TFCS- ahID-11

**Interpretation document/guidance for Regulation on Cyber Security**

|  |  |  |  |
| --- | --- | --- | --- |
|  | United Nations | ECE/TRANS/WP.29/201x/xx | |
| _unlogo | **Economic and Social Council** | | Distr.: General  DD MM YYYY  Original: English |

**Economic Commission for Europe**

Inland Transport Committee

**World Forum for Harmonization of Vehicle Regulations**

**xxx session**

Geneva, DD–DD MM YYYY

Item XXX of the provisional agenda

**Draft new Regulation on software updates**

**Interpretation document for Regulation on uniform provisions concerning the approval of cyber security**

**Submitted by the expert from xxx**

The text reproduced below was prepared by the experts from xxx

Contents

*Page*

6. Cyber Security Management System (CSMS) Certificate of compliance 4

7. Specifications 5

Annexes

1. Information document 8

**Introduction**

The purpose of this document is to help clarify the requirements of the Regulation on uniform provisions concerning the approval of software update processes and provide information on what may be used to evidence those requirements.

The target audience for this document are for vehicle manufacturers submitting systems for test and for the Technical Services/ Appropriate Authorities assessing those systems.

The outcome should be that this document is able to help harmonise the testing between different Technical Services/ Appropriate Authorities.

**Note regarding evidencing the requirements**  
This document is only guidance. It provides information on what information might/would be acceptable for the Technical Services/ Appropriate 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 Annex A) has shown that especially the ISO/SAE 21434 DIS can be very supportive in implementing the requirements on the CSMS to the organizations along the supply chain. Depending on the vehicle type defined by the vehicle manufacturer and the practices and procedures they use alterative and/or equivalent information may be supplied.

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/ Appropriate Authority prior to testing/audit. A demonstration may be provided through an overview + Diagrams + Experience. Argument that the requirements are met needs to be logical, understandable and convincing. Documents need not necessarily be large documents.

**~~Note for test phase~~**

~~For the test phase this document is intended to be a “living document”. It should aim to capture generic evidence/solutions/formats/standards that were provided by vehicle manufacturers as evidence against each requirement that was accepted by a Technical Service/ Appropriate Authority. Where the evidence supplied may be attributable to a given manufacturer it will not be recorded in this document.~~

~~At the end of the test phase the Task Force on Cyber Security and Over the Air Updates will validate this document and its contents.~~

