Submitted by the experts from
SAE International

Informal document **GRVA-13-27**
13th GRVA, 23-27 May 2022
Provisional agenda item 5(a)

Proposal for amendments to the Interpretation Document ECE/TRANS/WP.29/2021/59 for UN Regulation No. 155 (Cyber security and cyber security management system)

A. Part A

1. Preamble

1.1. The purpose of Part A of this document is to help clarify the requirements of paragraphs 5, 7 and 8 and Annex 1 of the UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system (UN Regulation No. 155) and provide information on what may be used to evidence those requirements. The target audience for this document are vehicle manufacturers submitting systems for test and the Technical Services / Approval Authorities assessing those systems. The outcome should be that this document is able to help harmonise evaluations between different Technical Services/ Approval Authorities.

2. Note regarding evidencing the requirements

2.1. This document is only guidance. It provides information on what information might/would be acceptable for the Technical Services/ Approval Authorities and what level of information might be supplied. It is not intended to be exhaustive. The standards referenced are intended as examples, not mandatory. Nevertheless, a coherence-check (see section 6 "Link with ISO/SAE ~~DIS~~ 21434 (E)") has shown that especially ~~the~~ ISO/SAE ~~DIS~~ 21434 can be very supportive in implementing the requirements on the CSMS to the organizations along the supply chain. ~~It should be noted that the clauses of ISO/SAE DIS 21434 referred to may change during later edition of the standard, but it is expected that the standard will still be relevant to those requirements.~~ Depending on the vehicle type defined by the vehicle manufacturer and the practices and procedures they use, alternative and/or equivalent information may be supplied.

2.2. For all the requirements in the regulation, demonstration that they are met may be achieved via documentation/presentation and/or audit. The format of what documentation is supplied is open but should be agreed between the vehicle manufacturer and Technical Service/ Approval Authority prior to testing/audit. A demonstration may be provided through an overview, diagrams and experience. Argument that the requirements are met needs to be logical, understandable and convincing. Documents need not necessarily be large documents.

2.3. The wording used in this document seeks to respect the ISO/IEC Directives, Part 2, Principles and rules for the structure and drafting of ISO and IEC documents (ISBN 978-92-67-10603-8) described in section 7 of the 8th edition 2018.

3. Guidance on the requirements of the Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system (UN Regulation No. 155)

Note. The paragraphs referred to below refer to the paragraphs of the on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system.

A. Paragraphs 1. to 4. of the Regulation

"1. Scope"

No guidance included in this document with regards this requirement

"2. Definitions"

No guidance included in this document with regards this requirement

"3. Application for Approval"

No guidance included in this document with regards this requirement

"4. Marking"

No guidance included in this document with regards this requirement

B. Paragraph 5. to 5.3.

"5. Approval"

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

Explanation of the requirement

In addition to the conditions referred to in paragraph 5.1., the Approval Authority is bound to verify if all the requirements quoted in section 7 of the Regulation have been effectively fulfilled. This includes the Cyber Security Management System referred to in paragraphs 7.2. and 7.3.1.

C. Paragraph 5.3.1., part (a)

"5.3.1. The Approval Authority and its Technical Services shall ensure, in addition to the criteria laid down in Schedule 2 of the 1958 Agreement that they have:

(a) Competent personnel with appropriate cyber security skills and specific automotive risk assessments knowledge;"

Explanation of the requirement

The requirement would imply that the authority or the Technical Service (the organisation) have at their disposal, in a sufficient number, the following categories of personnel:

(a) Personnel competent and experienced in application of the Cyber Security Regulation, as well as of any national or organisation’s rules, standards and procedures necessary for its implementation and application. Applicable standards may include ISO 21434 and ISO 27001 for the content and aspects of ISO 19011 and ISO PAS 5112 for the audit processes;

(b) Personnel competent and experienced in application of methods of cyber security laboratory testing, such as, pen-, fuzz- and side channel-testing, in relation to cyber security of the vehicle.

This competence should be demonstrated by appropriate qualifications or other equivalent training records.

The Regulation does not impose any specific contractual relation between the Approval Authority/Technical Service and the personnel concerned. These might be employment (labour) contracts, services contracts etc.

The number of personnel concerned must be proportionate to the actual workload.

The internal procedures of the organisation should ensure that the tasks under the Regulation are performed or effectively controlled by the personnel having relevant skills.

D. Paragraph 5.3.1., part (b)

"(b) Implemented procedures for the uniform evaluation according to this Regulation."

Explanation of the requirement

The organisation should have in place procedures ensuring that evaluation of every vehicle type is conducted according to the same scheme. If necessary, the evaluation may include variants. Application of variants is determined by clear criteria set out and explained in the internal documentation of the organisation.

In case the Approval Authority has designated several Technical Services, it needs to ensure uniformity of evaluation between different Technical Services, notably by arranging regular meetings where the experience is exchanged.

The organisation should have processes installed for secure storage and transmission of confidential information.

The Technical Services should have processes to assure that the integrity of the personnel involved in assessments is appropriate to the risks involved.

The requirement of the Regulation cannot be discharged by mere establishment of the required processes and procedures. It also requires their effective application, implying the necessity for adequate training and effective quality control.

Examples of documents/evidence proving correct implementation

Interpretation documents of the Technical Services

Best practice guidelines of the Approval Authority. These are the consolidated interpretations of the Technical Services.

Minutes of exchange of experience meetings of Approval Authority and Technical Services.

E. Paragraph 5.3.2.

"5.3.2. Each Contracting Party applying this Regulation shall notify and inform by its Approval Authority other Approval Authorities about the method and criteria taken as a basis by the notifying Authority to assess the appropriateness of the measures taken in accordance with this regulation and in particular with paragraphs 5.1., 7.2. and 7.3.

This information shall be shared only before granting an approval according to this Regulation for the first time and each time the method or criteria for assessment is updated.

This information is intended to be shared for the purposes of collection and analysis of the best practice and in view of ensuring the convergent application of this Regulation by all Approval Authorities applying this Regulation."

Explanation of the requirement

This requirement aims at convergence across the Contracting Parties in the manner the requirements of paragraphs 5.1., 7.2. and 7.3. are applied. Importantly, the following sub-paragraphs must be interpreted in the manner permitting to achieve this objective. Additionally, the exchange should permit mutual learning and building of a pool of best practices which may be inspiration for further works on the amendment of UN Regulation No. [155] in the future.

As it can be understood from joint reading of paragraphs 5.3.2. and 5.3.3., information about methods and criteria should contain:

(a) minimum performance levels that the Approval Authority will require to be met with regard to the specifications provided for under paragraphs 7.2. and 7.3.;

(b) measures and processes the Approval Authorities/their Technical Services will follow when assessing the compliance following an application for a type approval.

In particular, the information should include:

(c) the characteristics and the minimum performance criteria that processes referred to in paragraph 7.2.2.2. must meet, including the information on the criteria used to establish if the risks referred to in paragraph 7.2.2.2.(d) are "appropriately managed";

(d) the criteria that the Approval Authority will apply to assess if these processes ensure that cyber threats and vulnerabilities referred to in paragraph 7.2.2.3. shall be mitigated within a reasonable timeframe, including the information on the conditions for these threats and vulnerabilities to be considered as mitigated and on the understanding of "reasonable timeframe";

(e) the criteria that the Approval Authority will apply to assess that the processes meet the requirement referred to in paragraph 7.2.2.4.;

(f) the criteria that the approval authority will apply to assess if the manufacturer has demonstrated that the CSMS manages dependencies referred to in paragraph 7.2.2.5.;

(g) the criteria that the Approval Authority will apply to assess whether the CSMS certificate to be considered relevant for the vehicle type under approval;

(h) for type approvals prior to 1 July 2024, the criteria that the Approval Authority will apply to assess if cyber security was adequately considered during the development phase of the vehicle type to the effect that it results in an equivalent cybersecurity performance;

(i) the criteria that the Approval Authority will apply to assess whether the manufacturer has taken sufficient measures to identify and manage, for the vehicle type being approved, supplier-related risks, including the required standards for such risk management;

(j) the criteria that the Approval Authority will apply to assess if the vehicle manufacturer has identified the critical elements of the vehicle type, including the definition of "critical elements" that the authority has adopted to this effect;

(k) the criteria that the Approval Authority will apply to assess if the vehicle manufacturer has performed an exhaustive risk assessment for the vehicle type, as required under subparagraph 7.3.3. of the Regulation;

(l) the criteria that the Approval Authority will apply to assess if the vehicle type is protected against risks identified in the vehicle manufacturer’s risk assessment;

(n) the criteria that the Approval Authority will apply to assess if the mitigations applied by the manufacturer are proportionate, including the explanation of the interpretation of the term "proportionate";

(o) the criteria that the approval authority will apply to assess if the mitigations referred to in Annex 5, Part B or C, are not relevant, not sufficient for the risk identified or

not feasible;

(p) the criteria that the approval authority will apply to assess if "another mitigation" implemented by the manufacturer pursuant to subparagraph 7.3.4. is "appropriate";

(q) the criteria that the Approval Authority will apply to assess if the testing performed by the manufacturer to verify the effectiveness of the security measures implemented were "appropriate" and "sufficient";

(r) the criteria that the Approval Authority will apply to assess if measures put in place by the manufacturer to secure dedicated environments on the vehicle type for the storage and execution of aftermarket software, services, applications or data, are "appropriate" and "proportionate", including the explanation of the interpretation of the term "proportionate" in this context;

(s) the documents that the Approval Authority will require to check if the vehicle manufacturer has taken the necessary measures referred to in subparagraph 5.1.1.;

(t) the tests that the Approval Authority or Technical Services will perform and the testing strategy it will apply to verify that that the vehicle manufacturer has implemented the cyber security measures they have documented;

(u) the internal procedures that the Approval Authority will apply in the process of assessment under section 5 of the Regulation.

It is important to stress that the Approval Authorities of the Parties are implicitly obliged to follow the methods and requirements which are subject to sharing and assessment.

F. Paragraph 5.3.3.

"5.3.3. The information referred to in paragraph 5.3.2. shall be uploaded in English language to the secure internet database established by the United Nations Economic Commission for Europe (DETA) in due time and no later than 14 days before an approval is granted for the first time under the methods and criteria of assessment concerned. The information shall be sufficient to understand what minimum performance levels the Approval Authority adopted for each specific requirement referred to in paragraph 5.3.2. as well as the processes and measures it applies to verify that these minimum performance levels are met."

Explanation of the requirement

Information uploaded must be objectively sufficient to understand the minimal performance levels that an authority adopted to consider that the requirements of the Regulation are complied with. This is of crucial importance, given the high-level nature and the frequent use of general clauses in formulation of these requirements.

Although the obligation to share the information, as referred to in paragraph 5.3.3., is an obligation of result and must always be met by the Approval Authority, the latter should discharge this obligation mindful of the need to avoid putting at risk the cyber security of a vehicle type approved in accordance with this Regulation.

