Approval of vehicles with regards to Cyber Security and Cyber Security management system

Interpretation Manual May 2024 Version

INTRODUCTION

The purpose of this document is to help clarify the requirements of clause 5, 7 and 8 and Annex A of this standard, on uniform provisions concerning the approval of vehicles with regard to Cyber Security and Cyber Security Management Systems 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 Test agencies assessing those systems. The outcome should be that this document is able to help harmonize evaluations between different test agencies.

This document is only guidance. It provides information on what information might / would be acceptable for the Test agencies and what level of information might be supplied. It is not intended to be exhaustive. The standards referred are intended as examples, not mandatory, Nevertheless, a coherence-check (refer clause 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 24134 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.

For all the requirements in the standard, 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 test agency 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.

The Standard cannot include all the security and threats, since the list is quite exhaustive, actual conditions and threats in the real world should not result in failure of the system and encourage the driver to opt out from such technology.

While preparation of this manual considerable assistance is derived from WP.29-182-05 and equivalent Japanese Type approval manual and Certification manuals for Cyber Security, January 2021 versions. The clauses for which interpretation is available are retained with explanation, rest are deleted for the sake of better readability.

	Interpretation Manual for Cyber Security and Management System (CSMS)
1.0	**SCOPE**
	No guidance included in this document with regards this requirement
2.0	**DEFINITIONS**
	No guidance included in this document with regards this requirement
3.0	**APPLICATION FOR APPROVAL**
	No guidance included in this document with regards this requirement
4.0	**RESERVED**
5.0	**APPROVAL**
5.3	Test Agency 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 Standard.
	Explanation of the requirement
	In addition to the conditions referred to in paragraph 5.1, the Test Agency will verify if all the requirements quoted in section 7 of this standard have been effectively fulfilled. This includes the cyber security management system referred to in paragraph 7.2 and 7.3.1
5.3.1	The Test Agency shall ensure, that they have:
	(a) Competent personnel with appropriate cyber security skills and specific automotive risk assessments knowledge[1]
	1. E.g. ISO 26262-2018, ISO/PAS 21448-2019, ISO/SAE 21434-2021
	Explanation of the requirement
	The requirement would imply that the Test agency have at their disposal, in a sufficient number, the following categories of personal
	(a) Personal competent and experienced in application of the Cyber Security standards and procedures necessary for its implementation and application. Applicable standards may include ISO 21434 and ISO 27001 for the content aspects of ISO 19011 and ISO PAS 5112 for the audit processes.
	(b) Personal 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 standard does not impose any specific contractual relation between the Test Agency and the personal concerned, these might be employment (labor) contracts, services contracts etc.
	The number of personal concerned must be proportionate to the actual workload
	The internal procedures of the organization should ensure that the tasks under the Standard are performed or effectively controlled by the personal having

	relevant skills.
	(b) Implemented procedures for the uniform evaluation according to this Standard.
	Explanation of the requirement
	The organization 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 organization.
	The organization should have processes installed for secure storage and transmission of confidential information.
	The Test Agency should have processes to assure that the integrity of the personnel involved in assessments is appropriate to the risks involved.
	The requirement of the Standard 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 and best practice guidelines of the Test Agencies
6.0	**CERTIFICATE OF COMPLIANCE FOR CYBER SECURITY MANAGEMENT SYSTEM**
	No guidance included in this document with regards this requirement
7.0	**SPECIFICATIONS**
7.2.1	For the assessment the test agency shall verify that the vehicle manufacturer has a Cyber Security Management System in place and shall verify its compliance with this Standard.
	Explanation of the requirement
	The intention of this requirement is that the Test Agency shall verify:
	(a) The vehicle manufacturer has a CSMS
	(b) The presented CSMS complies to the requirements listed below in this standard
	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 requirement of the CSMS.
	The following clarifications should be noted:
	(a) The CSMS may be a part of the organization's Quality Management System or be independent of it.
	(b) 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
	(a) ISO/ SAE 21434 may be used as the basis for evidencing and evaluating the CSMS. herein;
	- Clause 5 "Overall cybersecurity management";

	- Clause 6 "Project dependent cybersecurity management", and
	- Clause 7 "Continuous cybersecurity activities";
	could be used to evaluate the CSMS in general.
	(b) Other standards like ISO 18045, ISO 15408, ISO 27000 series, ISO 31000 series may be applicable to relevant parts of the CSMS.
7.2.2.1	The vehicle manufacturer shall demonstrate to an test agency that their Cyber Security Management System applies to the following phases:
	(a) Development phase;
	(b) Production phase;
	(c) Post-production phase.
	Explanation of the requirement
	The intention of this requirement is that the cyber security 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.
	Clause 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 phase also applies 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 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 be used as the basis for evidencing and evaluating the required phase of the CSMS:
	- clause 9 "Concept Phase", clause 10 "Product Development"; and clause 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", Clause 13 "Operations and maintenance" and Clause 14 "Decommissioning" could be used to evaluate the post-production 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.

