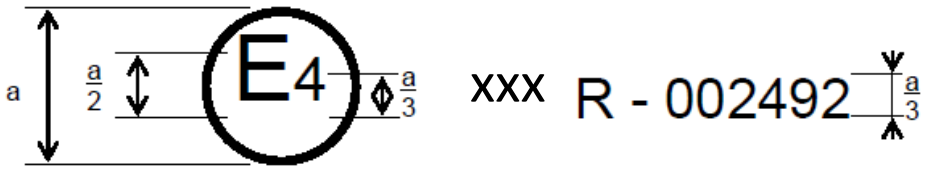
…

x.y ……

Annex 3

Arrangement of approval mark

Model A
(See paragraph 4.2 of this Regulation)



a = 8 mm min.

The above approval mark affixed to a vehicle shows that the road vehicle type concerned has been approved in the Netherlands (E 4), pursuant to Regulation No. xxx, and under the approval number 002492. The first two digits of the approval number indicate that the approval was granted in accordance with the requirements of Regulation No. xx.

Annex 4

Model of CSMS Certificate Certificate of Compliance

CYBER SECURITY MANAGEMENT SYSTEM CERTIFICATE OF COMPLIANCE
WITH REGULATION No. [Cyber Security Regulation] xxx
No. [Reference number]
[……. Approval Authority]
Certifies that

Manufacturer: .....

Address of the manufacturer: .....

complies with the provisions of paragraph 7 of Regulation No. xxx

Checks have been performed on:

by (name and address of the Type Approval Authority or Technical Service):

Number of report:

The certificate is valid until […..date]
Done at [……Place]
On […….Date]
[…….Signature]

Annex B

List of threats and corresponding mitigations

1. The examples within this annex are not to be viewed as mandatory within any assessment of a system. This annex is informative. That is it provides examples of possible threats and mitigations but these are not to be viewed as complete or appropriate to all vehicle systems or designs.

2. This annex consists of two parts. Part A of this annex describes the example of vulnerability or attack method. Part B of this annex describes the example of mitigation to the threats.

3. The examples should be considered by vehicle manufacturers and suppliers during the design, development, testing and implementation of vehicles and their systems, as appropriate. The examples of vulnerability or attack method in Part A is intended to help vehicle manufacturers, suppliers and competent authorities to understand the threats e.g. attack entries or security holes. The examples of mitigation in Part B is intended to help vehicle manufacturers, suppliers and competent authorities to consider what mitigation may be available to reduce risks for the threats identified e.g. usable industrial standards. Detailed security controls corresponding to the mitigation are described in Annex C to this recommendation.

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

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

   - Safe operation of vehicle affected
   - Vehicle functions stop working
   - Software modified, performance altered
   - Software altered but no operational effects
   - Data integrity breach
   - Data confidentiality breach
   - Loss of data availability
   - Other, including criminality

6. As technology progresses new threats or mitigations should be considered. This annex may also need to be periodically updated to ensure its contents reflect state of the art.

Part A. Examples of vulnerability or attack method related to the threats

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

Table 1
List of examples 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	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	**Unauthorised internet access** to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)
			1.3	**Unauthorised 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	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	**Unauthorised internet access to the server** (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)
			3.4	**Unauthorised 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, storing data in servers in garages)
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

High level and sub-level descriptions of vulnerability/ threat			*Example of vulnerability or attack method*	
			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 **unauthorised 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	12	Misuse or compromise of update procedures	12.1	Compromise of **over the air software update procedures**, This includes fabricating system update program or firmware

High level and sub-level descriptions of vulnerability/ threat			*Example of vulnerability or attack method*	
their update procedures			12.2	Compromise of **local/physical software update procedures**. This includes fabricating 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	14	Misconfiguration of equipment or systems by legitimate actor, e.g. owner or maintenance community	14.1	**Misconfiguration of equipment** by maintenance community or owner during installation/repair/use causing unintended consequence
			14.2	**Erroneous use** or administration of devices and systems (incl. OTA updates)
	15	Legitimate actors are able to take actions that would unwittingly facilitate a cyber-attack	15.1	Innocent victim (e.g. owner, operator or maintenance engineer) being **tricked into taking an action** to unintentionally load malware or enable an attack
			15.2	**Defined security procedures** are not followed
4.3.5 Threats to vehicles regarding their external 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, immobiliser, 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

High level and sub-level descriptions of vulnerability/ threat			*Example of vulnerability or attack method*	
			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 Potential targets of, or motivations for, an attack	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/unauthorised 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	Unauthorised 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.