Preferably, the information should be shared with other authorities well in advance (i.e. long before the first assessment conducted under these methods and criteria), so as to permit other authorities to examine them and, if necessary, obtain additional clarification, so as to fully achieve the objectives. However, under no circumstances can an Approval authority grant a type approval based on such methods and criteria within less than 14 days from the moment when the information was shared via DETA.

Examples of documents/evidence that could be provided

Please refer to Annex 1, which provides a template for data exchange via DETA in accordance with paragraph 5.3.

G. Paragraph 5.3.4.

"5.3.4. Approval Authorities receiving the information referred to in paragraph 5.3.2. may submit comments to the notifying Approval Authority by uploading them to DETA within 14 days after the day of notification."

Explanation of the requirement

Approval Authorities of other Contracting Parties are given the possibility, but are under no obligation, to provide comments on the information shared.

The 14-day time limit applies also in case where the information referred to in line with paragraph 5.3.2. has been shared earlier than 14 days before the approval decision. Ideally, comments of other authorities should be discussed and, if legitimate/useful, taken into account before the methods and criteria shared through DETA are applied for the first time. Therefore, interested approval authorities should react as quickly as possible by transmitting their views to the Approval authority.

H. Paragraph 5.3.5.

"5.3.5. If it is not possible for the granting Approval Authority to take into account the comments received in accordance with paragraph 5.3.4., the Approval Authorities having sent comments and the granting Approval Authority shall seek further clarification in accordance with Schedule 6 to the 1958 Agreement. The relevant subsidiary Working Party of the World Forum for Harmonization of Vehicle Regulations (WP.29) for this Regulation shall agree on a common interpretation of methods and criteria of assessment. That common interpretation shall be implemented and all Approval Authorities shall issue type approvals under this Regulation accordingly."

Explanation of the requirement

Possible comments of Approval Authorities of other Contracting Parties have no suspensive effect on the issuance of a type approval by the Approval Authority. However, if the latter decides not to take the comments on board, the Approval Authorities having made comments and the Approval Authority having issued a decision are bound to initiate a discussion before the GRVA on the methods and criteria submitted and the comments received. Although the obligation to seek further clarification is on both authorities, it is not necessary for the procedure under Schedule 6 to start that both the Authority having submitted information and the Authority having made comments take formal steps to this effect. Under Schedule 6 paragraph 3, the Chair of the GRVA is required to "identify the issues arising from diverging interpretations" of the Cyber Security Regulation.

The interpretation of the GRVA should be guided by the purpose of the consultation procedure, as specified under paragraph 5.3.2., hence ensuring convergence in the application of the Regulation. Therefore, it should contain elements permitting to clearly establish whether the minimum performance levels and processes applied by the Approval Authority are sufficient/adequate to verify if the requirements of the Regulation have been complied with. Once the GRVA agrees on the interpretation, this interpretation of the Regulation must be applied by all approval authorities, in all future assessment procedures (for type approvals, modifications and extensions) under the Regulation. This may require updates of the existing methods and criteria by Approval Authorities of certain or all Contracting Parties.

I. Paragraph 5.3.6.

"5.3.6. Each Approval Authority granting a type approval pursuant to this Regulation shall notify other Approval Authorities of the approval granted. The type approval together with the supplementing documentation shall be uploaded in English language by the Approval Authority within 14 days after the day of granting the approval to DETA."

Explanation of the requirement

This requirement is distinct from and additional to the requirement of notification based on a standard form included in paragraph 5.2. The type approval must be notified together with supplementing documentation which is not specified in paragraph 5.3.6. The objective of sharing is not explicitly stated in the Regulation, but can be inferred from paragraph 5.3.7. it is to allow the approval authorities to "study" the approvals and possibly address "diverging views" in compliance with, notably, Schedule 6. Therefore, the supplementing documentation should include all elements (including test reports) sufficient to permit the approval authorities to understand if and how the methods and criteria referred to in previous paragraphs have been applied in the context of an individual approval decision.

The information must be uploaded to the DETA database. A template for uploading information to the database is provided in section 5.

The obligation of notification in the first sentence of paragraph 5.3.6. is not dependant on possibility to reconcile the requirement of uploading the information to DETA with its obligations under national law pertaining to security and possible confidentiality of the notified information. In the situation where uploading the information to DETA might conflict with such other obligations, the approval authority must find a way to notify the information in a secure manner.

J. Paragraph 5.3.7.

"5.3.7. The Contracting Parties may study the approvals granted based on the information uploaded according to paragraph 5.3.6. In case of any diverging views between Contracting Parties this shall be settled in accordance with Article 10 and Schedule 6 of the 1958 Agreement. The Contracting Parties shall also inform the relevant subsidiary Working Party of the World Forum for Harmonization of Vehicle Regulations (WP.29) of the diverging interpretations within the meaning of Schedule 6 to the 1958 Agreement. The relevant Working Party shall support the settlement of the diverging views and may consult with WP.29 on this if needed."

Explanation of the requirement

In case of "diverging views" regarding the information on the type approval among the Approval Authorities, reference is made to Article 10 of the Agreement and to Schedule 6. The procedure under Article 10 is reserved for cases where there is dispute on the interpretation of the Agreement. By contrast, any dispute, arising in the context of the type approval, which concerns the application or interpretation of the Regulation (hence also the application of the methods and criteria referred to in paragraph 5.3.3.) must be solved pursuant to Schedule 6, paragraph 2.

K. Paragraphs 6. to 7.1.1.

"6. Certificate of Compliance for Cyber Security Management System"

No guidance included in this document with regards this requirement

"7. Specifications

7.1. General specifications

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

Explanation of the requirement

The requirements of this Regulation shall not restrict provisions or requirements of other UN Regulations as well as national or regional legislations as described in points 1.3. and 1.4. of

the scope of this Regulation.

L. Paragraphs 7.2. to 7.2.1.

"7.2. Requirements for the Cyber Security Management System

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

Explanation of the requirement

The intention of this requirement is that the Technical Service or Approval Authority shall verify that:

(a) The vehicle manufacturer has a CSMS;

(b) The presented CSMS complies to the requirements listed below in this regulation.

For this requirement the focus is on the manufacturer's processes and assessing if they are in place, in order to get an overview of the capability of the manufacturer to fulfil the requirements of the CSMS.

The follow clarifications should be noted:

(c) The CSMS may be a part of the organization's Quality Management System or be independent of it;

(d) If the CSMS is part of the organization's QMS it should be clearly identifiable.

Examples of documents/evidence that could be provided

The following standards may be applicable:

(e) ~~ISO/SAE 21434~~ ISO PAS 5112 may be used as the basis for evidencing and evaluating the CSMS~~,~~ utilising requirement and recommendations in ISO/SAE 21434 (E) ~~C~~clauses 5 "~~Overall~~ Organizational cybersecurity management", 6 "Project dependent cybersecurity management", and ~~7~~8 "Continu~~a~~l~~ous~~ cybersecurity activities" ~~could be used~~ to evaluate the CSMS in general;

(f) ISO 18045, ISO 15408, ISO 27000 series, ISO 31000 series may be applicable to relevant parts of the CSMS.

M. Paragraphs 7.2.2. to 7.2.2.1.

"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 applies to the following phases:

- Development phase;
- Production phase;
- Post-production phase."

Explanation of the requirement

The intention of this requirement is that the cybersecurity management system should be able to demonstrate how a manufacturer will handle cybersecurity during the operational life of vehicles produced under a vehicle type. This includes evidencing that there are procedures and processes implemented to cover the three phases. The different phases of the lifecycle

may have specific activities to be performed in each of them.

7.2.2.1. describes the different phases of the vehicle type to be considered in the CSMS and 7.2.2.2. applies to all these phases if not stated otherwise. The phases also apply to 7.2.2.4.

The CSMS may include active and/or reactive processes or procedures covering the end of support for a vehicle type and how this is implemented or triggered. It may include the possibility to disconnect non-mandatory functions/systems and under what conditions this might happen.

The operational life (use phase) of an individual vehicle will commence during the production phase of the vehicle type. It will end during either the production phase or post-production phase of the vehicle type.

Examples of documents/evidence that could be provided

The following standards may be applicable:

(a) ~~ISO/SAE 21434 can~~ISO PAS 5112 may be used as the basis for evidencing and evaluating the required phases of the CSMS~~.~~, utilising ISO/SAE 21434 (E) ~~C~~clauses 9 "Concept ~~Phase~~", 10 "Product ~~D~~development", and 11 "Cybersecurity validation" ~~could be used~~ to evaluate the Development phase of the CSMS~~;~~. ~~C~~clause 12 "Production" ~~could be used~~ to evaluate the Production phase of the CSMS~~.~~; and ~~C~~clauses ~~7~~8 "Continua~~lous~~ cybersecurity activities", 13 "Operations and maintenance", and 14 "End of cybersecurity support and ~~D~~decommissioning" ~~could be used~~ to evaluate the Post-~~production~~ development phase of the CSMS;

(b) Other standards that may be applicable to 7.2.2. and its sub-requirements include: ISO 18045, ISO 15408, ISO 27000 series, ISO 31000 series.

N. Paragraph 7.2.2.2., part (a)

"7.2.2.2. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System ensure security is adequately considered, including risks and mitigations listed in Annex 5. This shall include:

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

Explanation of the requirement

The aim of this requirement is to ensure that the organization has processes to manage the implementation of the CSMS. Its scope is limited to processes that are relevant for the cyber security of the vehicle types and not other aspects of the organization. For example, the scope of this requirement is not intended to cover the entire Information Security Management System of an organization.

The following could be used to show the range of activities performed by the manufacturer to manage the cyber security of the development, production and post-production phases of a vehicle type:

(a) Organizational structure used to address cyber security;

(b) Roles and Responsibilities regarding cybersecurity management incl. accountability.

Examples of documents/evidence that could be provided

(c) ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-05-01], [RQ-05-02]. [RQ-05-0~~6~~7], [RQ-05-0~~7~~8];

(d) BSI PAS 1885 or ISO PAS 5112 could be used to help evidence this requirement. National certification schemes, like the UK Cyber Essentials, could be used to evidence a manufacturer's organizational processes.

Commented [NJR1]: Aligning to verb used above in L.

Commented [NJR2]: If we need to reference ISO/SAE 21434, then referencing of its exact requirements needs to be avoided due to the possibility of tailoring by organisations.

FYI, tailoring is when an organisation proves, via a provided rationale, that they still meet the requirements of a particular clause but have not needed to perform certain activities.

Also, clause 11 (Validation) would also be useful to quote here, as essentially it mandates the application of the right-hand side of the "V" development model.

The requirement should be considered unfulfilled if one of the following statements is true

1. Processes are absent or incomplete.

2. Processes are not applied universally or consistently.

3. Processes are often or routinely circumvented to achieve business objectives.

4. The vehicle manufacturer's security governance and risk management approach has no bearing on its processes.

5. System security is totally reliant on users' careful and consistent application of manual security processes.

6. Processes have not been reviewed in response to major changes (e.g. technology or regulatory framework), or within a suitable period.