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 D. This shall include:
	(a) The processes used within the manufacturer's organization to manage cyber security;
	Explanation of the requirement
	The "process to manage cybersecurity" refers to the process for managing "vehicles and functions protected from threats" as an organization. In other words, as an organization, it is required to explain how its approach to security is processual (that is, it has its own rules and regulations in place).
	The following could be used to show the range of activities performed by the manufacturer to manage the cybersecurity 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 including accountability.
	Following standards may be referred:
	- ISO / SAE 21434 can be used as the basis for evidencing and evaluating as required especially based on [RQ-05-02]. [RQ-05-08];
	- BSI PAS 1885 could be used to help evidence this requirement National certificate schemes, link the UK Cyber Essentials, could be used to evidence a manufacturer's organizational processes.
	Examples of documents/evidence that could be provided:
	- Materials explaining the internal management system (organization chart) and the overall structure of internal rules need to be submitted.
	- Key aspects to be covered in Internal management system:
	- Security management must be deployed from the top of the organization to the field. Feedback from the field must be reflected in the system.
	- Internal management systems and processes defined, and there must be a section or department responsible for driving improvements to those processes and checking compliance with rules.
	- The organization chart should address following aspects in the organization:
	(i) provide overview of cyber security promotion system from top to department level. The management path from the top management to each department level and the general role of each department and the responsible persons may be specified.
	(ii) The organization structure must be clear from the department heads to each group/ section, and reflect how the policies determined at the top management are developed into specific operations within each department and section or groups. It shall be able to be confirmed how related departments or sections are cooperating with the goals of each department determined by top management.
	- The internal rules and regulations shall cover following aspects:

	(i) There shall be Basic Policy that covers internal development of actions to be taken by the organization.
	(ii) There should be internal standards aligned to the Basic policy and describe "what must be done".
	(iii) Implementation procedures that specifically describe the work procedures and manual for the person in charge.
	- Test agency need to check whether the regulations are in place and the processes for management (including updating) are in place. Some of the key checkpoints for test agencies are as follows:
	1.The areas related to the product life cycle (development, production, and post-production) shall be covered.
	2. The process is commonly applied to the organizations involved and there are no discrepancies in interpretation among the applicable departments.
	3. A variety of factors, such as cost and vehicle development timelines, shall not cause legitimate security processes to be skipped.
	4. Security governance and risk management activities shall be process-based.
	5. Security related development activities shall not rely on individual judgment or personal skill to carry out the process. Clear criteria shall be included in the process.
	6. The process shall be revised in line with changes in the status of new product technologies and legislations. In addition, a system shall be available for periodic review.
	7. The existence of the process shall be known within the company and shall be viewed/utilized by employees. The content should not be too detailed to remember, or too hard to understand. Organization should also put efforts to promote understanding (education, etc.) on the processes.
	8. Processes are systematically developed and documented. In addition, the results of compliance with the process are reported to executives as KPIs.
	9. The processes are appropriate and practical for the business system.
	10. The process is based on the behavior of the user (the person using the security process), resulting in a detailed level of procedure that can be implemented.
	11. There shall be a mechanism to review the process on a regular basis and in the event of a serious incident.
	12. There shall be a process for checking the system from a third party's point of view when there are omissions in the system that the designer is not aware of or when there are intentional irregularities or attacks.
	(b) The processes used for the identification of risks to vehicle types. Within these processes, the threats in Annex D, 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 D of the Cyber Security standard, 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 platform:
	(b) Lessons learned regarding risks and vulnerabilities.
	The following standard may be referred:
	- 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;
	(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);
	- Identification of assets;
	- Identification of threats;
	- Identification of vulnerabilities.
	Examples of documentation / evidences that could be provided :
	Documents describing specific operating procedures for the process (item definition, asset analysis, threat analysis, etc.) used to identify risks to vehicles. e.g.
	- Departments involved in the operations and workflow.
	- Specific practical process i.e. Documents at a description level that can specify the work policy of the actual PIC by referring to them. They should include the input information and output results of each process, and the specific tasks involved in obtaining the results. Includes consideration of the threats listed in Annex D.
	- Sample of risk identification results （The format in which the evaluation results are to be entered may be used as the submission document, and the format in which the evaluation results are finally completed may be presented to Test Agency at the time of the face-to-face discussion or audit, in consideration of addressing confidentiality aspect.
	Note : The above shall not be a document specially prepared for certification but a document used in regular practice. An excerpt of only the necessary parts shall be acceptable for evidence submission.
	With regard to the threats specified in Annex D, a threat that clearly cannot occur in a vehicle may be excluded from consideration by the process after clarifying the reason. Documentation of the reasons shall be kept within the OEM as well as the risk identification results.
	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 organizational process ensures that security risks to vehicle types are identified, analyzed, prioritized, 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 organization in the context of the threat to its vehicle models.
	(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.
	- Risk Assessment: A series of processes for risk identification, risk analysis, and risk assessment
	- Categorization: risk holding (tolerance), risk transfer (transfer), risk reduction, and risk avoidance
	- Treatment: Security goals, security request creation (except for risk holding)
	The following standards may be referred:
	(a) 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].
	(b) BSI PAS 11281:2018 may be applicable for the consideration of safety and security.
	Documents to be submitted:
	Documents describing specific operating procedures for the key processes comprising the risk assessment:
	- Risk assessment process
	- Risk categorization process