**1. Scope**

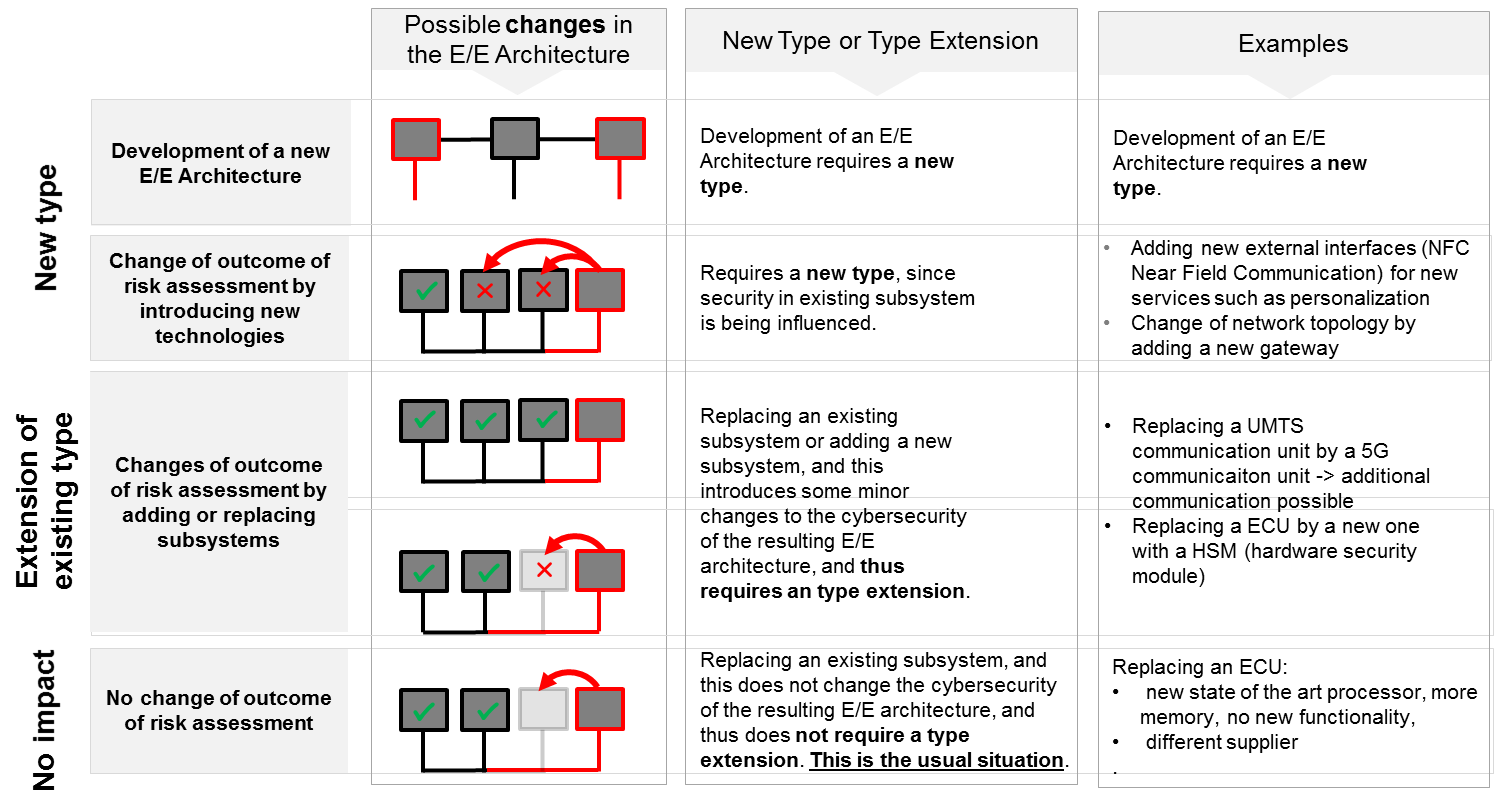
No guidance included in this document with regards this requirement

**2. Definitions**

~~2.1. c) Specifying the essential aspects – 1958 Agreement – safety, energy saving, anti-theft (vehicle UN R-116), environment protection.~~

New Type: Development of a new E/E architecture or fundamental change(s) that influences security in the existing E/E architecture.

Type Extension: Changes that can occur with the introduction of an additional subsystem or the replacement of an existing subsystem that have minor impact to the cybersecurity of the existing E/E architecture.



**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

**5. Approval**

No guidance included in this document with regards this requirement

**6. Cyber Security Management System (CSMS) Certificate of Compliance**

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. |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| - |

**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:  - The vehicle manufacturer has a CSMS  - 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:   * The CSMS may be a part of the organization’s Quality Management System or be independent of it * 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:   * ISO/SAE 21434 may be used as the basis for evidencing and evaluating the CSMS. Clauses 5. “Overall cybersecurity management”, 6. “Project dependent cybersecurity management”, and 7. “Continuous cybersecurity activities” could be used to evaluate the CSMS in general. * ISO 18045, ~~ISO 15048~~ ISO 15408, ISO 27000 series, ISO 31000 series may be applicable to relevant parts of the CSMS   The following examples may be used for evidencing that there is a CSMS and it complies:   * The manufacturer might have an organization specific handbook for the standard processes (or similar) that could cover part or all of the CSMS. |

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 follow clarifications should be noted:   * ‘Production phase’ refers to the duration of production of a particular vehicle type * ‘Post-production phase’ ~~refers to the time frame after the End of Production of the particular vehicle type~~ refers to the period in which a vehicle type is no longer produced until the end-of-life of all vehicles under the vehicle type.   The operational life (use phase) of an individual vehicle will commence during the production phase of the vehicle type. ~~It will end (at decommissioning) 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:   * ISO/SAE 21434 can be used as the basis for evidencing and evaluating the required phases of the CSMS. Clauses 9. “Concept Phase”, 10. “Product Development”, and 11. “Cybersecurity validation” could be used to evaluate the Development phase of the CSMS. Clause 12. “Production” could be used to evaluate the Production phase of the CSMS. Clauses 7. “Continuous cybersecurity activities”, 13. “Operations and maintenance”, and 14. “Decommissioning” could be used to evaluate the Post-production phase of the CSMS. * Other standards that may be applicable to 7.2.2 and its sub-requirements include: ISO 18045, , ~~ISO 15048~~ ISO 15408, ISO 27000 series, ISO 31000 series |