High level and sub-level descriptions of vulnerability/ threat			*Example of vulnerability or attack method*	
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
	30	Physical loss of data can occur	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
			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)

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. Private or sensitive 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 OEM hardware**, e.g. unauthorised hardware added to a vehicle to enable "man-in-the-middle" attack **Replacement of OEM hardware (e.g., sensors) with unauthorised 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 (see Digital Tachograph experience)**

Part B. Examples of mitigation to the threats

1. Examples of mitigation for "Back-end servers"

Examples of mitigation to the threats which are related to "Back-end servers" are listed in Table B1.

Table B1
Examples of mitigation 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 shall be applied to back-end systems to minimise the risk of insider attack. Example Security Controls can be found in OWASP.
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 shall be 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. Example Security Controls can be found in.
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 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.
3.2	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 shall be 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 shall be applied to back-end systems to prevent data breaches. Example Security Controls can be found in OWASP.

2. Examples of mitigation for "Vehicle communication channels "

Examples of mitigation to the threats which are related to "Vehicle communication channels" are listed in Table B2.

Table B2
Examples of 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)
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

Table 1 reference	*Threats to "Vehicle communication channels"*	*Ref*	*Mitigation*
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 Security Controls can be found in 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. Examples of mitigation for "Update process"

Examples of mitigation to the threats which are related to "Update process" are listed in Table B3.

Table B3
Examples of mitigation 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 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 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. Examples of mitigation for "Unintended human actions "

Examples of mitigation to the threats which are related to "Unintended human actions" are listed in Table B4.

Table B4
Examples of mitigation to the threats which are related to "Unintended human actions"

Table 1 reference	*Threats relating to "Unintended human actions"*	*Ref*	*Mitigation*
14.1	Misconfiguration of equipment by maintenance community or owner during installation/repair/use causing unintended consequences	M17	Measures shall be implemented for defining and controlling configuration and maintenance procedures
14.2	Erroneous use or administration of devices and systems (inc. OTA updates)		
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.

4. Examples of mitigation for "External connectivity and connections "

Examples of mitigation to the threats which are related to "external connectivity and connections " are listed in Table B5.

Table B5
Examples of mitigation to the threats which are related to "external connectivity and connections"

Table 1 reference	*Threats to "External connectivity"*	*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		

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

Examples of mitigation to the threats which are related to "Potential targets of, or motivations for, an attack " are listed in Table B6.

Table B6
Examples of mitigation 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.
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. Example of Security Controls can be found in OWASP.
19.3	Extraction of cryptographic keys	M11	Security controls shall be implemented for storing cryptographic keys like High 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		

Table 1 reference	*Threats to "Potential targets of, or motivations for, an attack"*	*Ref*	*Mitigation*
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 (e.g., manipulation of odometer data can be mitigated by comparing it with GNSS data)
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. Examples of mitigation for "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened"

Examples of mitigation to the threats which are related to "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened" are listed in Table B7.

Table B7
Examples of mitigation 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. Example Security Controls can be found in SAE J3061
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 certification with 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. Examples of mitigation for "Data loss / data breach from vehicle"

Examples of mitigation to the threats which are related to "Data loss / data breach from vehicle" are listed in Table B8.

Table B8
Examples of mitigation 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*
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	Data protection best practices shall be followed for storing private and sensitive 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)		
31.1	Information breach. Private or sensitive data may be breached when the car changes user (e.g. is sold or is used as hire vehicle with new hirers)		

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

Examples of mitigation to the threats which are related to "Physical manipulation of systems to enable an attack" are listed in Table B9.

Table B9
Examples of mitigation 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

Annex C

Examples of Security Controls related to mitigations

1. Introduction

1.1. This annex is informative.

1.2. This annex may be referred to by Technical Services and other stakeholders, if required, to aid their understanding of possible security controls.