	- Risk treatment decision process
	Specifically, documents stating the followings:
	- Departments involved in the operations and workflow.
	- Specific practical process i.e. Documents at a description level that can specify the work policy of the actual PIC by referring to them. They should include the input information and output results of each process, and the specific tasks involved in obtaining the results.
	- A Sample of risk assessment, categorization result and treatment which include a sequence of steps from the start of consideration to the end result can be submitted to test agency for evidence for certification.
	Note: It shall not be a document specially prepared for certification but a document used in practice. An excerpt of only the necessary parts shall be acceptable for evidence submission.
	These requirements should be considered unfulfilled if one of the following statements is true:
	1. The results of the judgment of acceptability of each risk value based on the risk standard are complicated with a huge amount of information. In addition, because risks are not prioritized, internal communication is difficult and cannot be used for decision-making.
	2. Security requirements and mitigation measures have not been evaluated based on cybersecurity goals.
	3. The content and asset list pertaining to asset identification at the time of risk identification are managed only in specific areas.
	4. The asset list is in an inappropriate state, such as being managed only in a specific area, lacking content, being too granular, or not being updated.
	5. Inappropriate condition such as asset list not being updated.
	6. When the system to be evaluated works with multiple systems, the interaction among the systems not be taken into account, and there is a possibility of misunderstanding or oversight.
	7. The results of the risk assessment do not reflect product functions or assumptions.
	8. Risk identification has not been reviewed (re-evaluated) according to the change point.
	The requirements 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 organizational approach to security.
	2. All sets 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 recognized and recorded.
	5. The vehicle manufacturer has prioritized 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.
	8. The manufacturer can demonstrate the effectiveness and repeatability of their processes for their categorization and treatment of risk.
	(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 result 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 D of cyber security regulations shall be considered in the processes.
	The following standards may be referred:
	(a) ISO / SAE 21434 can be used as the basis for evidencing and evaluating as required. especially based on [RQ-09-09];
	(b) 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.
	Documents to be submitted:
	Documents describing specific operating procedures for the internal review process (e.g. internal reviews, quality gates etc.) to ensure that countermeasures are applied to risks (e.g., implementation procedures).
	Specifically, documents stating the followings:
	- Departments involved in the operations and workflow.
	- Specific practical process i.e. Documents at a description level that can specify the work policy of the actual PIC by referring to them. They should include the input information and output results of each process, and the