|  |
| --- |
| Remark for test phase |
| * ~~A definition of the three phases may be needed~~ * ~~Clarify if more details are needed for evidencing whether the requirements are met~~   ~~Issues noted for further consideration of how to evidence include:~~   * ~~Post-production is subject to other legal requirements/obligations. How/whether to consider these~~ * ~~There is an inherent difficulty to support indefinitely, in the test phase, participants will remain open to strategies proposed~~ |

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 and procedures 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:   * Organizational structure used to address Cybersecurity * Roles and Responsibilities regarding cybersecurity management incl. accountability |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| * 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-05-07], [RQ-05-08]. * BSI PAS 1885 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. |

|  |
| --- |
| The requirement may be considered not to be achieved if one of the following statements is true |
| 1. Your policies and processes are absent or incomplete. 2. Policies and processes are not applied universally or consistently. 3. People often or routinely circumvent policies and processes to achieve business objectives. 4. Your organisation’s security governance and risk management approach has no bearing on your policies and processes. 5. System security is totally reliant on users' careful and consistent application of manual security processes. 6. Policies and processes have not been reviewed in response to major changes (e.g. technology or regulatory framework), or within a suitable period. 7. Policies and processes are not readily available to staff, too detailed to remember, or too hard to understand. |

|  |
| --- |
| The requirement may be considered to be achieved if all of the following statements are true |
| 1. You fully document your overarching security governance and risk management approach, technical security practice and specific regulatory compliance. Cyber security is integrated and embedded throughout these policies and processes and key performance indicators are reported to your executive management. 2. Your organisation’s policies and processes are developed to be practical, usable and appropriate for your technologies. 3. Policies and processes that rely on user behaviour are practical, appropriate and achievable. 4. You review and update policies and 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 policies and processes. 6. Your systems are designed so that they remain secure even when user security policies and processes are not always followed. For such claim a justification should be provided. |

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 may include risks identified in Chapter 4 and Annex B of Cyber Security Recommendation e.g. risks arising from connected services or dependencies external to the vehicle.  Sources for risk identification may be stated. These may include:   * Vulnerability/ Threats sharing platforms * Lessons learned regarding risks and vulnerabilities |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| The following standards may be applicable:  ISO/SAE 21434, especially based on [RQ-08-01], [RQ-08-02], [RQ-08-08], [RQ-08-09].  The processes may consider:   * Identification the relevance of a system to cybersecurity * Description of the overall system with respect to   + - Definition of the system/function     - Boundaries and interactions with other systems     - Architecture     - Environment of operation of the system (context, constraints and assumptions) * Identification of assets * Identification of threats * Identification of vulnerabilities |

|  |
| --- |
| The requirement may be considered not to be achieved if one of the following statements is true |
| 1. Risk assessments are not based on a clearly defined set of threat assumptions. 2. 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. 3. Risk assessments for vehicle types are a "one-off" activity (or not done at all). 4. 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 to be achieved if the process covers all of the following statements |
| 1. Your organisational process ensures that security risks to vehicle types are identified, analysed, prioritised, and managed. 2. Your approach to risk is focused on the possibility of adverse impact to your 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 your networks and systems. 3. Your risk assessments are based on a clearly understood set of threat assumptions, informed by an up-to-date understanding of security threats to your vehicle types and your sector. 4. Your risk assessments are informed by an understanding of the vulnerabilities in your vehicle types. 5. You perform detailed threat analysis and understand how this applies to your organisation in the context of the threat to your sector. |

