TFCS-15-03

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

|  |  |  |
| --- | --- | --- |
|  | United Nations | ECE/TRANS/WP.29/201x/xx |
| _unlogo | **Economic and Social Council** | Distr.: GeneralDD MM YYYYOriginal: 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. 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**

Not included in this document as it is assumed guidance is not needed here for testing

**2. Definitions**

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

**3. Application for approval**

Not included in this document as it is assumed guidance is not needed here for testing

**4. Marking**

Not included in this document as it is assumed guidance is not needed here for testing

**5. Approval**

Not included in this document as it is assumed guidance is not needed here for testing

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

Not included in this document as it is assumed guidance is not needed here for testing

**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 |
| - |

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

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

|  |
| --- |
| Explanation of the requirement |
| The intention is to highlight that the principles, threats and mitigations/controls listed in the Cyber security recommendation (particularly annexes B and C) can be used as a reference for evidencing the risk assessment or the approach taken by a vehicle manufacturer and as a reference point for a technical service assessing the evidence provided. The Cyber security recommendation could be used to show: - How the principles listed have been demonstrated through the CSMS- How the risk assessment has considered the risks identified - How the mitigations/controls listed have been considered or what other controls have been implemented to reduce any risks identifiedIt is to be noted that the risks and mitigations listed in the recommendation are not to be considered to include all possibilities and may not be applicable to all vehicle designs. Therefore, the manufacturer may need to consider other risks and other mitigations/controls may be equally (or more) appropriate. Other standards or reference material may be used.The follow clarifications should be noted:- Vehicle Manufacturer is the legal entity registering for initial assessment and requesting type approval |

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

**7.2. Requirements for the Cyber Security Management System**

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

|  |
| --- |
| 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 regulationFor 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:* Preliminary assessment is the same as initial assessment
* The CSMS may be a part of the organization’s Quality Management System or be independent of it
 |

|  |
| --- |
| 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. Clause 5,6,7,8,9 processes could be used to evaluate the CSMS.
* ISO/SAE 21434, ISO 18045, ISO 15048, 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 considers 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
* 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 may be used to evidence this
* Other standards that may be applicable to 7.2.2 and its sub-requirements include: ISO 18045, ISO 15048, 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. 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 |
| Standards such as ISO/SAE 21434 and 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.  |

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

|  |
| --- |
| 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

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
 |

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
* 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
 |

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
* 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
 |

e)  The **processes** used for **testing** the security of the ~~system~~ vehicle type throughout its development and production phases;

|  |
| --- |
| 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
* 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
 |

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 |
| The following standards may be applicable:* ISO/SAE 21434
 |

g)  The **processes** used to **monitor** for, **detect** and **respond** to **cyber-attacks** on vehicle types;

|  |
| --- |
| 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 {Clause 9}. The clause will be updated from the interim draft

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
	+ Vehicles not yet registered
* Evidence that the response procedures would work, for example through exercising and verification that planning assumptions remain valid under test.
 |

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

|  |
| --- |
| Explanation of the requirement |
| The intention of this requirement is to ensure that the manufacturer has processes to monitor for threats that were not anticipated to vehicle types during development and production, or threats that have significantly changed, and that there are processes to assess their relevance to those vehicles. It is noted that requirements 7.2.2.2 parts f) to h) may have overlaps in terms of the processes used and therefore the same evidence may be applicable to demonstrating that these requirements are met.  |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| The following standards may be applicable:* ISO/SAE 21434 Clause 9. The clause will be updated from the interim draft
* ISO/SAE 21434 Clause 5.1.4.5. The clause will be updated from the interim draft

The following could be used to evidence the processes used:* Monitoring processes or activities that would identify threats and vulnerabilities from comparable industries or other threat sharing platforms
* Processes used to assess whether the threats identified are relevant to existing vehicle types
 |

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

|  |
| --- |
| Explanation of the requirement |
| The intention of this requirement is to ensure that the manufacturer has processes to assess whether any new or evolving threat, that may be relevant to a given vehicle type, would require them to initiate a response plan. An outcome of the process may be a decision not to act/accept the risk or to initiate a response.The following clarification should be noted:- The term “react” can be used synonymously with “respond” (suggestion to amend regulatory text) |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| The following standards may be applicable:* ISO/SAE 21434, clause 9 - The clause will be updated from the interim draft

The following could be used to evidence the processes used:* Cybersecurity information assessment processes. These will be processes for the identification of the relevance of the information collected with respect to a vehicle type and its risk assessment
* Processes for risk determination/assessment
* Identified or stated triggers (risks) that would lead to an escalation or action
* Incident response procedures, which may include evidence of procedures for:
* Handling any dependencies and interactions with suppliers
* Determining what response options might be implemented for which condition
* Already registered vehicles
* Vehicles not yet registered
* Demonstration of the processes either through practical application or through internal exercising

It is noted that evidence submitted for clause g) may be used here in terms of assessment and response procedures. |

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

|  |
| --- |
| Explanation of the requirement |
| The intention of this requirement is to highlight that the “resolution”/guidance part of the Cyber security recommendation can be used as a reference.This requirement does not exclude the use of other standards or reference material as evidence.It should be noted that the Recommendation / Resolution on Cyber Security may be updated. |

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

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

|  |
| --- |
| 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:* 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 cloud providers, telecom providers and internet 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.