	specific tasks involved in obtaining the results.
	- A description of the process by which mitigation measures in Annex D are taken into account to address identified risks.
	Note : It shall not be a document specially prepared for certification but a document used in practice. An excerpt of only the necessary parts shall be acceptable for evidence submission.
	The requirement should be considered unfulfilled if one of the following statements is true.
	1. The security elements of projects or programs 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 allocations to resolve.
	The requirements 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.
	(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.
	The following standards may be referred:
	(a) 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].
	(b) BSI PAS 11281:2018 may be utilized 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 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.
	Documents to be submitted:
	- Documents that describe specific implementation procedures for the process of confirming that the results of the measures determined in 7.2.2.2. (C)(Risk Treatment) have been reliably implemented (e.g., implementation procedures)
	- Each company has a different evaluation process, so it is difficult to write in a uniform way, but the following documents can be provided:
	- Security testing process of the vehicle, include security test procedures (containing roles, workflows, and work contents).
	- Include responses (upstream F/B method) in case of a problem with the confirmation result.
	- The process of ensuring that the envisaged measures for the production vehicles are in place.
	- Provide an explanation that the identical vehicles will be produced as at the time of the certification test.
	- Sample Test Results (The result description may be blank or reference content.)
	The requirement should be considered unfulfilled if one of the following statements is true:
	1. It is a process in which mitigation can be implemented without actual testing the vendor's security products and services, believing the vendor's claims.
	2. When actual vehicle tests such as penetration tests and bench tests are used, the advantages and disadvantages are not understood and applied as a security assurance method.
	3. Guaranteed on the basis that there has never been a problem.
	The requirement may be considered fulfilled if all the following statements are

	true:
	1. The security measures are verified to function as designed and to reduce the risk of attacks, and to ensure that the security measures are effective throughout the life of the vehicle.
	2. There is a process to consider the test methodology and test specifications in view of the purpose of the test.
	3. The vehicle manufacturer demonstrates and verifies to third parties outside the design department their confidence in the security associated with their technology, personnel and processes.
	4. Security deficiencies uncovered by assurance activities are assessed, prioritized and, if necessary, corrected in a timely and effective manner.
	5. Based on the technological trend of the test method and the tool used, the test method is reviewed
	(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.
	The following standards may be referred:
	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].
	Documents to be submitted:
	Implementation procedures for SIRT activities (vulnerability monitoring process)
	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.

	(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.
	The following standards may be referred:
	(a) 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:
	- 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;
	- 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.
	- Processes for risk determination/assessment for the relevant information;
	- 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.
	- Evidence that the response procedures would work, for example through exercising and verification that planning assumptions remain valid under test.
	Documents to be submitted:
	Procedures for implementing SIRT activities (incidents)
	– Field monitoring (obtaining incident vulnerability information) procedures
	– Procedure when an incident occurs
	– Procedure when a vulnerability discovered

	− Procedures to ensure that the implemented countermeasures are still effective against new threats obtained through monitoring and detection.
	"The requirement should be considered unfulfilled if one of the following statements is true:
	1. The vehicle manufacturer is not gathering information to understand the attackers' motivations, targets, and attack patterns.
	2. When information on cyber-attacks, threats, and vulnerabilities to vehicle types is updated, updates are not applied in a timely manner based on the impact assessment of the results of the risk assessment.
	3. The vehicle manufacturer has not verified the usefulness of the information to understand the attacker's motivations, targets, attack patterns. Or it has not shared feedback with the provider, authorized aftermarket service provider, or other users on relevant information.
	4. There is no system to carry out monitoring work or there is no human resource with the necessary specialized skills.
	5. Monitoring staff do not have the appropriate expert skills to be able to obtain an overview and identify and share information with relevant departments (for cyber-attacks, threats and vulnerability information related to their vehicle type).
	6. There is no system to carry out the monitoring work, or there is no human resource with the necessary specialized skills, and the information cannot be reported to internal personnel.
	7. It is not a priority process to deal with security warnings related to its own vehicle type when they are reported."
	"The requirement may be considered fulfilled if all the following statements are true:
	1. Security and vehicle behavior data are collected even in normal times in anticipation of possible security problems (cyber-attacks, threats, and vulnerabilities) related to the vehicle type.
	2. Upon receiving security alert information from third parties, the process is to conduct necessary activities such as impact analysis and risk assessment on the company's products.
	3. Some log data sets can be easily confirmed using a fault diagnostic tool or the like.
	4. When asset or system warning information is received, those that fall within the company's vehicle type and are deemed to require action as a result of the risk assessment are dealt with in accordance with the defined process.
	5. When a security warning is issued for a vehicle type, it is a process to take the necessary action as a priority.
	6. When the vehicle manufacturer obtains information on cyber-attacks, threats, and vulnerabilities, it applies updates as appropriate to the types of its vehicles for which it has determined, as a result of the risk assessment, that action is necessary.
	7. The vehicle manufacturer has processes to monitor, detect and respond to cyber-attacks, cyber threats and vulnerabilities related to business needs, or specific threats in the automotive domain.