1.3. The examples of security controls within this annex are not to be viewed as mandatory within any assessment of a system. The examples listed are not necessarily exhaustive or appropriate to all vehicle systems or designs.

1.4. As technology progresses new security controls should be considered. This annex may also need to be periodically updated to ensure its content reflects state of the art.

2. Mapping between high level mitigations given in Annex B and more detailed examples of security controls

2.1. The following table provides further detail on example security controls for the "Mitigations". The list of security controls in this table is not exhaustive. Similarly, it may not be necessary to apply all security controls listed. The selection will depend on a risk assessment and any legal, contractual, regulatory requirements in a specific Intelligent Transport Systems / Automated Driving environment.

ID	*Mitigation*	*Security controls that may be relevant, with informative examples*
M1	Security Controls shall be applied to back-end systems to minimize the risk of insider attack	3.1 Security policies 3.2 Organizational security 3.3 Human resource security and security awareness 3.4 Asset management 3.5 Access control · Dual control principle applied · Role based access controls ("need to know" principle, "separation of duties") and appropriate training for staff 3.6 Cryptographic security 3.7 Physical and environmental security 3.8 Monitoring · Staff activity logging/ monitoring mechanisms · Security information and event management 3.10 Software security 3.12 Security incident management 3.13 Information exchange
M2	Security Controls shall be applied to back-end systems to minimize unauthorized access	3.5 Access control and authentication 3.6 Cryptographic security 3.7 Physical and environmental security 3.8 Monitoring · Monitor server systems and communications

ID	*Mitigation*	*Security controls that may be relevant, with informative examples*
		3.9 System design · Securely configuring servers (e.g. system hardening) · Protection of external internet connections, including authentication/verification of messages received and provision of encrypted communication channels · Manage the risks and security of cloud servers (if used) 3.10 Software security 3.12 Security incident management · Security information and event management 3.13 Information exchange
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	3.5 Access control · Role based access controls for staff 3.8 Monitoring 3.9 System design · Apply data minimisation techniques to reduce the impact should data be lost · Harden systems to minimise and prevent unauthorised physical access · Enact proportionate physical protection and monitoring 3.10 Software security 3.12 Security incident management 3.13 Information exchange
M4	Security Controls shall be applied to minimize risks associated with cloud computing	3.1 Security policies 3.2 Organizational security 3.3 Human resource security and security awareness 3.4 Asset management 3.5 Access control 3.6 Cryptographic security 3.7 Physical and environmental security 3.8 Monitoring · Monitoring of server systems 3.9 System design · Manage the risks and security of cloud servers · Apply data minimisation techniques to reduce the impact should data be lost 3.10 Software security 3.11 Supplier relationships security 3.12 Security incident management · Security information and event management 3.13 Information exchange
M5	Security Controls shall be applied to back-end systems to prevent data breaches	3.1 Security policies 3.2 Organizational security 3.3 Human resource security and security awareness · Appropriate procedures for handling transferring and disposing of data assets · Appropriate training for staff especially those handling data assets 3.4 Asset management 3.5 Access control 3.6 Cryptographic security 3.7 Physical and environmental security

ID	*Mitigation*	*Security controls that may be relevant, with informative examples*
		3.8 Monitoring 3.9 System design · Apply data minimisation and purpose limitation techniques to reduce the impact should data be lost 3.10 Software security 3.12 Security incident management 3.13 Information exchange
M6	The principle of security by design shall be adopted to minimise the impact of an attack on the vehicle ecosystem	3.1 Security policies 3.5 Access control · Access control and read/write procedures established for vehicle files and data 3.6 Cryptographic security 3.7 Physical and environmental security 3.8 Monitoring · System monitoring 3.9 System design · Message integrity and authentication checking · Hardening of e.g. operating system · Active memory protection · Network segmentation and implementation of trust boundaries 3.10 Software security · Software integrity checking techniques 3.12 Security incident management 3.13 Information exchange
M7	Access control techniques and designs shall be applied to protect system data/code	3.5 Access control · Access control and read/write procedures established for vehicle files and data 3.6 Cryptographic security 3.7 Physical and environmental security 3.8 Monitoring · System monitoring 3.9 System Design · Active memory protection · Network segmentation and implementation of trust boundaries · Application based input validation (in terms of what kind of data/input the affected application is expecting) · Secure storage of sensitive information 3.10 Software security · Software integrity checking techniques · Software testing 3.12 Security incident management 3.13 Information exchange
M8	Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data	3.5 Access control · Role based access controls 3.6 Cryptographic security 3.8 Monitoring 3.9 System Design · Harden systems to minimise and prevent unauthorised access · Enact proportionate physical protection and monitoring