7. Processes are not readily available to staff, too detailed to remember, or too hard to understand.

The requirement may be considered fulfilled if all the following statements are true

1. The vehicle manufacturer fully documents its overarching security governance and risk management approach, technical security practice and specific regulatory compliance. Cyber security is integrated and embedded throughout these processes and key performance indicators are reported to its executive management.

2. The vehicle manufacturer's processes are developed to be practical, usable and appropriate for its policies and technologies.

3. Processes that rely on user behaviour are practical, appropriate and achievable.

4. The vehicle manufacturer reviews and updates processes at suitably regular intervals to ensure they remain relevant. This is in addition to reviews following a major cyber security incident.

5. Any changes to the essential function or the threat it faces triggers a review of processes.

6. The vehicle manufacturer's systems are designed so that they are, and remain, secure even when user security policies and processes are not always followed. For such claim a justification should be provided.

O. Paragraph 7.2.2.2., part (b)

"(b) The processes used for the identification of risks to vehicle types. Within these processes, the threats in Annex 5, Part A, and other relevant threats shall be considered."

Explanation of the requirement

The aim of this requirement is for a manufacturer to demonstrate the processes and procedures they use to identify risks to vehicle types.

Processes implemented should consider all probable sources of risk. This shall include risks identified Annex 5 of the Cyber Security Regulation e.g. risks arising from connected services or dependencies external to the vehicle.

Sources for risk identification may be stated. These may include:

(a) Vulnerability/ Threats sharing platforms;

(b) Lessons learned regarding risks and vulnerabilities.

Examples of documents/evidence that could be provided

The following standards may be applicable:

(c) ISO/SAE 21434, especially based on [RQ-0815-01], [RQ-0815-02], [RQ-0815-08], [RQ-08-09].

(d) ISO PAS 5112.

The processes may consider:

(de) Identification the relevance of a system to cybersecurity;

(ef) Description of the overall system with respect to:

(i) Definition of the system/function;

(ii) Boundaries and interactions with other systems;

(iii) Architecture;

(iv) Environment of operation of the system (context, constraints and assumptions).

(fg) Identification of assets;

(gh) Identification of threats;

(hi) Identification of vulnerabilities.

The requirement should be considered unfulfilled if one of the following statements is true

1. Risk identification is not based on a clearly defined set of assumptions.

2. Risk identification for vehicle types are a "one-off" activity (or not done at all).

3. Vehicle types are assessed in isolation, without consideration of dependencies and interactions with other systems. (e.g. interactions between IT and OT environments).

The requirement may be considered fulfilled if all the following statements are true

1. The vehicle manufacturer's organisational process ensures that security risks to vehicle types are identified, analysed, prioritised, and managed.

2. The vehicle manufacturer's approach to risk is focused on the possibility of adverse impact to its vehicle types, leading to a detailed understanding of how such impact might arise as a consequence of possible attacker actions and the security properties of its networks and systems.

3. The vehicle manufacturer's risk identification is based on a clearly understood set of assumptions, informed by an up-to-date understanding of security threats to its vehicle types and its sector.

4. The vehicle manufacturer's risk identification is informed by an understanding of the vulnerabilities in its vehicle types.

5. The vehicle manufacturer performs detailed threat analysis and understand how this applies to your its organisation in the context of the threat to its vehicle types and its sector.

P. Paragraph 7.2.2.2., part (c)

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

Explanation of the requirement

The aim of this requirement is that the manufacturer demonstrates the processes and rules they use to assess, categorize and treat risks identified.

Examples of documents/evidence that could be provided

The following standards may be applicable:

Commented [NJR3]: Similar comment as above i.e. if we need to reference ISO/SAE 21434, then referencing of its exact requirements needs to be avoided due to the possibility of tailoring by organisations.

Clause 9 (Concept phase) would also be useful to include here, as it's during the concept phase that the identification of risk occurs i.e. creation of Cybersecurity Goals.

Formatted: _Bullet 2_G, Indent: Before: 3.7 cm, Hanging: 0.8 cm, After: 0 cm, Automatically adjust right indent when grid is defined, Widow/Orphan control, Snap to grid

(a) ISO/SAE 21434, especially based on [RQ-0815-151], [RQ-0815-0413], [RQ-0815-0556], [RQ-1508-10], [RQ-08-172], [RQ-09-057], [RQ-05-06], [RQ-09-068];

(b) ISO PAS 5112;

(bc) BSI PAS 11281:2018 may be applicable for the consideration of safety and security.

The processes may consider:

(cd) Assessing the associated impact related to the risks identified in requirement 7.2.2.2. b);

(de) Identification of potential attack paths related to risks identified in requirement 7.2.2.2. b);

(ef) Determination of feasibility/likelihood of attack for every attack paths identified above;

(fg) Calculation and categorization of risks;

(gh) Treatment options of those identified and categorized risks.

The requirement should be considered unfulfilled if one of the following statements is true

1. Risk assessment outputs are too complex or unwieldy to be consumed by decision-makers and are not effectively communicated in a clear and timely manner.

2. Security requirements and mitigation techniques are arbitrary or are applied from a control catalogue without consideration of how they contribute to the security of vehicle types.

3. Only certain domains or types of asset are documented and understood. Dependencies between assets are not understood (such as the dependencies between IT and OT).

4. Inventories of assets relevant to vehicle types are incomplete, non-existent, or inadequately detailed.

5. Asset inventories are neglected and out of date.

6. Systems are assessed in isolation, without consideration of dependencies and interactions with other systems (e.g. interactions between IT and OT environments).

7. Risk assessments are not based on a clearly defined set of assumptions.

8. Risk assessments for vehicle types are a "one-off" activity (or not done at all).

The requirement may be considered fulfilled if all the following statements are true

1. The output from the vehicle manufacturer's risk management process is a clear set of security requirements that will address the risks in line with its organisational approach to security.

2. All assets relevant to the secure operation of its vehicle types are identified and inventoried (at a suitable level of detail).

3. The inventory is kept up-to-date.

4. Dependencies on supporting infrastructure are recognised and recorded.

5. The vehicle manufacturer has prioritised assets according to their importance to the operation of its vehicle types.

6. The vehicle manufacturer's risk identification is based on a clearly understood set of assumptions, informed by an up-to-date understanding of security threats to its vehicle types and its sector.

7. The vehicle manufacturer's risk identification is informed by an understanding of the vulnerabilities in its vehicle types.

Formatted: English (United Kingdom)

Commented [NJR4]: If we need to reference ISO/SAE 21434, then referencing of its exact requirements needs to be avoided due to the possibility of tailoring by organisations.

Formatted: English (United Kingdom)

8. The manufacturer can demonstrate the effectiveness and repeatability of their processes for their categorisation and treatment of risk.

Q. Paragraph 7.2.2.2., part (d)

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

Explanation of the requirement

The aim of this requirement is that the manufacturer demonstrates the processes and rules they use to decide how to manage the risks. This can include the decision criteria for risk treatment, e.g. the process for selecting what controls to implement and when to accept a risk.

The results of the process for risks identification and assessment should feed into selecting the appropriate treatment category options to address those risks. The outcome of this process should be that the residual risk (risks remaining after treatment) is within the manufacturer's stated tolerance of risks (i.e. within stated acceptable limits).

Mitigations identified in Annex 5 of the Cyber Security Regulation shall be considered in the processes.

Examples of documents/evidence that could be provided

The following standards may be applicable:

(a) ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-09-079];

(b) ISO PAS 5112;

(~~b~~c) ISO 31000 may be applicable if adapted for product related risks.

The processes may consider:

(~~c~~d) Appropriate and proportional risk treatment methodologies;

(~~d~~e) Treatment of critical elements (with safety and environment) to ensure the risks to them are appropriately mitigated and proportionately based on the safety or environmental goal of dependent vehicle systems;

(~~e~~f) Ensuring the residual risk remains within acceptable limits for components or the overall vehicle type;

(~~f~~g) Detailing any cases where the organization would accept justification for non-adherence to their stated risk tolerance.

The requirement should be considered unfulfilled if one of the following statements is true

1. The security elements of projects or programmes are solely dependent on the completion of a risk management assessment without any regard to the outcomes.

2. There is no systemic process in place to ensure that identified security risks are managed effectively.

3. Risks remain unresolved on a register for prolonged periods of time awaiting senior decision-making or resource allocation to resolve.

The requirement may be considered fulfilled if all the following statements are true

1. Significant conclusions reached in the course of the vehicle manufacturer's risk management process are communicated to key security decision-makers and accountable individuals.

2. The effectiveness of the vehicle manufacturer's risk management process is reviewed periodically, and improvements made as required.

Commented [NJR5]: If we need to reference ISO/SAE 21434, then referencing of its exact requirements needs to be avoided due to the possibility of tailoring by organisations.

R. Paragraph 7.2.2.2., part (e)

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

Explanation of the requirement

The aim of this requirement is to ensure the manufacturer has appropriate capabilities and processes for testing the vehicle type throughout its development and production phases.

Testing processes in the production phase may be different to the ones used during the development phase.

Examples of documents/evidence that could be provided

The following standards may be applicable:

(a) ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-09-~~0910~~], [RQ-10-01]. [RQ-11-01], ~~[RQ-11-02],~~ [RQ-12-01], [RQ-12-02], [RQ-12-03];

(b) ISO PAS 5112;

(~~b~~c) BSI PAS 11281:2018 may be utilised for considering the interaction of safety and security and processes for evidencing security outcomes are met.

The processes may consider:

Development Phase:

(~~c~~d) Organization specific rules for testing during development;

(~~d~~e) Processes for creation and execution of test strategies;

(~~e~~f) Processes for cybersecurity testing planning;

(~~f~~g) Processes for cybersecurity system design testing;

(~~g~~h) Processes for cybersecurity software unit testing;

(~~h~~i) Processes for cybersecurity hardware testing;

(~~i~~j) Processes for cybersecurity integration testing;

(~~j~~k) Processes for documentation of the results of testing;

(~~k~~l) Processes for handling vulnerabilities identified during testing;

(~~l~~m) Justification and requirements for cybersecurity tests, like Functional (requirement-based, positive and negative) testing, Interface testing, Penetration testing, Vulnerability scanning, Fuzz testing but not limited to the same.

Production Phase:

(~~m~~n) Processes for testing to ensure the produced system has the cybersecurity requirements, controls and capabilities outlined in the production plan;

(~~n~~o) Processes for testing to ensure the produced item meets the cybersecurity specifications which are in accordance with the system in the development phase;

(~~o~~p) Processes for testing to assure that cybersecurity controls and configuration as cybersecurity specifications are enabled in the produced item;

(~~p~~q) Processes for documenting the test results and findings handling.