	8. The vehicle manufacturer knows how effective its processes are (For example, by tracking how they help to identify security issues).
	9. Monitoring staff have appropriate expertise and knowledge at a level that enables them to obtain an overview of cyber-attack, threat and vulnerability information, identify relevant departments and share information.
	10. Monitoring staff have the necessary professional skills and can report to other parties in the organization.
	11. The vehicle manufacturer has demonstrated a risk assessment process to verify that implemented cybersecurity measures are still effective in the event of a security issue (cyberattack, threat or vulnerability) related to its vehicle type."
	(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.
	It shall be demonstrated that a process has been established to provide the data necessary for the analysis to the department in charge of the analysis (or the person conducting the analysis, if the analysis is outsourced).
	The following standards may be referred:
	(a) 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 Security Incident Response Team 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 a vulnerability is discovered (including an overview of what information is passed to the analyst in what steps).
	- Example format used to provide relevant data (result description can be blank or reference)
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 clause 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.
	The following standards may be referred:
	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
	The following could be used to evidence the processes used:
	(a) 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) Demonstration of how the procedures are implemented.
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 clause 7.2.2.2 (g) shall be continual. This shall:
	(a) Include vehicles after first registration in the monitoring;
	(b) Include the capability to analyze and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs. This capability shall respect clause 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 vehicles of the manufacturer that fall within the scope of their Cyber Security Management System and use:
	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, (as applicable) are particularly relevant to this requirement,
	The following standards may be referred:
	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:
	(a) 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
	(b) Demonstration of how the procedures are implemented.
	If 7.2.2.4.(a) and 7.2.2.4.(b) are not mentioned in the above documents, a separate standard or procedure shall be submitted.
	For 7.2.2.4. (a), procedures for collecting and analyzing published vulnerability information, incidents, etc. and for 7.2.2.4.(b), procedures for detecting and analyzing threats, vulnerabilities, cyber-attacks, etc. from vehicle data and logs shall be described.
	It should be stated that privacy protection including personal information is taken into consideration when handling these items.
	A sample format for reporting discovery and analysis results can be submitted as evidence (The result description may be blank or reference.)
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 clause 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. OEMs shall enter into a contract (e.g., CIA, etc.) that clarifies the division of responsibility between the supplier and the OEM for the requirements of 7.2.2.2.
	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 authorized 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-organizations 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).
	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:
	(a) Contractual agreements in place or evidence of such agreements. They should cover liability breakdown points and how to manage supplier liability.
	(b) Evidenced arguments for how their processes will ensure suppliers / service providers will be considered in the risk assessment process. For this purpose, Internal procedures for selecting and contracting suppliers (for security targets only) & Supplier CS management rules (security only) may be considered.
	(c) Procedures/Methods of sharing information on risk between suppliers and manufacturers;
	(d) Existing solutions / contracts like ISMS (Information Security Management System) Standard can be used for evidence. This may be evidenced by certificates based on ISO/IEC 27001 or TISAX (Trusted Information Security Assessment exchange).
	In addition, even after the development and production contracts with suppliers expire, the process for OEMs to take countermeasures if new threats or vulnerabilities are detected must be described.
	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 organizations 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.
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 new model type approvals prior to All Model implementation date (after new model implementation date), 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
	(i) The Certificate of Compliance for CSMS to demonstrate it is still valid;
	(ii) Confirmation that the CSMS is appropriately applied to the vehicle type model 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
	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:
	"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.
	The following standards may be referred:
	(a) 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 D, 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 D, 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 services shall refer to Annex D, of the Cyber Security Standard 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 D 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.
	(h) ETSI TS 103 645 may be used for demonstrating the security of Internet of Things elements of a vehicle;
	(i) 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, indicating 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 vehicles in production will use the same measure as pretended to the Approval Authority / Technical Services for the vehicle type. Confidentiality of specifies and how these are handled should be agrees