ID	*Mitigation*	*Security controls that may be relevant, with informative examples*
		3.10 Software security 3.13 Information exchange
M9	Measures to prevent and detect unauthorized access shall be employed	3.5 Access control · Multi factor authentication for applications involving root access · Apply "least privilege access controls", for example separating admin accounts 3.8 Monitoring · System monitoring 3.9 System design · Establish trust boundaries and access controls · Avoid flat networks (apply defence in depth and network segregation) 3.10 Software security 3.13 Information exchange
M10	The vehicle shall verify the authenticity and integrity of messages it receives	3.5 Access control · Access control and read/write procedures established for vehicle files and data 3.6 Cryptography security · Encryption for communications containing sensitive data 3.8 Monitoring · System monitoring · Limit and monitor message content and protocols 3.9 System design · Message authentication for all messages received · Message integrity and authentication checking · Consistency checks using other vehicle sensors (e.g. temperature, radar…) · Use of techniques for integrity checking, such as hashing, secure protocols and packet filtering · Use of techniques for protecting against replay attacks, such as timestamping or use of a freshness value · Session management policies to avoid session hijacking · Harden operating system · Active memory protection · The use of combinations of gateways, firewalls, intrusion prevention or detection mechanisms, and monitoring are employed to defend systems · Network segmentation and implementation of trust boundaries · Correlation of data from different sources and sensors. 3.10 Software security · Software integrity checking techniques 3.13 Information exchange
M11	Security controls shall be implemented for storing cryptographic keys	3.6 Cryptographic security · Actively manage and protect cryptographic keys · Consider use of Hardware Security Module (HSM), tamper detection, and device authentication techniques to reduce vulnerabilities
M12	Confidential data transmitted to or from the vehicle shall be protected	3.6 Cryptographic security · Encryption for communications containing sensitive data 3.9 System design · Data minimisation techniques applied to communications 3.10 Software security

ID	*Mitigation*	*Security controls that may be relevant, with informative examples*
		· Software and systems used to protect confidential information is tested for vulnerabilities
M13	Measures to detect and recover from a denial of service attack shall be employed	3.8 Monitoring 3.9 System design · Verify size of received data matches expected values · Authentication of data · Timestamping messages and setting expiration time for messages · Employing rate limiting measures based on context · Setting acknowledgement messages for V2X messages (currently not standardised) · Fall-back strategy for loss of communications 3.10 Software security 3.12 Security incident management 3.13 Information exchange
M14	Measures to protect systems against embedded viruses/malware should be considered	3.8 Monitoring · System monitoring 3.9 System design · Message authentication and integrity checking · Input validation for all messages · Establish trust boundaries and access controls · Avoid flat networks (apply defence in depth and network segregation) 3.10 Software security 3.12 Security incident management 3.13 Information exchange
M15	Measures to detect malicious internal messages or activity should be considered	3.8 Monitoring · System monitoring including the adoption of techniques based on machine learning or statistical analysis of the data. 3.9 System design · Message authentication and integrity checking · Input validation for all messages · Establish trust boundaries and access controls · Avoid flat networks (apply defence in depth, isolation of components and network segregation) 3.10 Software security 3.12 Security incident management 3.13 Information exchange
M16	Secure software update procedures shall be employed	3.6 Cryptographic security · Effective key management and protection for any cryptography used 3.8 Monitoring 3.9 System design 3.10 Software security · Establish secure procedures, including configuration templates and policies · Secure communications used for updates · Ensure the veracity of updates · Version and timestamp logging of updates · Implement cryptographic protection and signing of software updates · Ensure configuration control and that it is possible to roll-back updates 3.13 Information exchange