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:   * ISO/SAE 21434, especially based on [RQ-08-11], [RQ-08-04]. [RQ-08-06], [RQ-08-10], [RQ-08-12], [RQ-09-07], [RQ-05-06], [RQ-09-08].BSI PAS 11285 may be applicable for the consideration of safety and security.   The processes may consider:   * Assessing the associated impact related to the risks identified in requirement 7.2.2.2 b) * Identification of potential attack paths related to risks identified in requirement 7.2.2.2 b) * Determination of feasibility/likelihood of attack for every attack paths identified above * Calculation and categorization of risks * Treatment options of those identified and categorized risks |

|  |
| --- |
| The requirement may be considered not to be achieved if one of the following statements is true |
| 1. Security requirements and mitigation's are arbitrary or are applied from a control catalogue without consideration of how they contribute to the security of vehicle types. 2. 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). 3. Inventories of assets relevant to vehicle types are incomplete, non-existent, or inadequately detailed. 4. Asset inventories are neglected and out of date. 5. Systems 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 to be achieved if all of the following statements are true |
| 1. The output from your risk management process is a clear set of security requirements that will address the risks in line with your organisational approach to security. 2. All assets relevant to the secure operation of your 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. You have prioritised assets according to their importance to the operation of your vehicle types. |

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).  Controls identified in Chapter 5 and Annex C of Cyber Security Recommendation may be included in the processes. |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| The following standards may be applicable:   * ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-09-09].ISO 31000 may be applicable if adapted for product related risks   The processes may consider:   * Appropriate and proportional risk treatment methodologies * 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 * Ensuring the residual risk remains within acceptable limits for components or the overall vehicle type * Detailing any cases where the organization would accept justification for non-adherence to their stated risk tolerance |

|  |
| --- |
| The requirement may be considered not to be achieved 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 systematic 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 to be achieved if all of the following statements are true |
| 1. Significant conclusions reached in the course of your risk management process are communicated to key security decision-makers and accountable individuals. 2. The effectiveness of your risk management process is reviewed periodically, and improvements made as required. |

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 activities in the production phase may be different to the ones during the development phase. |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| The following standards may be applicable:   * ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-09-10], [RQ-10-01]. [RQ-11-01], [RQ-11-02], [RQ-12-01].BSI PAS 11825 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:   * Organization specific rules for testing during development * Processes for creation and execution of test strategies * Processes for cybersecurity testing planning * Processes for cybersecurity system design testing * Processes for cybersecurity software unit testing * Processes for cybersecurity hardware testing * Processes for cybersecurity integration testing * Processes for documentation of the results of testing * Processes for handling vulnerabilities identified during testing * 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:   * Processes for testing to ensure the produced system has the cybersecurity requirements, controls and capabilities outlined in the cybersecurity production plan * Processes for testing to ensure the produced item meets the cybersecurity specifications which are in accordance with the system in the development phase * Processes for testing to assure that cybersecurity controls and configuration as cybersecurity specifications are enabled in the produced item * Processes for documenting the test results and findings handling |

|  |
| --- |
| ~~Remark for test phase~~ |
| * ~~The term ‘processes may consider’ may need refinement~~ * ~~The list of processes may be reviewed further~~ |

|  |
| --- |
| The requirement may be considered not to be achieved 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, 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 to be achieved if all of the following statements are true |
| 1. You validate that the security measures in place to protect systems are effective and remain effective ~~for the lifetime~~ over the end-of-life of the vehicle which they are needed. 2. You understand the assurance methods available to you and choose appropriate methods to gain confidence in the security of vehicle types. 3. Your confidence in the security as it relates to your 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. |

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:   * Vulnerability/ Threats sharing platforms * Lessons learned regarding risks and vulnerabilities * 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 |
| ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-11-03], [RQ-06-08]. [RQ-07-05], [RQ-07-06]. |

|  |
| --- |
| The requirement may be considered not to be achieved if one of the following statements is true |
| 1. No entries. |

|  |
| --- |
| The requirement may be considered to be achieved if all of the following statements are true |
| 1. You conduct risk assessments when significant events potentially affect vehicle types, such as replacing a system or a change in the cyber security threat. 2. Your 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. |