The requirement should be considered unfulfilled if one of the following statements is true

1. A particular product or service is seen as a "silver bullet" and vendor claims are taken at face value.

2. Assurance methods are applied without appreciation of their strengths and limitations,

Commented [NJR6]: If we need to reference ISO/SAE 21434, then referencing of its exact requirements needs to be avoided due to the possibility of tailoring by organisations.

such as the risks of penetration testing in operational environments.

3. Assurance is assumed because there have been no known problems to date.

The requirement may be considered fulfilled if all the following statements are true

1. The vehicle manufacturer validates that the security measures in place to protect systems are effective and remain effective until the end-of-life of all vehicles under the vehicle types for which they are needed.

2. The vehicle manufacturer understands the assurance methods available to it and chooses appropriate methods to gain confidence in the security of vehicle types.

3. The vehicle manufacturer's confidence in the security as it relates to its technology, people, and processes can be justified to, and verified by, a third party.

4. Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way.

5. The methods used for assurance are reviewed to ensure they are working as intended and remain the most appropriate method to use.

S. Paragraph 7.2.2.2., part (f)

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

Explanation of the requirement

The aim of this requirement is to ensure the risk assessment is kept current. This should include processes to identify if the risks to a vehicle type have changed and how this will be considered within the risk assessment.

Sources for risk identification may be stated. These may include:

(a) Vulnerability/ Threats sharing platforms;

(b) Lessons learned regarding risks and vulnerabilities;

(c) Conferences.

It is noted that requirements 7.2.2.2. parts f) to h) may have overlaps in terms of the processes used and therefore the same evidence may be applicable to demonstrating that these requirements are met.

Examples of documents/evidence that could be provided

(d) ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on ~~[RQ-11-03],~~ [RQ-06-0~~8~~9],~~.~~ [RQ-0~~7~~8-0~~5~~7], ~~[RQ-07-06]~~;

(e) ISO PAS 5112.

Commented [NJR7]: If we need to reference ISO/SAE 21434, then referencing of its exact requirements needs to be avoided due to the possibility of tailoring by organisations.

The requirement should be considered unfulfilled if one of the following statements is true

1. No processes are in place which require the risk assessment to be updated.

The requirement may be considered fulfilled if all the following statements are true

1. The vehicle manufacturer conducts risk assessments when significant events potentially affect vehicle types, such as replacing a system or a change in the cyber security threat.

2. The vehicle manufacturer's risk assessments are dynamic and updated in the light of relevant changes which may include technical changes to vehicle types, change of use and new threat information.

T. Paragraph 7.2.2.2., part (-g)

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

Explanation of the requirement

The aim of this requirement is to ensure that the manufacturer has processes to monitor for cyber-attacks, threats or vulnerability to vehicles that the manufacturer has had type approved, i.e. are in the post-production or production phase, and that they have established processes that would permit them to respond in an appropriate and timely manner.

It is noted that requirements 7.2.2.2. parts f) to h) may have overlaps in terms of the processes used and therefore the same evidence may be applicable to demonstrating that these requirements are met.

Examples of documents/evidence that could be provided

The following standards may be applicable:

(a) ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-078-01], [RQ-078-02],. [RQ-08-03], [RQ-078-043], [RQ-078-045], [RQ-078-057], [RQ-1507-046], [RQ-15-05], [RC-1507-038], [RQ-13-01], [RQ-13-02], [RQ-13-03];

(b) ISO PAS 5112.

The following could be used to evidence the processes used:

(bc) Cyber security monitoring processes for post-production vehicles. This may include processes that will collect information that may or may not be pertinent to the manufacturer's vehicle/system;

(cd) Cyber security information assessment processes. These will be processes for the identification of the relevance of the information collected with respect to the system/vehicle of the manufacturer;

(de) Processes for risk determination/assessment for the relevant information;

(ef) Incident response procedures for both vehicles already registered and yet to be registered of the vehicle types covered by the CSMS, which may include evidence of procedures for:

(i) Interaction with authorities;

(ii) Identified or stated triggers that would lead to an escalation or action;

(iii) Determining what response options might be implemented for which condition;

(iv) Handling any dependencies and interactions with suppliers.

(fg) Evidence that the response procedures would work, for example through exercising and verification that planning assumptions remain valid under test.

The requirement should be considered unfulfilled if one of the following statements is true

1. The vehicle manufacturer has no sources of threat intelligence.

2. The vehicle manufacturer does not apply updates in a timely way, after receiving them.

3. The vehicle manufacturer does not evaluate the usefulness of its threat intelligence or share feedback with providers, authorised aftermarket service providers or other users.

4. There are no staff who perform a monitoring function.

Commented [NJR8]: If we need to reference ISO/SAE 21434, then referencing of its exact requirements needs to be avoided due to the possibility of tailoring by organisations.

Formatted: Indent: Before: 2 cm, Hanging: 1 cm

Formatted: Indent: Before: 2 cm, Hanging: 1 cm

Formatted: _Bullet 2_G, Indent: Before: 3.7 cm, Hanging: 0.8 cm, After: 0 cm, Automatically adjust right indent when grid is defined, Widow/Orphan control, Snap to grid

5. Monitoring staff do not have the correct specialist skills.

6. Monitoring staff are not capable of reporting against governance requirements.

7. Security alerts relating to vehicle types are not prioritised.

The requirement may be considered fulfilled if all the following statements are true

1. Data relating to the security and operation of vehicle types is collected.

2. Alerts from third parties are investigated, and action taken.

3. Some logging datasets can be easily queried with search tools to aid investigations.

4. The resolution of alerts to an asset or system is performed regularly.

5. Security alerts relating to vehicle types are prioritised.

6. The vehicle manufacturer applies updates in a timely way.

7. The vehicle manufacturer has processes to monitor for, detect and respond to cyber-attacks, cyber threats and vulnerabilities which are relevant to its business needs, or specific threats in its sector.

8. The vehicle manufacturer knows how effective its processes are (e.g. by tracking how they helps it identify security problems).

9. Monitoring staff have appropriate investigative skills and a basic understanding of the data they need to work with.

10. Monitoring staff can report to other parts of the organisation (e.g. security directors, resilience managers).

11. The vehicle manufacturer successfully demonstrates the processes to evaluate whether the cyber security measures implemented are robust enough to conclude whether they are still effective.

U. Paragraph 7.2.2.2., part (h)

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

Explanation of the requirement

The intention of this requirement is to ensure that a process has been established to provide the data required for analysis and associated responsibilities for handling the data and analysis.

Examples of documents/evidence that could be provided

The following standards may be applicable:

(a) ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-078-034];

(b) ISO PAS 5112.

~~*Examples of documents/evidence that could be provided*~~

The following could be used to evidence the processes used:

(b) Procedure for implementing Security Incident Response Team activities (incidents);

(c) Field monitoring (obtaining information on incidents and vulnerabilities);

(d) Procedure when an incident occurs (including an overview of what information is passed to the analyst in what steps);

Commented [NJR9]: If we need to reference ISO/SAE 21434, then referencing of its exact requirements needs to be avoided due to the possibility of tailoring by organisations.

(e) Procedure when a vulnerability is discovered (including an overview of what information is passed to the analyst in what steps).

V. Paragraph 7.2.2.3.

"7.2.2.3. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that, based on categorization referred to in paragraph 7.2.2.2. (c) and 7.2.2.2. (g), cyber threats and vulnerabilities which require a response from the vehicle manufacturer shall be mitigated within a reasonable timeframe."

Explanation of the requirement

The intention of this requirement is to ensure that after the identified risks have been classified, a process has been established to determine the response time limit based on the classification results.

It is necessary to set the response deadline by processes such as triage and explain the monitoring process to see if it is executed within the deadline.

The timeframes provided by the manufacturers should be able to be justified and explained. There may be a set of timeframes covering different possible situations. This should include timeframes for deciding and implementing possible reactions or responses.

Examples of documents/evidence that could be provided

The following standards may be applicable:

(a) ISO/SAE 21434 can be used as the basis for evidencing the required processes, especially based on [RQ-05-02] b).

~~*Examples of documents/evidence that could be provided*~~

(b) ISO PAS 5112.

The following could be used to evidence the processes used:

(a~~c~~) Procedure for implementing cyber security incident response activities, including:

(i) Field monitoring (obtaining information on incidents and vulnerabilities);

(ii) Procedure for incident handling, including how the timeframe to respond is determined;

(iii) Procedures for discovering vulnerabilities.

(b~~d~~) Demonstration of how the procedures are implemented.

W. Paragraph 7.2.2.4.

"7.2.2.4. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that the monitoring referred to in paragraph 7.2.2.2. (g) shall be continual. This shall:

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

(b) Include the capability to analyse and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs. This capability shall respect paragraph 1.3. and the privacy rights of car owners or drivers, particularly with respect to consent."

Explanation of the requirement

The intention of this requirement is to ensure that processes of monitoring for cyber-attacks, cyber threats and vulnerabilities on vehicle types are continual and apply to all registered

Formatted: _ H_5/6_G, Justified

Formatted: _Bullet 1_G, Left, Indent: Before: 3 cm, After: 0 cm, Automatically adjust right indent when grid is defined, Widow/Orphan control, Snap to grid

Commented [NJR10]: If we need to reference ISO/SAE 21434, then referencing of its exact requirements needs to be avoided due to the possibility of tailoring by organisations.

Formatted: _Bullet 1_G, Left, Indent: Before: 3 cm, After: 0 cm, Automatically adjust right indent when grid is defined, Widow/Orphan control, Snap to grid

Formatted: _Bullet 2_G, Indent: Before: 3.7 cm, Hanging: 1.05 cm, After: 0 cm, Automatically adjust right indent when grid is defined, Widow/Orphan control, Snap to grid

vehicles of the manufacturer that fall within the scope of their Cyber Security Management System and use:

(a) the information on monitoring acquired in accordance with 7.3.7. in addition to other sources of information on monitoring acquired in accordance with 7.2.2.2. (g) (such as social media).

It is noted that paragraph 1.3., and compliancy with data privacy laws, are particularly relevant to this requirement,

Examples of documents/evidence that could be provided

The following standards may be applicable:

(a) ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on clauses ~~7~~8.3 "Cybersecurity Monitoring", ~~7~~8.4 "Cybersecurity event ~~assessment~~evaluation", ~~7~~8.5 "Vulnerability analysis.

(b) ISO PAS 5112.

~~*Examples of documents/evidence that could be provided*~~

The following could be used to evidence the processes used:

(b) Procedure for implementing cyber security incident response activities, including:

(i) Field monitoring (obtaining information on incidents and vulnerabilities)

(ii) Procedure for incident handling

(iii) Procedures for discovering vulnerabilities

(c) Demonstration of how the procedures are implemented.