ID	*Mitigation*	*Security controls that may be relevant, with informative examples*
M17	Measures shall be implemented for defining and controlling maintenance procedures	3.3 Human resource security and security awareness · Appropriate training of maintenance staff 3.8 Monitoring 3.9 System design · Implement the use of configuration templates and policies · Device configurations to be verified · Only allow a safe set of instructions to be passed to a vehicle · Apply message and device authentication techniques · Implement appropriate data controls 3.10 Software security 3.12 Security incident management 3.13 Information exchange
M18	Measures shall be implemented for defining and controlling user roles and access privileges based on the principle of least access privilege	3.1 Security policies 3.2 Organizational security 3.3 Human resource security and security awareness 3.4 Asset management 3.5 Access control and authentication
M19	Organizations shall ensure security procedures are defined and followed	3.1 Security policies 3.2 Organizational security 3.3 Human resource security and security awareness · There is a security programme defining procedures · Establish security development and maintenance process including at review, cross-check and approval gateways/ stages · Specific cyber awareness and security training needs are identified for roles, especially those in the design and engineering functions, and then implemented
M20	Security controls shall be applied to systems that have remote access	3.5 Access control · Access control rights established and implemented for remote systems to a vehicle 3.8 Monitoring · System monitoring for unexpected messages/behaviour 3.9 System design · Apply message and device authentication techniques · Only allow a safe set of instructions to be passed to a vehicle · Use of techniques for message integrity checking, such as hashing, secure protocols and packet filtering · Use of techniques for protecting against replay attacks, such as timestamping or use of a freshness value · Network segregation applied 3.10 Software security · Software and hardware testing to reduce vulnerabilities 3.12 Security incident management 3.13 Information exchange
M21	Software shall be security assessed, authenticated and integrity protected	3.8 Monitoring 3.9 System design 3.10 Software security 3.13 Information exchange

ID	*Mitigation*	*Security controls that may be relevant, with informative examples*
M22	Security controls shall be applied to external interfaces	3.8 Monitoring · System monitoring for unexpected messages/ behaviour 3.9 System design · Apply message and device authentication techniques · Only allow a safe set of instructions to be passed to a vehicle · Enforce boundary defences and access control between external interfaces and other vehicle systems · Systems are hardened to limit access 3.10 Software security 3.12 Security incident management 3.13 Information exchange
M23	Cybersecurity best practices for software and hardware development shall be followed	3.2 Organisational security · There is an active programme in place to identify critical vulnerabilities · Organizations plan for how to maintain security over the lifetime of their systems 3.6 Cryptographic security 3.7 Physical and environmental security 3.9 System design · Adopt secure coding practices for network segmentation · Security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain · Secure design methodologies, including assurance that network design requirements are met by corresponding implementations 3.10 Software security · Encryption of software code · Only permit applications that have had an accepted level of software testing to reduce vulnerabilities · Software and its configuration shall be security assessed, authenticated and integrity protected 3.11 Supplier relationships security · It is possible to ascertain and validate the authenticity and origin of supplies · Organisations, including suppliers, are able to provide assurance of their security processes and products 3.13 Information exchange
M24	Data protection best practices shall be followed for storing private and sensitive data	3.6 Cryptographic security 83. Monitoring 3.9 System design · Systems are designed so that end-users can efficiently and appropriately access, delete and manage their personal data. · Define measures to ensure secure deletion of user data in case of a change of ownership · Possibility to define rules for the management of the personal data. 3.10 Software security 3.13 Information exchange
M25	Systems should be designed to respond appropriately if an attack on a vehicle is detected	3.8 Monitoring 3.9 System design · Security risks are assessed and managed appropriately and proportionately · Redundancy or back-ups designed in, in case of system outage · Safety critical systems are designed to fail safe

ID	*Mitigation*	*Security controls that may be relevant, with informative examples*
		· Measures to ensure the availability of data are recommended 3.10 Software security 3.12 Security incident management 3.13 Information exchange

3. Further information on Security Controls

The following provides further informative details or suggestions regarding the example security controls provided in the above table.

The selection of appropriate security controls and the application of the implementation guidance provided, will depend on the vehicle design as defined by the vehicle type, its risk assessment and any relevant legal, contractual, or regulatory factors.