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 to vehicles that they have had type approved, i.e. are in the post-production or production phase, and that they have established processes that would permit them, when an event is detected, to respond in an appropriate and timely manner.  The following clarification should be noted:   * "cyber-attack" means a manifest attack at the software and hardware level   It is noted that requirements 7.2.2.2 parts f) to i) 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:  ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-07-01], [RQ-07-02]. [RQ-07-03], [RQ-07-04], [RQ-07-05], [RQ-15-04], [RQ-15-05], [RC-15-03], [RQ-13-01], [RQ-13-02], [RQ-13-03].  The following could be used to evidence the processes used:   * Cybersecurity 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 * Cybersecurity 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 * Processes for risk determination/assessment for the relevant information * Incident response procedures, which may include evidence of procedures for::   + Interaction with authorities   + Identified or stated triggers that would lead to an escalation or action   + Determining what response options might be implemented for which condition   + Handling any dependencies and interactions with suppliers   + Already registered vehicles of the concerned vehicle type   + Vehicles of the concerned vehicle type that are not yet registered * Evidence that the response procedures would work, for example through exercising and verification that planning assumptions remain valid under test. |

|  |
| --- |
| The requirement may be considered not to be achieved if one of the following statements is true |
| 1. Your organisation has no sources of threat intelligence. 2. You do not apply updates in a timely way, after receiving them. 3. You do not evaluate the usefulness of your threat intelligence or share feedback with providers, authorised aftermarket service providers or other users 4. There are no staff who perform a monitoring function. 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 to be achieved if all of 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. Your organisation uses threat intelligence services which are relevant to your business needs, or specific threats in your sector 7. You apply updates in a timely way. 8. You know how effective your threat intelligence is (e.g. by tracking how threat intelligence helps you identify security problems). 9. Monitoring staff have some 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) |

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 the process has been established to provide the data required for analysis to the department in charge of analysis (or the person who performs the analysis if the analysis is outsourced)  ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-07-03].. |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| The following could be used to evidence the processes used:  Procedure for implementing SIRT activities (incidents)  -Field monitoring (obtaining information on incidents and vulnerabilities)  -Procedure when an incident occurs (Including an overview of what information is passed to the analyst in what steps)  -Procedure when vulnerability is discovered (Including an overview of what information is passed to the analyst in what steps) |

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.  Also, be able to explain the process by which OEMs take countermeasures when new threats or vulnerabilities are detected even after the development and production contract with the supplier has expired.  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. |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| The following could be used to evidence the processes used:  Procedure for implementing SIRT activities (incidents)  -Field monitoring (obtaining information on incidents and vulnerabilities)  -Procedure when an incident occurs  -Procedures for discovering vulnerabilities |

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 utilizing the information on monitoring acquired in accordance with 7.3.7 and other manufacturer's storage, a process for utilizing the relevant data etc. for analysis shall be established.  ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on 7.3 “Cybersecurity Monitoring”, 7.4 “Cybersecurity event assessment”, 7.5 “Vulnerability analysis. |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| The following could be used to evidence the processes used:  Procedure for implementing SIRT activities (incidents)  -Field monitoring (obtaining information on incidents and vulnerabilities)  -Procedure when an incident occurs  -Procedures for discovering vulnerabilities |

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.  Within the CSMS there may be processes to (the final processes are subject to bilateral agreement between vehicle manufacturer and supplier)   * identify risks associated with parts, components, systems or services provided by suppliers * 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 and internet providers and authorised aftermarket service providers. * ensure contracted suppliers 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. * Ensure that authorised aftermarket service providers are able to evidence how they can manage cybersecurity for development and installation/system integration of replacement of parts and components. This process requires information to be shared from vehicle manufacturers to authorised aftermarket service providers:   + For development, this may include relevant cybersecurity goals, specifications and requirements including validation and authentication procedures.   + For system integration, this may include the relevant cybersecurity specifications, requirements and necessary means for installation and activation of authenticated replacement parts. * delegate availability and stability requirements to functional safety departments of the manufacturer, in order to care for robustness of vehicle systems against Denial-of-Service of backend-provided services   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:   * ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-06-09], [RQ-15-03], [RC-15-02].)   The following could be used to evidence the processes used:   * Contractual agreements in place or evidence of such agreements * Evidenced arguments for how their processes will ensure suppliers / service providers will be considered in the risk assessment process * Procedures/Methods of sharing information on risk between suppliers and manufacturers * Existing solutions / contracts like ISMS (Information Security Management System) regulation can be used for evidence * ~~Other means such as requirements for certification of suppliers may be appropriate (for example requiring suppliers are accredited to schemes like Cyber Essentials Plus in the UK)~~ |