	and recorded.
	Documents to be submitted
	- List of controllers comprising the vehicle (security targets only)
	- A summary of the following implementation status for each controller. (A table summarizing whether it has been implemented or not is sufficient. ）
	(i) Identifying essential elements of the vehicle (assets to be protected)
	(ii) Implementation of risk assessment (for all risks associated with the type)
	- The consideration of each item in Annex D Part A should also be explained. (Provide a list of relevant Annex D threats for the type. However, the reasons for items that do not apply should be briefly explained. ）
	(iii) Implementation of risk management (all managements related to the type)
	- It is sufficient to have a table summarizing whether or not measures have been implemented to control internally whether the implementation status and contents are appropriate regarding (i) and (ii).
	②Documents to be checked
	- Evidences describing the contents of documents corresponding to 7.2.2.2_b) and c) shall be provided for all electronic controllers presented in ①.
	(= a document stating the specific results of implementation of i, ii and iii above)
	Note : On the back-end side, the same concept as in the vehicle is applied, but the submission of a list of controllers is not required. However, a schematic of the system comprising the back-end side shall be submitted, and the mitigations to be applied and the results of confirming that the measures corresponding to 7.2.2.2 _b) and
	c) are applied to the system described here shall be explained.
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 D, Part B and C which are relevant for the risks identified. However, if a mitigation referred to in Annex D, 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 new model type approvals prior to All Model implementation date (after new model implementation date), the vehicle manufacturer shall ensure that another appropriate mitigation is implemented if a mitigation measure referred to in Annex D, 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 D, 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 D being "not relevant or not sufficient", but also may present a rationale, that another mitigation other than the ones listed in Annex D 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.
	The following standards may be referred:
	(i) 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;
	(ii) 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:
	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.
	① Documents to be submitted
	- List of controllers comprising the vehicle (security targets only)
	- A summary of the following implementation status for each controller. A table summarizing whether it has been implemented or not is sufficient.
	(i) Implementation of mitigation measures to protect vehicle types (for all mitigation measures deemed necessary as a result of the risk assessment)
	- The consideration of each item in Annex D Part B and C shall also be explained. Provide a list of applications of the mitigations specified in

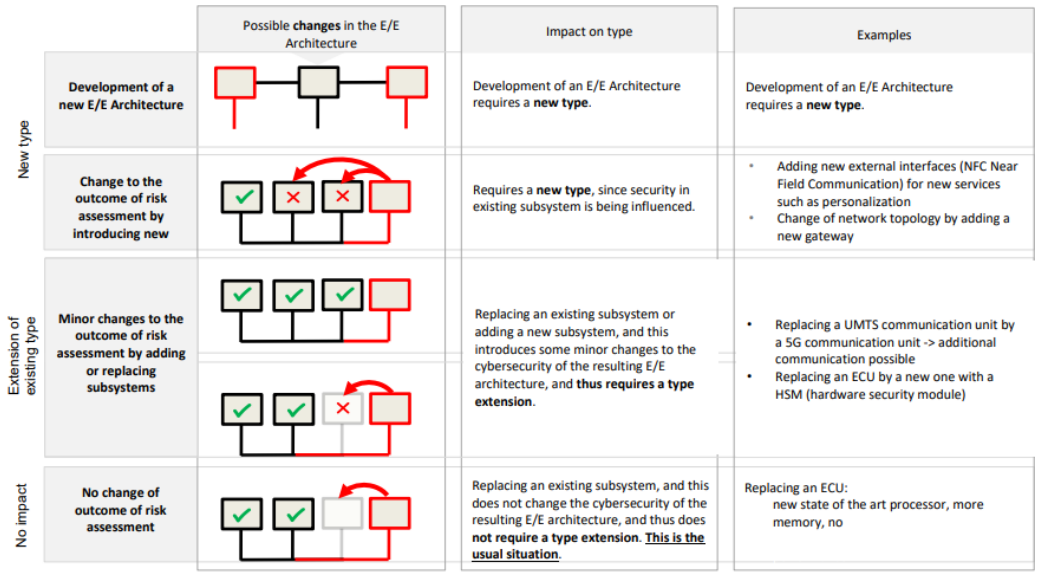
	Annex D for the relevant threat in that type. However, for items for which mitigation measures are not applied, a brief explanation of the reason shall be provided.
	② Documents to be checked
	Evidences describing the contents of documents corresponding to 7.2.2.2_b) and c) should be provided for all electronic controllers presented in ①.
	(= a document stating the specific results of implementation of (i) above)
	Note: On the back-end side, the same concept as in the vehicle is applied, but the submission of a list of controllers is not required. However, a schematic of the system
	comprising the back-end side shall be submitted, and the mitigations to be applied and the results of confirming that the measures corresponding to 7.2.2.2_d) are applied to the system described here shall be explained.
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 intention of this requirement is to explain measures for aftermarket products and services (including services that utilize connected feature). The objective is not to screen aftermarket products and services per se, but to ensure that the subject vehicles are adequately protected when they are fitted.
	Also, give clear notice that any service not approved by the OEM is the customer's responsibility. (Use owner's manual, etc.)
	Even in this case, appropriate measures should be taken on the vehicle side to the extent possible by the OEM in accordance with 7.2.2.2.
	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.
	The following standards may be referred:
	- 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) A description of the dedicated environment;
	(b) What security measures are implemented, including information on how they work;
	(c) Information on any security measures should permit the Test Agency be assured that they do what the manufacturer intends and that vehicles in production will use the same measure as presented to the Test Agency for the vehicle type approval. Confidentiality of specifics and how these are handled