Formatted: _Bullet 1_G, Left, Indent: Before: 2.7 cm, Hanging: 0.8 cm, After: 0 cm, Automatically adjust right indent when grid is defined, Widow/Orphan control, Snap to grid

X. Paragraph 7.2.2.5.

"7.2.2.5. The vehicle manufacturer shall be required to demonstrate how their Cyber Security Management System will manage dependencies that may exist with contracted suppliers, service providers or manufacturer's sub-organizations in regards of the requirements of paragraph 7.2.2.2."

Explanation of the requirement

The intention of this requirement is to ensure that it can be shown that risks from suppliers are able to be known and can be managed within the processes described in the CSMS. The steps taken should be proportionate to the risks from what is supplied.

The final implementation of the processes may be incorporated into bilateral agreement between the vehicle manufacturer and their suppliers.

Within the CSMS there may be processes to:

(a) identify risks associated with parts, components, systems or services provided by suppliers;

(b) manage risks to the vehicle coming from service providers providing connectivity functions or services that a vehicle may rely on, this may include for example cloud providers, telecom providers, internet providers and authorised aftermarket service providers;

(c) ensure contracted suppliers and/or service providers are able to evidence how they have managed risks associated with them. The processes may include consideration of validation or testing requirements that may be used to evidence that risks are appropriately managed;

(d) delegate relevant requirements to relevant departments or sub-organisations of the manufacturer, in order to manage risks identified.

It is noted that it is possible to put requirements on Tier1 suppliers and to require they cascade it to Tier 2 suppliers. However, it may be difficult for a manufacturer to cascade requirements further down in the supply chain (especially legally binding requirements).

Examples of documents/evidence that could be provided

The following standards may be applicable:

(e) ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-06-~~09~~10], [RQ-~~15~~07-0~~3~~4], [RC-~~15~~07-0~~2~~5];

(f) ISO PAS 5112.

The following could be used to evidence the processes used:

(~~f~~g) Contractual agreements in place or evidence of such agreements;

(g~~h~~) Evidenced arguments for how their processes will ensure suppliers / service providers will be considered in the risk assessment process;

(~~h~~i) Procedures/Methods of sharing information on risk between suppliers and manufacturers;

(~~i~~j) Existing solutions / contracts like ISMS (Information Security Management System) regulation can be used for evidence. This may be evidenced by certificates based on ISO/IEC 27001 or TISAX (Trusted Information Security Assessment eXchange).

The requirement should be considered unfulfilled if one of the following statements is true

1. Relevant contracts with suppliers and service providers do not have cyber security requirements.

The requirement may be considered fulfilled if all the following statements are true

1. The vehicle manufacturer has a deep understanding of its supply chain, including sub-contractors and the wider risks it faces. The vehicle manufacturer considers factors such as supplier's partnerships, competitors, nationality and other organisations with which they sub-contract. This informs its risk assessment and procurement processes.

2. The vehicle manufacturer's approach to supply chain risk management considers the risks to its vehicle types arising from supply chain subversion by capable and well-resourced attackers.

3. The vehicle manufacturer has confidence that information shared with suppliers that is essential to the operation of your vehicle types is appropriately protected from sophisticated attacks.

4. The vehicle manufacturer can clearly express the security needs it places on suppliers in ways that are mutually understood and are laid in contracts. There is a clear and documented shared-responsibility model.

5. All network connections and data sharing with third parties is managed effectively and proportionately.

6. When appropriate, the vehicle manufacturer's incident management process and that of its suppliers provide mutual support in the resolution of incidents.

Y. Paragraphs 7.3. to 7.3.1.

"7.3. Requirements for vehicle types

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

Commented [NJR11]: If we need to reference ISO/SAE 21434, then referencing of its exact requirements needs to be avoided due to the possibility of tailoring by organisations.

However, for type approvals prior to 1 July 2024, if the vehicle manufacturer can demonstrate that the vehicle type could not be developed in compliance with the CSMS, then the vehicle manufacturer shall demonstrate that cyber security was adequately considered during the development phase of the vehicle type concerned."

Explanation of the requirement

The intention of this requirement is to ensure that there is a valid Certificate of Compliance for CSMS to enable type approval to be given for any new vehicle type and that it is appropriate to the vehicle type.

The following clarification should be noted:

(a) "relevant to the vehicle type being approved." means the CSMS should be applicable to the vehicle type being approved.

Examples of documents/evidence that could be provided

The following could be used to evidence the validity of the CSMS certificate:

(b) The Certificate of Compliance for CSMS to demonstrate it is still valid;

(c) Confirmation that the CSMS is appropriately applied to the vehicle type and any information required to provide assurance.

Z. Paragraph 7.3.2.

"7.3.2. The vehicle manufacturer shall identify and manage, for the vehicle type being approved, supplier-related risks"

Explanation of the requirement

This requirement specifically references gaining sufficient information from the supply chain and is linked to 7.2.2.5. The intention of this requirement is to ensure that information presented (together with that from the manufacturer) is sufficient to allow an assessment to be conducted of the requirements 7.3.3. to 7.3.6.

The following clarification should be noted:

(a) "supplier-related risks" - The aim is that it can be shown that risks from suppliers are able to be known and can be managed. It is accepted that it is difficult to cascade requirements down in the supply chain beyond Tier 2 suppliers and ensure they are legally binding.

Examples of documents/evidence that could be provided

The following standards may be applicable:

(b) ISO/SAE 21434.;

(c) ISO PAS 5112.

The following could be used to evidence the processes used:

(c) Evidence in the form of contract sections with suppliers that deal with the requirements of this regulation.

AA. Paragraph 7.3.3.

"7.3.3. The vehicle manufacturer shall identify the critical elements of the vehicle type and perform an exhaustive risk assessment for the vehicle type and shall treat/manage the identified risks appropriately. The risk assessment shall consider the individual elements of the vehicle type and their interactions. The risk assessment shall further consider interactions

with any external systems. While assessing the risks, the vehicle manufacturer shall consider the risks related to all the threats referred to in Annex 5, Part A, as well as any other relevant risk."

Explanation of the requirement

The intention of this requirement is that the vehicle manufacturers shall identify the critical elements of a vehicle type with respect to cyber security and provide justification for how risks related to them are managed.

The manufacturer should be able to provide justification for why they have identified elements of a vehicle type as critical (or not).

The following clarifications should be noted

(a) Critical elements may be elements contributing to vehicle safety, environment protection or theft protection. They could be parts which provide connectivity. They may also be parts of the vehicle architecture which are critical for sharing information or cyber security (e.g. gateways could be also considered critical);

(b) The intention of this requirement is to ensure that risks shall be appropriately processed / managed by considering all threats including Annex 5, Part A and judging the necessity of countermeasures based on the results of risk analysis and risk evaluation;

(c) The intention of this requirement is to allow the vehicle manufacturer to demonstrate the application of the relevant process in requirements 7.2.2.2. and 7.2.2.4. of the CSMS to the vehicle type;

(d) The approval authority or technical service shall refer to Annex 5 of the Cyber Security Regulation to aid their assessment of the manufacturer's risk assessment;

(e) The consideration of risks should consider the requirements of 7.3.4. and the requirement for proportionate mitigations;

(f) The consideration of the threats and mitigations of Annex 5 within a risk assessment may lead to ratings like "not relevant" or "negligible risks".

Examples of documents/evidence that could be provided

The following standards may be applicable:

(g) ISO/SAE 21434 ~~describes the way to define the concept. This also includes the consideration of critical elements based on risk treatment decisions. The results are documented in "Cybersecurity goals" and "Cybersecurity concept". If further describes exhaustive risk assessment in clause 8 "Risk assessment methods". This is documented in Threat analysis and risk assessment~~ can be used as the basis for evidencing and evaluating as required, especially based on clauses 9.5 "Cybersecurity concept" and 15 "Threat analysis and risk assessment methods";

(h) ISO PAS 5112 may be used;

(~~h~~i) ETSI TS 103 645 may be used for demonstrating the security of Internet of Things elements of a vehicle;

(~~i~~j) BSI PAS 1885 may be used.

The following could be used to evidence this requirement:

(j) The vehicle type claimed;

(k) An explanation of why elements within the vehicle type are critical;

(l) What security measures are implemented, including information on how they work;

(m) Information on any security measures should permit the Technical Service/ Approval Authority to both be assured that they do what the manufacturer intends and that

Commented [NJR12]: Much of this is out-of-date and incorrect. Overall, it would be better to stick to the prose used above. See following marked-up changes as a proposal.

vehicles in production will use the same measure as presented to the Approval Authority/Technical Service for the vehicle type. Confidentiality of specifics and how these are handled should be agreed and recorded.

AB. Paragraph 7.3.4.

"7.3.4. The vehicle manufacturer shall protect the vehicle type against risks identified in the vehicle manufacturer's risk assessment. Proportionate mitigations shall be implemented to protect the vehicle type. The mitigations implemented shall include all mitigations referred to in Annex 5, Part B and C which are relevant for the risks identified. However, if a mitigation referred to in Annex 5, Part B or C, is not relevant or not sufficient for the risk identified, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented.

In particular, for type approvals prior to 1 July 2024, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented if a mitigation measure referred to in Annex 5, Part B or C is technically not feasible. The respective assessment of the technical feasibility shall be provided by the manufacturer to the approval authority."

Explanation of the requirement

The intention of this requirement is to ensure that vehicle manufacturers implement appropriate mitigation measures in accordance with the results of their risk assessment.

The manufacturer should provide reasoned arguments and evidence for the mitigations they have implemented in the design of the vehicle type and why they are sufficient. This may include any assumptions made, for example about external systems that interact with the vehicle.

The technical mitigations from Annex 5, Parts B and C shall be considered wherever applicable to the risks to be mitigated. The Manufacturer may present a rationale not only for a listed mitigation from Annex 5 being "not relevant or not sufficient", but also may present a rationale, that another mitigation other than the ones listed in Annex 5 is appropriate to the respective risk. That rationale may be substantiated by a risk assessment and risk rating showing the appropriateness of the alternative mitigation. This is to allow the adoption of new or improved defensive technologies.

The following clarifications should be noted:

(a) The design decisions of the manufacturer should be linked to the risk assessment and risk management strategy. The manufacturer should be able to justify the strategy implemented;

(b) The term "proportionate" should be considered when choosing whether to implement a mitigation and what mitigation should be implemented. If the risk is negligible then it may be argued that a mitigation would not be necessary;

(c) Protection from identified risks means to mitigate the risk.

Examples of documents/evidence that could be provided

The following standards may be applicable:

(d) ISO/SAE 21434 describes the identification of risk and the deduced ~~C~~cybersecurity goals and cybersecurity concept based on the identified risks. The results are documented in [WP-09-0~~4~~3] Cybersecurity goals and [WP-09-0~~7~~6] Cybersecurity concept;

(e) ISO PAS 5112;

(~~e~~f) BSI PAS 11281: 2018 and other standards regarding claims, arguments and evidence may be used to justify the design decisions of the manufacturer.