|  |
| --- |
| ~~Remark for test phase~~ |
| ~~ACTION ITEM: Check during the test phase how practical it is to assess the evidence from all involved suppliers.~~ |

|  |
| --- |
| The requirement may be considered not to be achieved 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 to be achieved if all of the following statements are true |
| 1. You have a deep understanding of your supply chain, including sub-contractors and the wider risks it faces. You consider factors such as supplier’s partnerships, competitors, nationality and other organisations with which they sub-contract. This informs your risk assessment and procurement processes. 2. Your approach to supply chain risk management considers the risks to your vehicle types arising from supply chain subversion by capable and well-resourced attackers. 3. You have confidence that information shared with suppliers that is essential to the operation of your vehicle types is appropriately protected from sophisticated attacks. 4. You can clearly express the security needs you place 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, your incident management process and that of your suppliers provide mutual support in the resolution of incidents. |

**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.

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:   * "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:   * The Certificate of Compliance for CSMS to demonstrate it is still valid * Confirmation that the CSMS is appropriately applied to the vehicle type and any information required to provide assurance. |

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

1. **~~Collect and verify~~****~~information~~****~~required~~** ~~under this Regulation through the~~ **~~supply chain~~**~~;~~

|  |
| --- |
| 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:   * "supply chain" - 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:   * ISO/SAE 21434   The following could be used to evidence the processes used:   * Evidence in the form of contract sections with suppliers that deal with the requirements of this regulation |

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 to ensure that risks shall be appropriately processed / managed by considering all threats including Annex5\_PartA and judging the necessity of countermeasures based on the results of risk analysis and risk evaluation.  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.   * The approval authority or technical service may refer to *Chapter 4 and annex B* of the cyber security Resolution to aid their assessment of the manufacturer’s risk assessment.   Note: This capability shall respect paragraph 1.3. |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| The following standards may be applicable:   * ISO/SAE 21434 describes exhaustive risk assessment in clause 8 “Risk assessment methods”. This is documented in [WP-09-02] Threat analysis and risk assessment. |

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.

1. **~~Implement appropriate cyber security measures~~** ~~in the design of the vehicle and its systems;~~

|  |
| --- |
| Explanation of the requirement |
| The intention of this requirement is to ensure that vehicle manufacturers implement appropriate mitigation measures in accordance with the need for measures based on the results of risk analysis and risk assessment.  The intent of this requirement is for the manufacturer to provide a reasoned argument that the security measures they have implemented in the design of the vehicle type are sufficient, as provided by their responses to requirements 7.3.3 to 7.3.6.  The following clarifications should be noted:   * 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 * The appropriateness of the controls implemented may be justified by reasoned arguments.   This may include any assumptions made, for example about external systems that interact with the vehicle, however this capability shall respect provisions under paragraph 1.3. |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| The following could be used to evidence the processes used:  Evidence that mitigation measures were introduced according to the necessity of measures (this includes:  ・the reason ,If mitigation measures other than Annex5 Part B and C are applied  ・the reason, If mitigation measures are determined to be unnecessary  The following standards may be applicable:   * ISO/SAE 21434 describes the identification of risk and the deduced Cybersecurity goals and concept based on the identified risks. The results are documented in [WP-09-04] Cybersecurity goals and [WP-09-07] Cybersecurity concept. * PAS 11825 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 processes used:   * Manufacturer should demonstrate the implementation of mitigation measures to the vehicle type and its design. Annex C may be considered as a reference. It is noted that it is not exhaustive and other measures may be more applicable. It should further be considered with respect to the vehicle type |

|  |
| --- |
| ~~Remark for test phase~~ |
| ~~Note: during the test phase it should be clarified for the Technical Service:~~   * ~~The extent to which "appropriate security measures" can be assessed for a vehicle type and how~~ |

7.3.4. The vehicle manufacturer shall **demonstrate** to the satisfaction of the Approval Authority or its Technical Service **that critical elements** of the vehicle type **are protected** against risks identified in the vehicle manufacturer’s risk assessment. Proportionate mitigations shall be implemented to protect such elements.