3.1. Security policies

3.1.1. Guidance related to security policies specified in ISO/SAE 21434 may apply.

3.1.2. The following points may also apply:

Policies for cybersecurity shall be defined and approved by management and communicated to employees

Policies to be reviewed at planned intervals or when significant changes occur to ensure their suitability, adequacy and effectiveness.

3.2. Organizational security

The following points may apply:

Cyber security roles and responsibilities to be defined and allocated

Segregation of duties to reduce opportunities for unauthorized/ unintentional modification/misuse of organization’s assets

Appropriate contact with relevant authorities shall be made for activities like security incident management

Contact with special interest groups, specialist security forums and professional associations shall be maintained for effective cybersecurity knowledge management

3.3. Human resource security and security awareness

3.3.1. The following points may apply:

Specific cyber awareness and security training needs are identified for roles, especially those in the design and engineering functions, and then implemented

There is a security programme defining procedures

Appropriate training for staff, especially those handling data assets

Appropriate training of maintenance staff

Staff activity logging/ monitoring mechanisms

Establish security development and maintenance process including at review, cross-check and approval gateways/ stages

3.3.2. Specific points related to "End of life considerations":

Appropriate procedures for handling, transferring and disposing of data assets

Define measures to ensure secure deletion of user data in case of a change of ownership

3.4. Asset management

3.4.1. The following points may apply:

Assets associated with vehicle systems should be identified and an inventory of these assets should be drawn up and maintained.

Assets maintained in the inventory should be owned.

Rules for the acceptable use of vehicle systems and of assets associated with vehicle systems should be identified, documented and implemented.

Assets should be disposed of securely when no longer required, using formal procedures.

3.5. Access control

3.5.1. The following points may apply:

3.5.1.1. Points related to "Access control mechanisms"

- Establish trust boundaries and access controls
- Apply least access principle to minimise risk
- Role based access controls ("need to know" principle, "separation of duties") are established and applied
- Access control and read/write procedures established for vehicle files, systems and data
- Access control rights established and implemented for remote systems to a vehicle
- Enforce boundary defences and access control between external interfaces and other vehicle systems
- Enforce boundary defences and access control between hosted software (apps) and other vehicle systems
- Dual control principle
- Multi factor authentication for applications involving root access
- System and application access control
  - (a) Information access restriction
  - (b) Secure log-on procedures
  - (c) Password management system for users/drivers
  - (d) Use of privileged utility programs
  - (f) Access control to vehicle source code

3.5.1.2. Points related to "Device and application authentication"

- Apply device authentication techniques
- Authentication of devices and equipment
- Device configurations to be verified
- Establish procedures for what applications may be permitted, what they can do and under what conditions

3.5.1.3. Points related to "Authorization"

- Ensure that there are authorization mechanisms in place for vehicle access roles
- Ensure that the in-vehicle application has clearly defined the user types and the rights of said users
- Ensure there is a least privilege stance in operation
- Ensure that the Authorization mechanisms work properly, fail securely, and cannot be circumvented

3.6. Cryptographic security

3.6.1. The following points may apply:

3.6.1.1. Points related to "Cryptographic key management"

- Actively manage and protect cryptographic keys
- Effective key management and protection for any cryptography used

3.6.1.2. Points related to "Encryption of communication and software"

- Encryption for communications containing sensitive data, including software updates
- Encryption of software code
- Ensure no sensitive data is transmitted in clear text, internally or externally
- Ensure the application is implementing known good cryptographic methods

3.7. Physical and environmental security

3.7.1. No further points identified.

3.8. Monitoring

3.8.1. Guidance related to field monitoring specified in ISO/SAE 21434 may apply.

3.8.2. The following points may also apply:

- System monitoring for unexpected messages/behaviour
- Enacting proportionate physical protection and monitoring
- Monitoring of server systems and communications
- Systems to detect and respond to sensor spoofing
- Session management policies to avoid session hijacking
- Protection from malware

- Logging and monitoring
- Control of operational software
- Information systems audit considerations