	should be agreed and recorded;
	(d) Annex D of the cyber security Standard shall be referred to.
	① Documents to be submitted
	- System architecture diagram (showing the connection range of aftermarket products (range of measures taken))
	- Summary of Documents (Only state whether measures have been taken, and if the owner's manual or any other means reminds the user, state it.)
	② Documents to be checked
	Documents showing that the subject vehicle is properly protected when fitted with aftermarket products. Specifically, it shall be possible to confirm that the risk is being handled appropriately in the sections of 7.2.2.2. (The description of this section may be implemented in 7.2.2.2.)
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 Test Agency 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.
	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 refined cybersecurity specification, [WP-11-02] Validation report.
	The following could be used to evidence this requirement:
	(a) What is tested and why (e.g. what measures of success for the test look like);
	(b) Methodology used and why (e.g. this may include notes on the extent and effort contained within the testing);
	(c) 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);
	(d) Confirmation of its successful outcome (this may include the pass/fail criteria and result of the test).
	Documents to be submitted
	- List of controllers comprising the vehicle (security targets only)
	- Controllers' names and main functions
	- Summary of confirmation that the measures applied are working effectively
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
	(a) The vehicle is equipped with reasonable measures to detect cyberattacks and protect the vehicle. Take action according to the results of the risk assessment. e.g. Gateway filtering, message authentication, etc.)
	(b) OEM must have the capability to record logs necessary for analysis when an attack is attempted or the system is damaged.
	(c) There must be the function to retrieve the log of (b) above. e.g. via DLC, via server etc.)
	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 analyses 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, (as applicable) are particularly relevant to this requirement.
	The following standards may be referred:
	ISO/SAE 21434. A list of sources for cybersecurity monitoring is provided in clause 7.3. The results of analysis and how to document it is described in [WP-07-04] Vulnerability analysis.
	The following could be used to evidence this requirement:
	(a) Attack prevention measures applied to the vehicle type;
	(b) Demonstration of how a vehicle type's preventive measures and monitoring activities perform;
	(c) Demonstration of how forensic analysis is performed.
	Documents to be submitted
	(a) Explain the following for cyber attack detection and reasonable measures to protect vehicles. (The description in 7.3.4 may include the following)

	Detection: Outline appropriate measures to detect and protect vehicles from attacks that risk assessments have determined require mitigation.
	Mitigation: Explain that reasonable measures have been taken for detected attacks.
	(b) A list of log data stored and used for analysis and a summary of the parameters included in the data. And a summary explanation of the rationale for selecting the data. Include a description of where the log data is stored (cars, back end, etc.).
	(c) An overview of how to retrieve logs, etc., and a sample of the retrieved results. To retrieve logs, explain the path from where the logs are stored to where the information is transmitted via communication to the analysis department.
	In addition, samples may be explained using forms or formats that are actually used. Moreover, explain the methods of analysis and the methods of response based on the results.
7.3.8	Cryptographic modules used for the purpose of this Standard 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 encryption methods used can be justified.
	- When using cryptographic modules as a result of the risk assessment, use a common cryptographic module that is recognized for its robustness rather than each company's proprietary cryptographic method. Each company's proprietary cryptographic module, if used, shall be justified. (e.g. FIPS, CRYPTREC, SP800-57, SP800-140, NESSIE)
	- 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.
	Documents to be submitted
	List of the cryptographic modules used for the model which includes the following aspects:
	- Each cryptographic module. Whether it is a common module or a proprietary one.
	- In the case of a common module, it is necessary to explain the basis for considering it as common. (Eg. Explanation that the method has industry-standard strength at the time of examination, such as ISO, JIS, or some other industry standard.)
	- If a unique module is adopted, an outline of the module and its validity must be explained.
	- A technical explanation shall be given that the appropriate cryptographic modules are selected from the results of the risk assessment. The selection method may be based on the OEM's thinking. However, if it is presumed that the cipher strength is insufficient regardless of the transmission content that is important for safety (e.g., the cipher strength is obviously lower than that of recommended modules), the reason for using the module shall be confirmed in more detail.