|  |
| --- |
| 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. Justification can include residual risks and risk acceptance criteria.  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   * 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. gateway could be also considered critical) |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| The following standards may be applicable:   * 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 [WP-09-04] Cybersecurity goals and [WP-09-07] Cybersecurity concept. * ETSI TS 103 645 may be used for demonstrating the security of Internet of Things elements of a vehicle. * BSI PAS 1885 may be used   The following could be used to evidence this requirement:   * The vehicle type claimed * An explanation of why elements within the vehicle type are critical * What security measures are implemented, including information on how they work * Information on any security measures should permit the TS/AA 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 TS/AA for the vehicle type. Confidentiality of specifics and how these are handled should be agreed and recorded. * *Annexes A and B of the cyber security Resolution* may be referred to. |

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.

|  |
| --- |
| Explanation of the requirement |
| The following clarifications should be noted:   * "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 * 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:   * ISO/SAE 21434 describes on a process base steps to make conclusion for the architecture. This aspect is to be considered in [WP-08-03] Threat scenarios.   The following could be used to evidence this requirement:   * A description of the dedicated environment * What security measures are implemented, including information on how they work * Information on any security measures should permit the TS/AA 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 TS/AA for the vehicle type. Confidentiality of specifics and how these are handled should be agreed and recorded. * *Annexes A and B of the cyber security Resolution* may be referred to. |

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:   * 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:   * Manufacturers may describe the verification and validation measure implemented in accordance with ISO/SAE 21434 in form of [WP-09-08] Verification report of cybersecurity concept, [WP-10-03] Verification report for the refoined cybersecurity specification, [WP-11-02] Validation report.   The following could be used to evidence this requirement:   * What is tested and why (e.g. what measures of success for the test look like) * Methodology used and why (e.g. this may include notes on the extent and effort contained within the testing) * 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) * Confirmation of its successful outcome (pass/fail criteria of the test) |

|  |
| --- |
| ~~Remark for test phase~~ |
| ~~Note: during the test phase it should be clarified for the Technical Service:~~   * ~~what is expected in terms of proving the efficiency/effectiveness of the security measures implemented. (e.g. Time bound testing penetration, fuzz,..).~~ |

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 the outline of the technology mounted on a vehicle in response to a cyber attack on the vehicle will be described.  (a): Attack prevention measures for vehicles are applied.  (b): The results of defense by vehicle manufacturer's preventive measures and monitoring results are recorded.  (c): The vehicle manufacturer should be able to read the recorded results and use them for analysis.  In any case, the outline of the technology shall be explained.   * ISO/SAE 21434 is considering the monitoring in [WP-07-01] List of sources for cybersecurity monitoring], the analysis is documented in 8WP-07-04] Vulnerability analysis. * Any measure with regard to this clause may be implemented on the vehicle type or in its environment, e.g. the backend, the mobile network: “for the vehicle type”. * Measures to prevent cyber-attacks may be delivered asynchronously, i.e. after the actual event of the cyber-attack and its analysis and in form of a (delayed) response. This clause requires measures neither to analyse nor respond “in real-time” nor “in wire-speed” nor “automated”. * The “data forensic capability” may deliver data from a restricted time frame of observation. * The clause establishes a legal basis to extract related data from customers’ vehicles with regards to data privacy law. Types and amount of data shall nevertheless not be too extensive and should be pseudonomized; or anonymized if the customer decides so. |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| * Data forensic capability may deliver log data, diagnostic error codes. * Data forensic capability may be a circular buffer of persisting log data. |

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.

|  |
| --- |
| Explanation of the requirement |
| The intent of this requirement is to ensure:  Regarding the points where encryption measures are taken based on the results of risk analysis and risk assessment,  (1) explain whether it complies with the consensus standard, and  (2) if it does not, explain the rational reason.  Making a choice of cryptographic mechanisms may be delicate, accordingly it should be made with caution. The requirement of 7.3.8 makes clear that the manufacturer shall adhere to common sense/best practices/standards. Such are documented in recommendation documents of numerous cybersecurity bodies world wide. Keeping in mind, that such documents often may not look as far into the future as the lifetime of a vehicle time may be, the manufacturer should conduct and document its rationale behind the cryptographic choices. |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| As documents/evidences, there may be manufacturer specific guideline for allowed and recommended cryptographic mechanisms. This document then should reference approopriate consensus standards, additional assumptions made for the future as well as intentful deviations.  Then, for each vehicle type, there may only be additional documentation, if there is a specific deviation of the internal recommendation. This deviation should be substantiated by a detailed risk assessment, rating and treatment decision. |