The following could be used to evidence the mitigations used:

(~~f~~g) Evidence that mitigation measures were introduced according to the necessity of measures, this includes:

(i) the reason, if mitigation measures other than Annex 5 Part B and C are applied;

(ii) the reason, if mitigations listed in Annex 5 are not applied;

(iii) the reason, if mitigation measures are determined to be unnecessary.

Formatted: _Bullet 2_G, Indent: Before: 3.7 cm, Hanging: 0.8 cm, After: 0 cm, Automatically adjust right indent when grid is defined, Widow/Orphan control, Snap to grid

AC. Paragraph 7.3.5.

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

The following clarifications should be noted:

(a) "appropriate and proportionate measures" requires that the manufacturer is able to justify how risks associated with any dedicated environment, as defined in their risk assessment, are managed;

(b) Dedicated environments can be on the vehicle. If the vehicle interacts with servers or services located off the vehicle (for example in the cloud) then the risks to the vehicle originating from them, with respect to their cyber security, should be considered.

Examples of documents/evidence that could be provided

The following standards may be applicable:

(c) ISO/SAE 21434 describes on a process base steps to make conclusion for the architecture. This aspect is to be considered in [WP-~~0~~815-03] Threat scenarios.

Commented [NJR13]: Text does not make sense. Also, reference to clauses 9 and 10 might be a better reference here, as they provide a more complete process than just WP-15-03.

(d) ISO PAS 5112.

The following could be used to evidence this requirement:

(~~d~~e) A description of the dedicated environment;

(~~e~~f) What security measures are implemented, including information on how they work;

(~~f~~g) Information on any security measures should permit the Approval Authority/Technical Service to both be assured that they do what the manufacturer intends and that vehicles in production will use the same measure as presented to the Approval Authority/Technical Service for the vehicle type. Confidentiality of specifics and how these are handled should be agreed and recorded;

(~~g~~h) Annex 5 of the cyber security Regulation shall be referred to.

AD. Paragraph 7.3.6.

"7.3.6. The vehicle manufacturer shall perform, prior to type approval, appropriate and sufficient testing to verify the effectiveness of the security measures implemented."

Explanation of the requirement

The test results should be valid at time of type approval. The Technical Service may perform security tests to confirm the results.

The following clarifications should be noted:

(a) The aim of any security measures will be to reduce the risks. Testing should support justification for the security measures implemented.

Examples of documents/evidence that could be provided

The following standards may be applicable:

(b) Manufacturers may describe the verification and validation measure implemented in accordance with ISO/SAE 21434 in the form of [WP-09-087] Verification report ~~of~~ for the cybersecurity concept, [WP-10-034] Verification report for the ~~refined~~ cybersecurity specification, [WP-11-021] Validation report.

The following could be used to evidence this requirement:

(c) What is tested and why (e.g. what measures of success for the test look like);

(d) Methodology used and why (e.g. this may include notes on the extent and effort contained within the testing);

(e) Who has performed the tests and why (e.g. in-house, a supplier or an external organization and any relevant information regarding their qualification/experience);

(f) Confirmation of its successful outcome (this may include the pass/fail criteria and result of the test).

AE. Paragraph 7.3.7.

"7.3.7. The vehicle manufacturer shall implement measures for the vehicle type to:

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

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

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

Explanation of the requirement

The intention of this requirement is to ensure that there are specific measures implemented for the vehicle type to monitor for changes in the threat landscape, detect and prevent cyber-attacks and have the capability to forensically support the analysis of any attempted or successful attack.

The following clarifications should be noted:

(a) Measures with regard to this clause may be implemented on the vehicle type or in its operational environment, e.g. the backend, the mobile network "for the vehicle type";

(b) Measures should primarily look to prevent cyber-attacks being successful, with reference to 7.3.4. and 7.3.5. to protect against risks identified in the risk assessment;

(c) Measures to prevent cyber-attacks being successful against all vehicles of a vehicle type may additionally be delivered asynchronously, i.e. after the actual event of a cyber-attack and its analysis;

(d) Data forensic capability may include the ability to provide and analyse log data, diagnostic error codes, vehicle operational information, backend information to investigate cyber-attacks;

(e) Data forensic capability may include a circular buffer of persisting log data that supports investigatory procedures.

It is noted that paragraph 1.3., and compliancy with data privacy laws, are particularly relevant to this requirement.

Examples of documents/evidence that could be provided

The following standards may be applicable:

(f) ISO/SAE 21434. ~~A list of s~~Sources for cybersecurity ~~monitoring~~ information

is provided in ~~clause 7.3~~[WP-08-01], along with triggers (e.g. key words, reference for configuration information, names of components or suppliers) for those sources in [WP-08-02]. The results of analysis and how to document it is described in [WP-0~~7~~8-0~~4~~5] Vulnerability analysis.

Commented [NJR14]: It would be better, and more in alignment with sections above, to just reference all of clause 8, as that clause provides processes for meeting all of the above quoted requirements.

The following could be used to evidence this requirement:

(g) Attack prevention measures applied to the vehicle type;

(h) Demonstration of how a vehicle type's preventive measures and monitoring activities perform;

(i) Demonstration of how forensic analysis is performed.

AF. Paragraph 7.3.8.

"7.3.8. Cryptographic modules used for the purpose of this Regulation shall be in line with consensus standards. If the cryptographic modules used are not in line with consensus standards, then the vehicle manufacturer shall justify their use."

The following clarifications should be noted:

A consensus standard may be an internationally recognised standard, or it may be a national standard that is commonly used, e.g. FIPS.

Explanation of the requirement

The intent of this requirement is to ensure encryption methods used can be justified.

Examples of documents/evidence that could be provided

Where encryption measures are implemented, based on the results of risk analysis and risk assessment, the manufacturer should be able to:

(a) Explain whether the encryption algorithm or measure complies with a current consensus standard; and

(b) Explain the reason for the choice of encryption and why it adequately mitigates the risk identified.

AG. Paragraph 7.4.

"7.4. Reporting provisions

7.4.1. The vehicle manufacturer shall report at least once a year, or more frequently if relevant, to the Approval Authority or the Technical Service the outcome of their monitoring activities, as defined in paragraph 7.2.2.2.(g)), this shall include relevant information on new cyber-attacks. The vehicle manufacturer shall also report and confirm to the Approval Authority or the Technical Service that the cyber security mitigations implemented for their vehicle types are still effective and any additional actions taken."

Explanation of the requirement

The main purpose of this requirement is to confirm that the aspects of the CSMS related to the cyber security monitoring activities, as defined in paragraph 7.2.2.2.(g), continue to be applied properly after Development Phase and that the relevant cyber security mitigations implemented continue to be effective.

The manufacturer shall at least annually report to the Type Approval Authority who granted the type approval or the Technical Service who verified the compliance of its CSMS with this Regulation. The reporting should be more frequent if events such as new cyber-attacks are observed, especially to report on any actions taken.

Examples of documents/evidence that could be provided

The following standards may be applicable:

(a) ISO/SAE 21434 defines [WP-0~~7~~8-0~~2~~3] Cybersecurity events~~Results from the triage of cybersecurity information~~, [WP-08-04] Weaknesses from cybersecurity events, and [WP-0~~7~~8-0~~4~~5] Vulnerability Analysis. ~~Both~~ All three can be used as the baseline for the required reporting.

(b) ISO PAS 5112.

Commented [NJR15]: It might be better just to reference all of clause 8, as that clause provides processes for meeting all of the above quoted requirements.

AH. Paragraph 7.4.2.

"7.4.2. The Approval Authority or the Technical Service shall verify the provided information and, if necessary, require the vehicle manufacturer to remedy any detected ineffectiveness.

If the reporting or response is not sufficient the Approval Authority may decide to withdraw the CSMS in compliance with paragraph 6.8."

No guidance included in this document with regards this requirement

AI. Paragraph 8.

"8. Modification and extension of the vehicle type"

Examples of documents/evidence that could be provided

The following table gives some examples for modifications of E/E architectures and the potential impact on the vehicle type with regard to this regulation.

Note, the examples given are indicative of what may be considered but should not be viewed as limiting. When applied the example of changes given may result in a different outcome.

		Possible **changes** in the E/E Architecture	Impact on type	Examples
New type	**Development of a new E/E Architecture**		Development of an E/E Architecture requires a **new type**.	Development of an E/E Architecture requires a **new type**.
New type	**Change to the outcome of risk assessment by introducing new**		Requires a **new type**, since security in existing subsystem is being influenced.	• Adding new external interfaces (NFC Near Field Communication) for new services such as personalization • Change of network topology by adding a new gateway
Extension of existing type	**Minor changes to the outcome of risk assessment by adding or replacing subsystems**	 	Replacing an existing subsystem or adding a new subsystem, and this introduces some minor changes to the cybersecurity of the resulting E/E architecture, and **thus requires a type extension**.	• Replacing a UMTS communication unit by a 5G communication unit -> additional communication possible • Replacing an ECU by a new one with a HSM (hardware security module)
No impact	**No change of outcome of risk assessment**		Replacing an existing subsystem, and this does not change the cybersecurity of the resulting E/E architecture, and thus does **not require a type extension**. **<u>This is the usual situation</u>**.	Replacing an ECU: new state of the art processor, more memory, no

AJ. Paragraphs 9. to 12.

"9. Conformity of production

10. Penalties for non-conformity of production

11. Production definitively discontinued

12. Names and addresses of Technical Services responsible for conducting approval test, and of Type Approval Authorities"

No guidance included in this document with regards this requirement

4. Guidance regarding Annex 1, the Information Document

A. Paragraphs 9. to 9.1.

"9. Cyber Security

9.1. General construction characteristics of the vehicle type, including:

(a) The vehicle systems which are relevant to the cyber security of the vehicle type;

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

(c) The interactions of those systems with other systems within the vehicle type and external interfaces."

Examples of documents/evidence that could be provided

Shall be a written description of the E/E architecture

B. Paragraph 9.2.

"9.2. Schematic representation of the vehicle type"

Examples of documents/evidence that could be provided

Shall be a schematic of the E/E architecture – e.g. circuit diagram

C. Paragraphs 9.3. to 9.8.

"9.3. The number of the Certificate of Compliance for CSMS:

9.4. Documents for the vehicle type to be approved describing the outcome of its risk assessment and the identified risks:

9.5. Documents for the vehicle type to be approved describing the mitigations that have been implemented on the systems listed, or to the vehicle type, and how they address the stated risks:

9.6. Documents for the vehicle type to be approved describing protection of dedicated environments for aftermarket software, services, applications or data:

9.7. Documents for the vehicle type to be approved describing what tests have been used to verify the cyber security of the vehicle type and its systems and the outcome of those tests:

9.8. Description of the consideration of the supply chain with respect to cyber security:"

No guidance included in this document with regards this requirement

5. Template for data exchange via DETA in accordance with paragraph 5.3.

Important Note:

Information obtained through DETA for the purpose of information sharing scheme which is defined in the UN Regulation shall be protected in a secure manner. This information shall not be used for other purposes rather than vehicle type approval and certification of cyber security management system for vehicle type.