3.9. System Design

3.9.1. The following points may apply:

3.9.1.1. Points related to "Network design"

- Avoid flat networks (apply defence in depth, isolation of components and network segregation)
- Network segmentation and implementation of trust boundaries
- Protections of external internet connections, including authentication/verification of messages received and provision of encrypted communication channels
- Sandboxing for protected execution of 3rd party software
- The use of combinations of gateways, firewalls, intrusion prevention or detection mechanisms, and monitoring are employed to defend systems
- Ensure all internal and external connections (user and entity) go through an appropriate and adequate form of authentication. Be assured that this control cannot be bypassed
- Ensure that authentication credentials do not traverse in clear text form

3.9.1.2. Points related to "Control of data held on vehicles and servers and communicated therefrom"

(a) General

- Implement appropriate data controls
- Ensure that sensitive information is not compromised
- Apply data minimisation and purpose limitation techniques to reduce the impact should data be lost
- Data minimisation techniques applied to communications
- Systems are designed so that end-users can efficiently and appropriately access, delete and manage their personal data
- Apply techniques to prevent fraudulent manipulation of critical system data
- Apply strict write permissions and authentication measures for updating/ accessing vehicle parameters
- Ensure secure flag is set to prevent accidental transmission in the vehicular network

(b) Use of cryptography

- A policy on the use of cryptographic controls for protection of information is developed and followed. This should include an identification of what data is held and the need to protect it
- Secure storage of sensitive information should be applied

- Encrypt sensitive data and ensure keys are appropriately and securely managed
- Use active memory protection
- Consider the use of Hardware Security Module (HSM), tamper detection, and device authentication techniques to reduce vulnerabilities

(c) Authentication

- Ensure that whenever authentication credentials or any other sensitive information is passed, only accept the information via secure information protocols and channels through the vehicle communication channel
- Ensure all pages enforce the requirement for authentication for sensitive information

(d) Cookies

- Determine if all state transitions in the application code properly check for cookies and enforce their use
- Ensure that unauthorized activities cannot take place via cookie manipulation
- Ensure cookies contain as little private (user/driver) information as possible
- Ensure entire cookie is encrypted if sensitive data is persisted in the cookie
- Define all cookies being used by the application, their name, and why they are needed

(e) Data validation

- Ensure session data is being validated
- Ensure that a data validation mechanism is present
- Ensure all input that can (and will) be modified by a malicious user such as HTTP headers, input fields, hidden fields, drop down lists, and other web components are properly validated
- Ensure that proper length checks on all input exist
- Ensure that all fields, cookies, http headers/bodies, and form fields are validated
- Ensure that data is well formed and contains only known good characters if possible
- Ensure that data validation occurs on the server side
- Examine where data validation occurs and if a centralized model or decentralized model is used
- Ensure there are no backdoors in the data validation model
- Golden Rule: All external input, no matter what it is, is examined and validated

3.9.1.3. Points related to "Controls for messages"

(a) Only allow a safe set of instructions to be passed to a vehicle

(b) Message authentication and integrity checking

- Authentication of data

- Verify that the size of received data matches expected values
- Limit and monitor message content and protocols
- Employing rate limiting measures based on context
- Input validation for all messages

(c) Application based input validation (in terms of what kind of data/input the affected application is expecting)

(d) Consistency checks using other vehicle sensors (e.g. temperature, radar…)

(e) Setting acknowledgement messages for V2X messages (currently not standardised)

(f) Techniques to prevent replay attacks, such as timestamping and use of freshness values

(g) Timestamping messages and setting expiration time for messages

(e) Ensure that whenever authentication credentials or any other sensitive information is passed, only accept the information via the HTTP "POST" method and will not accept it via the HTTP "GET" method

(g) Any page deemed by the business or the development team as being outside the scope of authentication should be reviewed in order to assess any possibility of security breach

3.10. System Software security - acquisition, development and maintenance

3.10.1. The following points may apply:

- Secure communications used for updates
- Implement cryptographic protection and signing of software updates
- Implement the use of configuration templates and policies
- Ensure configuration control and that it is possible to roll-back updates
- Version and timestamp and logging of updates
- Ensure the veracity of the update
- Establish secure update procedures, including configuration templates and policies for updates
- For updates, applications should be reviewed and tested to ensure there is no adverse impact on vehicle and organisational security.