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 vehicle manufacturer runs CSMS related to the monitoring activities, as defined in paragraph 7.2.2.2.(g) properly after Development Phase. 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.   * ISO/SAE 21434 defines [WP-07-02] Results from the triage of cybersecurity information and [WP-07-04] Vulnerability Analysis. Both can be used as the baseline for the required reporting. |

|  |
| --- |
| Examples of documents/evidence that could be provided |
|  |

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.

|  |
| --- |
| Explanation of the requirement |
|  |

|  |
| --- |
| Examples of documents/evidence that could be provided |
|  |

**8. Modification and extension of the vehicle type**

No guidance included in this document with regards this requirement

**9. Conformity of production**

No guidance included in this document with regards this requirement

**10. Penalties for non-conformity of production**

No guidance included in this document with regards this requirement

**11. 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

**Annex 1**

**Information document**

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

1. Make (trade name of manufacturer):

2. Type and general commercial description(s):

3. Means of identification of type, if marked on the vehicle:

4. Location of that marking:

5. Category(ies) of vehicle:

6. Name and address of manufacturer/ manufacturer's representative:

7. Name(s) and Address(es) of assembly plant(s):

8. Photograph(s) and/or drawing(s) of a representative vehicle:

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.

|  |
| --- |
| Explanation of the requirement |
|  |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| Shall be a written description of the E/E architecture |

9.2. Schematic representation of the vehicle type

|  |
| --- |
| Explanation of the requirement |
|  |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| Note: Shall be a schematic of the E/E architecture – e.g. circuit diagram |

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:

Annex 2

Communication form

No guidance included in this document with regards this annex

Annex 3

Arrangement of approval mark

No guidance included in this document with regards this annex

Annex 4

Model of Certificate of Compliance for CSMS

No guidance included in this document with regards this annex

Annex A

Link with ISO/SAE 21434 DIS (E)

|  |  |
| --- | --- |
| **Sub-Category** | **Clauses from ISO/SAE 21434 DIS** |
| 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 Cybersecurity 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 9, 10,11 |
| Production phase | Clause 12 |
| Post-production phase | Clauses 7, 13, 14 |
| 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-05-09] |
| (a3) Establishment and Maintenance of cyber security culture and awareness | [RQ-05-07]. [RQ-05-08] |
| 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-08-01]. [RQ-08-02], [RQ-08-03], [RQ-08-08], [RQ-08-09], The threats in *Annex 5 of the UNECE document, part 5* are out of scope of ISO/SAE 21434 |
| 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-08-11], [RQ-08-04], [RQ-08-06], [RQ-08-10] |
| (c2) Is a process established to treat cyber security risks for vehicle types across development, production and post-production? | [RQ-08-12], [RQ-09-07], [RQ-05-06], [RQ-09-08] |
| 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-09-09] |
| (e) The processes used for testing the cyber security of a vehicle type | |
| (e1) Is a process established to specify cyber security requirements? | [RQ-09-10], [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] |
| 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-06-08], [RQ-07-05], [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-07-01] |
| (g2) Is a process established to detect cyber security events? | [RQ-07-02] |
| (g3) Is a process established to assess cyber security events and analyze cyber security vulnerabilities? | [RQ-07-03], [RQ-07-04] |
| (g4) Is a process established to manage identified cyber security vulnerabilities? | [RQ-07-05], [RQ-15-04], [RQ-15-05], [RC-15-03] |
| (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? | [RQ-11-01], [RQ11-03], [RQ-11-04] |
| (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-07-03] |
| 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 21434 DIS (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:   * 1. Include vehicles after first registration in the monitoring;   2. 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 7.3 “Cybersecurity Monitoring” |
| Capability to analyse and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs | Not explicitly mentioned in ISO/SAE 21434 DIS (E), but could be seen as Cybersecurity Information. |
| 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-06-09], [RQ-15-03], [RC-15-02] |
| Dependencies that may exist with contracted service providers | [RQ-06-09], [RQ-15-03], [RC-15-02] |
| Dependencies that may exist with manufacturer’s sub-organizations | [RQ-06-09], [RQ-15-03], [RC-15-02] |