5.1. Description of CSMS auditing

For the description of the CSMS audit the approval authority shall provide the following information to DETA.

5.1.1. Auditing process

Contact data of the approval authority and its organisational unit responsible for the audit process shall be provided.

The audit process should be documented in a process flow chart, including possible iterative steps and remediation workflow.

(Flow chart)

The chronological workflow of the audit should be documented in table format.

Audit phase	*Start date / time span*	*Resource requirement (in man-days)*
Pre-audit, if required *e.g. involvement of auditors in productive processes, planning of audit, adaptation of audit workflow*		
Document handover		
Preparation for audit activities *Including document review, e.g. sort, check for completeness, audit of contents*		
Conducting the on-site audit		
Assessment of rectification efforts *e.g. rectifications completed by auditee during the audit may address findings of the audit*		
Preparation and distribution of the audit report		
Findings from the audit		
Review of findings and rectifications by applicant (where applicable)		
Audit completion		

If deemed necessary additional information concerning the audit phases can be documented in the table below.

Audit-phase	*Remarks*

The information shall also include the workflow for verification measures according to UN Regulation No. 155, paragraphs 6.8. and 6.10. and re-audit according to UN Regulation No. 155, paragraph 6.10.

5.1.1.1. Conducting the On-site audit

If on-site assessments of the CSMS of applicants are part of the audit process, then the workflow and basic principles (rationale) of these shall be described.

5.1.1.2. Handling of findings and rectification efforts

This chapter describes the workflow associated with the rectification efforts of the auditee to address the audit findings.

(The respective workflow should be included in the flow chart in 5.1.1.)

5.1.1.3. Samples of application forms

A sample form for the application, for CSMS certification shall be documented.

5.1.1.4. References to standards and specifications

Any standard, specification or other external document on which (parts of) the audit process and assessment criteria are based shall be referenced.

5.1.2. Qualification requirements and auditing team setup

Here the minimum requirements of the approval authority on technical services and auditors conducting CSMS assessments shall be laid down. The positions in a potential auditing team shall be listed. Qualifications shall be attributed to auditing team position.

5.1.2.1. Potential auditing team setup

Position *Examples*	*Staffing requirement* *Examples*	*Tasks/remarks* *Examples*
Lead auditor	*1*	*Manage audit process; accountable and responsible*
CS process expert	*2*	*Responsible for process audit; ideally personal staffing overlap with type approval assessor team*
Product expert	*1*	…
…	…	
Documentation Management		

5.1.2.2. Qualification requirements

Qualification	*Concerned Positions*	*Minimum requirement*	*Evidence*
Educational achievements	*Example:* *Lead auditor, CS process expert*	*Example: University degree in computer science, mathematics, physics, engineering or similar.*	*Example: Diploma or certificate.*
Work experience		*Example: Five years of job experience including two years in the field of information security.*	*Example: Job reference.*
Practical experience			
Further trainings			

Accreditations			

5.1.3. Auditing requirements

In this chapter auditing requirements shall be listed. These shall be the evidence deemed sufficient by the approval authority to prove that all requirements as listed in paragraphs 7.2.2.1. to 7.2.2.5. are met by the manufacturer. (Including type approvals prior to 1 July 2024).

Requirements should include the prospective rational to decide if cyber security was adequately considered during the development phase of the vehicle type.

5.1.3.1. Formal requirements

In case formal requirements are set by the approval authority these shall be listed here. Formal requirements include the requirement for certifications, permits and licences for example.

Formal requirement	*Version / edition, date*
For example: ISO 27001 certification	

5.1.3.2. Required information

In this Chapter a structured list of the documentation which the auditing body requires from the audited entity should be provided. Any formal requirements on the documentation shall be stated here.

*Note: This could contain a list of topics that need to be addressed. A reference to documentation requirements from standard*s ~~*certifications like*~~*such as ISO/SAE 21434 and/or ISO PAS 5112 is also possible.*

Commented [NJR16]: ISO/SAE 21434 and ISO PAS 5112 do not define a certification.

5.1.3.3. Assessment of documentation

In this chapter details on the assessment rationale for the received documentation should be provided. There will be some general assessment criteria that apply to all documentation, e.g. that they are controlled, being used, are accessible, being reviewed, etc.

No.	*Title*	*Description*	*Remarks*	*Assessment rationale*
1				Note: This should contain the different levels of rationales. The level of the integration of the procedures (to assure that procedures are relevant to each other) rationales related to requirements and rationales.
2				

5.1.3.4. Auditing Questionnaire

<Focus Area 1*(e.g. threat analysis)*>

Requirement	*Audit question*	*Intent/purpose of question*	*Minimum performance criteria*	*Best practice*	*Additional information/context1*

<Focus Area 2 *(e.g. risk management)*>

Requirement	*Audit question*	*Intent/purpose of question*	*Minimum performance criteria*	*Best practice*	*Additional information/context1*

5.2. Description of type approval

5.2.1. Approval process

Contact data of the approval authority and its organisational unit responsible for the type approval process shall be provided.

The approval process should be documented in a process flow chart.

(Flow chart)

5.2.2. Qualification requirements and assessor team setup

Here the minimum requirements of the approval authority on technical services assessing the type approval requirements shall be laid down. The positions in a potential assessment team shall be listed. Qualifications shall be attributed to team position.

5.2.2.1. Potential auditing team setup

Position *Examples*	*Staffing requirement*	*Tasks/remarks*
Lead assessor	*1*	*Manage assessment process; accountable and responsible*
CS process expert	*1*	*Responsible for transferring CSMS knowledge and understanding to the assessment of the vehicle type; ideally personal staffing overlap with CSMS audit team*
CS Product expert	*2*	
Penetration tester	*1-2*	
…		
Documentation Management		

[1] If relevant, the circumstances in which the question can be asked or omitted or possible variations depending on the context etc.)

5.2.2.2. Qualification requirements

Assessor qualification	*Concerned positions*	*Minimum requirement*	*Evidence*
Educational achievements	*Example: lead assessor, product expert*	*Example: University degree in computer science, mathematics, physics, engineering or similar.*	*Example: Diploma or certificate.*
Work experience		*Example: Five years of job experience including two years in the field of information security.*	*Example: Job reference.*
Practical experience		*Example: Experience with automobile E/E architectures and experience with cybersecurity assessment and penetration testing*	*Example: Job or project reference.*
Further trainings			
Accreditations			

5.2.3. Assessment requirements

In this chapter measures fit for assessing if the vehicle manufacturer has taken the necessary measures referred to in subparagraph 5.1.1.

5.2.3.1. General assessment measures

These shall be the measures deemed sufficient by the approval authority to verify that:

(a) the CSMS certificate is relevant for the vehicle type under approval.

Risk Management

(b) the vehicle manufacturer has taken sufficient measures to identify and manage, for the vehicle type being approved, supplier-related risks, including the required standards for such risk management.

Risk Identification

(c) the vehicle manufacturer has identified the critical elements of the vehicle type;

(d) the definition of "critical elements";

(e) the vehicle manufacturer has performed an exhaustive risk assessment for the vehicle type, as required under subparagraph 7.3.3. of the Regulation.

Risk Mitigation

(f) the vehicle type is protected against risks identified in the vehicle manufacturer’s risk assessment;

(g) the mitigations applied by the manufacturer are proportionate, including the explanation of the interpretation of the term "proportionate";

(h) the reasons to support that the mitigations referred to in Annex 5, Part B or C are not relevant, not sufficient for the risk identified or not feasible;

(i) "another mitigation" implemented by the manufacturer pursuant to subparagraph 7.3.4. is "appropriate".

Monitoring and response

(j) the principles was laid out in the respective CSMS to monitor threats and respond to possible incidents have been thoroughly applied to the vehicle type and are effectively in place;

(k) effectiveness and efficiency of implemented mitigation measures has been tested and will be monitored.

The approval authority shall comprehensively lay down the evaluation standards used for the above verification.

2.3.2. Documentation requirements

Required documentation and expected main content of the documents shall be listed. The documentation shall be fit to assess the requirements as listed in 2.3.1.

2.3.3. Technical assessment

The technical assessment strategy shall be laid out. This shall include the tests and testing strategy envisaged/applied to verify that that the vehicle manufacturer has implemented the cyber security measures as required by the regulation and documented by the manufacturer. The testing strategy shall consider tests executed by third parties. *E.g. tests executed by specialized technical services or service providers, manufacturer's subcontractors or research institutions, as either initiated by the manufacturer or approval authorities.*

The strategy used for replicating manufacturer tests shall also be included.

Note: while the assessment measures in 2.3.1. are thought to include the assessment of past tests as documented by the manufacturer, the replication strategy shall lay down the rationale for choosing test which to replicate and how to replicate them.

6. Link with ISO/SAE ~~DIS~~ 21434 (E)

The following table provides a summary of the link between the requirements of the Regulation and the relevant paragraphs of ISO/SAE ~~DIS~~ 21434.

Paragraph	*Clauses from ISO/SAE ~~DIS~~ 21434*
7.2.1. For the assessment the Approval Authority or its Technical Service shall verify that the vehicle manufacturer has a Cyber Security Management System in place and shall verify its compliance with this Regulation.	
Verify that a Cyber Security Management System is in place	*Not applicable*
7.2.2.1. The vehicle manufacturer shall demonstrate to an Approval Authority or Technical Service that their Cyber Security Management System applies to the following phases: - Development phase; - Production phase; - Post-production phase.	
Development phase	Clauses 7, 8, 9, 10, 11~~, 15~~
Production phase	Clause 8, 12
Post-production phase	Clauses 7, 8, 13, 14~~, 15~~
7.2.2.2. (a) The processes used within the manufacturer's organization to manage cyber security	
Organization-wide cyber security policy	[RQ-05-01], [RQ-05-03]
Management of cyber security relevant processes	[RQ-05-02], [RQ-05-089]
(a3) Establishment and Maintenance of cyber security culture and awareness	[RQ-05-0~~7~~6]~~,~~, [RQ-05-0~~8~~7]
7.2.2.2. (b) The processes used for the identification of risks to vehicle types. Within these processes, the threats in Annex 5, Part A, and other relevant threats shall be considered.	
(b1) Process for identifying cyber security risks to vehicle types established across development, production, and post-production	[RQ-~~08~~15-01]~~,~~ [RQ-~~08~~15-02], [RQ-~~08~~15-03], [RQ-~~08~~15-08], [RQ-~~08~~15-09]. The threats in Annex 5 of UN Regulation No. 155. are out of scope of ISO/SAE 21434

Commented [NJR17]: Continual cybersecurity activities (clause 8) is relevant for all phases of the vehicle lifecycle, so development and product, not just post-production.

Commented [NJR18]: Clause 15 of the DIS is now clause 7, and clause 7 of the DIS is now clause 8.

Commented [NJR19]: FYI, RQ-15-09 in the IS is a different requirement to RQ-08-09 in the DIS, despite it being new however, it is relevant here.