3.10.1.1. Points related to "Secure software development"

(a) Adopt secure coding practices

- Ensure development/debug backdoors are not present in production code
- Ensure that no system errors can be returned to the user/ driver/ HMI
- Ensure all logical decisions have a default clause
- Ensure no development environment kit is contained in the build directories
- Memory management

- Input Validation
- Output Encoding
- Code modification prevention

(b) Error handling

- Error handling, exception handling and logging
- Ensure that the application fails in a secure manner and redundancy options are available in case of a failure
- Ensure resources are released if an error occurs
- Ensure that no sensitive information is logged in the event of an error
- Search for any calls to the underlying operating system or file open calls and examine the error possibilities
- Ensure application errors are logged

(c) Apply software testing and integrity checking techniques

- Examine the application for debug logging with the view to logging of sensitive data
- Examine the file structure. Are there any components, which should not be directly accessible, available to the user?
- Examine all memory allocations/de-allocations
- Examine the application for dynamic SQL and determine if it is vulnerable to SQL injection attacks
- Search for commented out code, commented out test code, which may contain sensitive information

(d) Session management

- Examine session invalidation
- Examine how and when a session is created for a user and how it is unauthenticated and authenticated
- Examine the session ID and verify if it is complex enough to fulfil requirements regarding strength
- Determine the actions the application takes if an invalid session ID occurs
- Determine how multithreaded/multi-user session management is performed.
- Determine the session HTTP inactivity timeout
- Determine how the log-out functionality functions

3.10.1.2. Points related to "Secure software testing"

- Testing of security functionality should be carried out during development.
- Acceptance testing programs and related criteria should be established for new systems, upgrades and software versions."

3.11. Supplier relationships security

3.11.1. Guidance related to distributed development specified in ISO/SAE 21434 may apply.

3.11.2. The points may also apply:

- Cyber security requirements for mitigating the risks associated with supplier's products/ system to the manufacturers products/system shall be agreed with the supplier and documented
- All relevant cyber security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide infrastructure components for, the manufacturers
- Agreements with suppliers shall include requirements to address the cyber security risks associated with information and communications technology services and product supply chain
- Manufacturer shall regularly monitor, review and audit supplier service delivery
- Changes to the provision of services by suppliers, including maintaining and improving existing cyber security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems, components and processes involved and re-assessment of risks

3.12. Security incident management

3.12.1. Guidance related to cyber security incident management for vehicles specified in ISO/SAE 21434 may apply.

3.12.1. The following points may also apply:

- Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to cyber security incidents.
- Cyber security incidents should be reported through appropriate management channels as quickly as possible.

3.13. Information Exchange

3.13.1 Guidance related to structured information exchange may be found in ITU-T X.1500 Series for Structured Cybersecurity Information Exchange (CYBEX) Techniques

3.13.2. The following provides references from the ITU-T X.1500 series may be used for exchanging structured cybersecurity information to enhance cybersecurity through coherent, comprehensive, global, timely and assured information exchange about vulnerabilities, weaknesses, attack patterns and so on:

- X.1520 Common vulnerabilities and exposures (CVE)
- X.1521 Common vulnerability scoring system (CVSS)
- X.1524 Common weakness enumeration (CWE)
- X.1525 Common weakness scoring system (CWSS)
- X.1544 Common attack pattern enumeration and classification (CAPEC)

Annex D

List of reference documents

The following list contains references to documents that were drawn upon and used in the creation of this paper:

ENISA report "Cyber Security and Resilience of Smart Cars"	TFCS-03-09
UK DfT Cyber Security principles	TFCS-03-07
NHTSA Cyber Security Guideline	TFCS-03-08
IPA "Approaches for Vehicle Information Security" (Japan)	TFCS-04-05
UNECE Cyber security guideline (ITS/AD)	ECE/TRANS/WP.29/2017/46

SAE J 3061

ISO/SAE 21434 Road vehicles – Cybersecurity Engineering (under development)

ISO/IEC 19790

ISO/IEC 27000 series

ISO/IEC 26262

ISO/IEC 19790 "Security requirements for cryptographic modules"

US Auto ISAC (report by Booz Allen Hamilton) https://www.automotiveisac.com/best-practices/

"OWASP"

GSMA CLP.11 IoT security guidelines and CLP.17 IoT Security Assessment