	The subject of the cryptographic module to be confirmed in this requirement shall be deemed to have been determined as a result of 7.3.4 (risk assessment) that encryption of communications is necessary as a means of mitigating a threat, and such function has been introduced.
	Note: Ensure that appropriate (robust) cryptographic module is used where risk is analyzed as high in the risk assessment. On the other hand, cryptographic module used arbitrarily in low-risk areas where there is no particular need for encryption are not subject to review.
7.4.1	The vehicle manufacturer shall report at least once a year, or more frequently if relevant, to the test agency the outcome of their monitoring activities, as defined in clause 7.2.2.2.(g)), this shall include relevant information on new cyber-attacks. The vehicle manufacturer shall also report and confirm to the test agency 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 Test Agency who granted the type approval and 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.
	The following standards may be applicable:
	(a) 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.
7.4.2	The test agency 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 test agency may decide to withdraw the CSMS in compliance with clause 6.8.
	Explanation of the requirement
	The Test Agency 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 Test Agency may decide to withdraw the CSMS in compliance with paragraph 6.8.”
	No guidance included in this document with regards this requirement
8.0	**MODIFICATION AND EXTENSION OF THE VEHICLE TYPE**
8.1	Every modification of the vehicle type which affects its technical performance with respect to cybersecurity and/or documentation required in this standard shall be notified to the test agency which approved the vehicle type. The test agency may then either:
8.1.1	Consider that the modifications made still comply with the requirements and documentation of existing type approval; or
8.1.2	Proceed to necessary complementary assessment pursuant to clause 6, and require, where relevant, a further test report by conducting the tests.

8.1.3	Confirmation or extension or refusal of approval, specifying the alterations, shall be communicated by means of a communication form conforming to the model in Annex B to this Standard. The test agency issuing the extension of approval shall assign a certificate number for such an extension and issue it to vehicle manufacturer by means of a communication form conforming to the model in Annex B to this Standard.
	Explanation of the requirement
	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.
	
	Link with ISO/SAE 21434:2021(E)
	The following table provides a summary of the link between the requirements of this Regulations and the relevant paragraphs of ISO /SAE 21434:2021

	Paragraph	*Clauses from ISO/SAE 21434:2021*
	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	Clauses 5, 6, 8
	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 8, 9, 10, 11
	Production phase	Clause 12
	Post-production phase	Clauses 8, 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]
	Management of cyber security relevant processes	[RQ-05-02], [RQ-05-08]
	(a3) Establishment and Maintenance of cyber security culture and awareness	[RQ-05-06]. [RQ-05-07]
	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-15-01]. [RQ-15-02], [RQ-15-03], [RQ-15-08]. The threats in Annex 5 of UN Regulation No. 155. 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-15-15], [RQ-15-04], [RQ-15-05], [RQ-15-10], [RQ-15-16]
	(c2) Is a process established to treat cyber security risks for vehicle types across development, production and post-production?	[RQ-15-17], [RQ-09-05], [RQ-09-06]
	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-09-07], [RQ-09-11], [RQ-11-01]
	(e) The processes used for testing the cyber security of a vehicle type	
	(e1) Is a process established to specify cyber security requirements?	[RQ-09-09], [RQ-10-01]

	(e2) Is a process established to validate the cyber security requirements of the item during development phase?	[RQ-11-01]
	(e3) Is a process established to validate the cyber security requirements of the item during production phase?	[RQ-11-01]
	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-08-07], [RQ-06-09], [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-08-01]
	(g2) Is a process established to detect cyber security events?	[RQ-08-02]
	(g3) Is a process established to assess cyber security events and analyse cyber security vulnerabilities?	[RQ-08-03], [RQ-08-04]
	(g4) Is a process established to manage identified cyber security vulnerabilities?	[RQ-08-05], [RQ-07-06], [RC-07-08]
	(g5) Is a process established to respond on cyber security incidents?	[RQ-13-01], [RQ-13-02]
	(g6) Is a process established to validate effectiveness of the response?	[RQ-11-01]
	(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-08-03], [RQ-08-04]
	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 21434:2021 [RQ-08-07], [RQ-08-08]
	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 8.3 "Cybersecurity Monitoring"
	Capability to analyse and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs	8.4 “Cybersecurity event evaluation”, 8.5 “Vulnerability analysis”
	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], [RQ-07-04], [RC-07-05]
	Dependencies that may exist with contracted service providers	[RQ-06-10], [RQ-07-04], [RC-07-05]
	Dependencies that may exist with manufacturer’s sub-organizations	[RQ-06-10], [RQ-07-04], [RC-07-05]