7.2.2.2. (c) The processes used for the assessment, categorization and treatment of the risks identified	
(c1) Is a process established to assess and categorize cyber security risks for vehicle types across development, production and post-production?	[RQ-0815-115], [RQ-0815-04], [RQ-0815-056], [RQ-0815-10]
(c2) Is a process established to treat cyber security risks for vehicle types across development, production and post-production?	[RQ-0815-127], [RQ-09-075], [RQ-05-06], [RQ-09-068]
7.2.2.2. (d) The processes in place to verify that the risks identified are appropriately managed	
(d1) Is a process established to verify appropriateness of risk management?	[RQ-09-079]
(e) The processes used for testing the cyber security of a vehicle type	
(e1) Is a process established to specify cyber security requirements?	[RQ-09-109], [RQ-10-01]
(e2) Is a process established to validate the cyber security requirements of the item during development phase?	[RQ-11-01], [RQ-11-02]
(e3) Is a process established to validate the cyber security requirements of the item during production phase?	[RQ-12-01], [RQ-12-02]
7.2.2.2. (f) The processes used for ensuring that the risk assessment is kept current	
(f1) Is a process established to keep the cyber security risk assessment current?	[RQ-11-03], [RQ-06-098], [RQ-078-057], [RQ-07-06]
7.2.2.2. (g) The processes used to monitor for, detect and respond to cyber-attacks, cyber threats and vulnerabilities on vehicle types and the processes used to assess whether the cyber security measures implemented are still effective in the light of new cyber threats and vulnerabilities that have been identified	
(g1) Is a process established to monitor for cyber security information?	[RQ-078-01]
(g2) Is a process established to detect cyber security events?	[RQ-078-02], [RQ-08-03]
(g3) Is a process established to assess cyber security events and analyze cyber security vulnerabilities?	[RQ-078-034], [RQ-078-045], [RQ-08-06]
(g4) Is a process established to manage identified cyber security vulnerabilities?	[RQ-078-057], [RQ-1507-046], [RQ-15-05], [RC-1507-038]
(g5) Is a process established to respond on cyber security incidents?	[RQ-13-01], [RQ-13-02], [RQ-13-03]
(g6) Is a process established to validate effectiveness of the response?	[RQ11-03], [RQ-11-024]
(h) The processes used to provide relevant data to support analysis of attempted or successful cyber-attacks.	
Is a process given to provide relevant data to support analysis?	[RQ-078-034]

Commented [NJR20]: Requirement removed from IS

Commented [NJR21]: Requirement merged into RQ-011-01 in IS

Commented [NJR22]: Requirement split in IS

Commented [NJR23]: Removed from IS (already covered in cl. 8)

Commented [NJR24]: Requirements merged into RQ-08-07 in IS

Formatted: Indent: Before: 0 cm

Commented [NJR25]: Requirement split in IS

Formatted: Indent: Before: 0 cm

Commented [NJR26]: New in IS and relevant here

Commented [NJR27]: Removed from IS

Commented [NJR28]: RQ-13-02 in DIS removed from IS but new RQ-13-02 introduced in IS is relevant here

Commented [NJR29]: RQ-13-03 merged into RQ-13-01

Formatted: Indent: Before: 0 cm

Commented [NJR30]: Removed from IS

Formatted: Indent: Before: 0 cm

Formatted: Indent: Before: 0 cm

7.2.2.3. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that, based on categorization referred to in point 7.2.2.2. (c) and 7.2.2.2. (g), cyber threats and vulnerabilities which require a response from the vehicle manufacturer shall be mitigated within a reasonable timeframe.	
Mitigation within reasonable timeframe	No timeframe defined by ISO/SAE ~~DIS~~ 21434 (E)
7.2.2.4. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that the monitoring referred to in point 7.2.2.2. (g) shall be continual. This shall: (a) Include vehicles after first registration in the monitoring; (b) Include the capability to analyse and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs. This capability shall respect paragraph 1.3. and the privacy rights of car owners or drivers, particularly with respect to consent.	
Monitoring after first registration	Clause ~~7~~8.3 "Cybersecurity Monitoring"
Capability to analyse and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs	~~Not explicitly m~~Mentioned in ISO/SAE ~~DIS~~ 21434 (E)~~, but could be seen~~ as an example of an internal source for Cybersecurity Information ("information received from the field"), which can be used as further supporting information for performing Cybersecurity Monitoring.
Respecting privacy rights of car owners or drivers, particularly with respect to consent	Out of scope of ISO/SAE 21434, so not applicable
7.2.2.5. The vehicle manufacturer shall be required to demonstrate how their Cyber Security Management System will manage dependencies that may exist with contracted suppliers, service providers or manufacturer's sub-organizations in regards of the requirements of paragraph 7.2.2.2.	
Dependencies that may exist with contracted suppliers	[RQ-06-10~~9~~], [RQ-~~15~~07-03~~4~~], [RC-~~15~~07-02~~5~~]
Dependencies that may exist with contracted service providers	[RQ-06-10~~9~~], [RQ-~~15~~07-03~~4~~], [RC-~~15~~07-02~~5~~]
Dependencies that may exist with manufacturer's sub-organizations	[RQ-06-10~~9~~], [RQ-~~15~~07-03~~4~~], [RC-~~15~~07-02~~5~~]

Formatted: Indent: Before: 0 cm

Formatted: Indent: Before: 0 cm

Formatted: Indent: Before: 0 cm

Formatted: Indent: Before: 0 cm

Formatted: Indent: Before: 0 cm

Formatted: Indent: Before: 0 cm

Formatted: Indent: Before: 0 cm

B. Part B

Guidelines for the use of DETA with regard to the exchange of information on Cyber Security (as per UN Regulation No. [155])

I. Introduction

1. This guidance document is intended to provide guidance to the approval authorities of Contracting Parties to the 1958 Agreement on the use of DETA for the implementation of UN Regulation No. [155] on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system (documents ECE/TRANS/WP.29/2020/79 as amended by ECE/TRANS/WP.29/2020/94 and ECE/TRANS/WP.29/2020/97).

2. This guidance document does not alter the provisions of UN Regulation No. 155. If there is any inconsistency between these guidelines and the text of the UN Regulation, the latter shall prevail.

3. This guidance document is without prejudice to any guidance, rules and instructions from manuals, user information, instructions on client administration, guidelines or any other DETA documents.

4. For the purpose of these guidelines, "CS" refers to ‘cyber security’ and "DETA" to the ‘Database for the Exchange of Type Approval documentation established by the United Nations Economic Commission for Europe’.

II. Main principles of exchanging CS information by DETA

5. The paragraphs of UN Regulation No. 155 relevant for the use of DETA:

5.3.2. Each Contracting Party applying this Regulation shall notify and inform by its Approval Authority other Approval Authorities of the Contracting Parties applying this UN Regulation about the method and criteria taken as a basis by the notifying Authority to assess the appropriateness of the measures taken in accordance with this regulation and in particular with paragraphs 5.1., 7.2. and 7.3.

This information shall be shared (a) only before granting an approval according to this Regulation for the first time and (b) each time the method or criteria for assessment is updated.

This information is intended to be shared for the purposes of collection and analysis of the best practices and in view of ensuring the convergent application of this Regulation by all Approval Authorities applying this Regulation.

5.3.3. The information referred to in paragraph 5.3.2 shall be uploaded in English language to the secure internet database "DETA", established by the United Nations Economic Commission for Europe, in due time and no later than 14 days before an approval is granted for the first time under the methods and criteria of assessment concerned. The information shall be sufficient to understand what minimum performance levels the Approval Authority adopted for each specific requirement referred to in paragraph 5.3.2 as well as the processes and measures it applies to verify that these minimum performance levels are met.

5.3.4. Approval Authorities receiving the information referred to in paragraph 5.3.2 may submit comments to the notifying Approval Authority by uploading them to DETA within 14 days after the day of notification.

6. Section 5 above results in the general use case for DETA that the approval authority that is about to grant a type approval for UN Regulation No. 155 (hereafter called "notifying authority"):

(a) Uploads the required CS information to DETA, and

(b) Notifies this to the other authorities by adding a notification message onto DETA.

7. The CS information uploaded to DETA is only available to the Contracting Parties applying UN Regulation No. 155. The notification message will be available to all DETA users.

III. General guidelines on the use of DETA for exchanging CS information

8. The notifying authority shall proceed as follows:

(a) All required CS information referred to in UN Regulation No. 155, paragraph 5.3.2. shall be put together as one or more pdf files. These files shall be uploaded as document parts of the type "OTHER".

(b) A number of attributes need to be entered. As a minimum the mandatory fields need to be completed. This includes:

(i) the ‘approval number’ which need to be reserved by the approval authority,

(ii) the ‘approval date’ which is the intended date for granting the type approval. This date must be at least 14 days after the notification date to the other authorities,

(iii) the ‘approval state’ which need to be the value "in progress".

(c) The notifying authority then enters the actual notification in the tab "News". This notification includes as a minimum the standard text and approval number, to trace the related CS information in the DETA archive, as follows:

"*The Approval Authority of [country name] hereby notifies the other Approval Authorities of the Contracting Parties applying UN Regulation No. 155 about the method and criteria taken as a basis to assess the appropriateness of the measures taken in accordance with UN Regulation No. 155 and in particular with paragraphs 5.1., 7.2. and 7.3. thereof. Please refer to the type approval No. […] for the details.*".

Note: "News" is not a mailing-system. Other users only see the messages after logging into the system. Therefore these guidelines recommend the approval authorities to check the "News" section of DETA on a daily basis.

(d) When, after a minimum of 14 days after the notification message to the other authorities, the notifying authority decides to grant the approval, it shall as soon as possible:

(i) complete all the necessary attributes, including the final value at ‘approval data’, and

(ii) upload the documents parts of the types "CERT", "IF" and "TR".

9. The other approval authorities of the Contracting Parties applying UN Regulation No. 155 taking note of the notification message from the notifying authority may submit comments to the notifying authority within 14 days of the notification. In such a case they shall:

(a) send an e-mail to the notifying authority including all relevant information;

(b) add a message in the tab "News" to inform the other authorities that comments had been submitted to the notifying authority. This message includes as a minimum the standard text and approval number, as follows:

"*The Approval Authority of [country name] hereby informs the other Approval Authorities of the Contracting Parties applying UN Regulation No. 155 that comments had been submitted with regard to the notification issued by the Approval Authority of [country name]. Please refer to the type approval No. […] for the details.*".

The notifying authority will, without undue delay, add the received comments to the DETA archive by uploading the comments as a pdf file of the document type "OTHER" to the same section as of the original documents.

Note: this is to be followed in order to disclose proprietary information to only the approval authorities of the Contracting Parties applying UN Regulation No. 155.

10. Section 8 and 9 above apply before granting an approval according to Regulation No. 155 for the first time and each time the method or criteria for CS related assessment is updated.