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 The clause for suppliers (Security and Supplier Relationships)

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. |

**7.3. Requirements for vehicle types**

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

|  |
| --- |
| Explanation of the requirement |
| The intention of this requirement is to ensure that there is a valid CSMS Certificate of Compliance 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 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 Approval Authority or Technical Service shall verify that the manufacturer has taken the necessary measures relevant for the vehicle type to:

|  |
| --- |
| Explanation of the requirement |
| The intention of this requirement is to prescribe the activities of the Approval Authority or Technical Service. The following clarification should be noted:* This requirement is linked to those described for the CSMS in 7.2.2 (and its sub-requirements). The CSMS describes the processes that the manufacturer is required to have. This requirement ensures that they are applied to the vehicle type being approved. Whilst the processes listed in the CSMS may be generic, how they are applied will be specific to each vehicle type.
 |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| Standards such as ISO/SAE 21434 and BSI PAS 1885 could be used to help evidence this requirement and its sub-clauses. ~~The use of relevant parts of analogous assessment frameworks, such as that used for the Network and Information Systems Directive, may be used by either Technical Services or Manufacturers to evidence or assess the information provided. An example of such a framework is provided here:~~ [~~https://www.ncsc.gov.uk/collection/nis-directive/cyber-assessment-framework~~](https://www.ncsc.gov.uk/collection/nis-directive/cyber-assessment-framework) |

1. **Collect and verify,** ~~as appropriate~~, **information** **required** under this regulation~~,~~ through the ~~full~~ **supply chain**;

|  |
| --- |
| Explanation of the requirement |
| This requirement specifically references gaining sufficient information from the supply chain and is linked to 7.2.2.4. 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:* "full 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
 |

1. ~~Maintain~~ Document **appropriate design** and **test information**;

|  |
| --- |
| Explanation of the requirement |
| This requirement is intended to ensure that the requirements listed in 7.3.3 – 7.3.6 are appropriately documented with respect to the vehicle type design and any tests of the cyber security aspects of that design. The following clarification should be noted:* Any design or test information will be related to the vehicle type, its risk assessment and any mitigation measures or controls that are implemented.
* ~~The term ‘maintain’ changed to ‘document’ since found more appropriate~~
 |

|  |
| --- |
| 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: * Annex 1, point 12.8.1.2 provides a list of documents required by the information document (the evidence may include additional documents)
 |

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

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

|  |
| --- |
| Examples of documents/evidence that could be provided |
| The following standards may be applicable:* ISO/SAE 21434
* 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
 |

7.3.3. The vehicle manufacturer shall **demonstrate the risk assessment** for the vehicle type, including its subsystems and their interactions ~~in terms of the vehicle systems, the interactions of the different vehicle systems and the entire vehicle~~.



|  |
| --- |
| Explanation of the requirement |
| 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 following clarifications should be noted:~~* ~~"vehicle system" is intended to refer to the dictionary definition of a “system” in terms of a vehicle in the assumption that a vehicle may comprise a number of “sub-systems”. It is for the manufacturer to consider what is a vehicle system. The number and type of systems in a vehicle type will be dependent on its design. Systems within a vehicle may refer to discrete parts of a vehicle type that may provide a given function, for example the HMI (human machine interface) or it may refer to an aspect of the vehicle provided by a supplier (for example the braking system)~~

The approval authority or technical service may refer to Chapter 4 and annex B of the cyber security recommendation to aid their assessment of the manufacturer’s risk assessment. |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| The following standards may be applicable:* ISO/SAE 21434
 |

7.3.4. The vehicle manufacturer shall demonstrate how the **design of critical elements** of the vehicle type **are protected** against risks identified in the vehicle manufacturer’s risk assessment. Proportionate mitigations shall be implemented to protect such elements.

|  |
| --- |
| 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:* 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 B and C of the cyber security recommendation may be referred to.
 |

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

|  |
| --- |
| 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

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 B and C of the cyber security recommendation may be referred to.
 |

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

|  |
| --- |
| 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

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,..).
 |

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

Not included in this document as it is assumed guidance is not needed here for testing

**9. Conformity of production**

Not included in this document as it is assumed guidance is not needed here for testing

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

Not included in this document as it is assumed guidance is not needed here for testing

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

Not included in this document as it is assumed guidance is not needed here for testing

**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. **General**

0.1 Make (trade name of manufacturer): .................................................................

0.2. Type: .................................................................................................................

0.2.0.1 Chassis: ..............................................................................................................

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

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

0.3.1 Location of that marking: ..................................................................................

0.4 Category of vehicle (c): .....................................................................................

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

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

|  |
| --- |
| Q: Any guidance required for this section |
| Answer to Q:  |
| Copied over from Annex 2 of UN R-46 as the below format is based on the UN regulation format. Above is the format of the EU regulation.**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) o*f 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: ...........................*** |

**12. MISCELLANEOUS**

**12.8. Cyber Security**

12.8.1 General construction characteristics of the vehicle type

|  |
| --- |
| Q: Any guidance required for how to evidence this requirement? Q: If relevant, what type of evidence would show compliance? |
| Answer to Q:  |
| **9. Cyber Security****9.1. General construction characteristics of the vehicle type** Note: Shall be a written description of the E/E architecture. |

12.8.1.1 Schematic representation of the vehicle type:

|  |
| --- |
| Q: Any guidance required for how to evidence this requirement? Q: If relevant, what type of evidence would show compliance? |
| Answer to Q: |
| **9.2. Schematic representation of the vehicle type** Note: Shall be a schematic of the E/E architecture – e.g. circuit diagram |

12.8.1.2 Documents for the vehicle type to be approved describing:

1. The outcome of the risk assessment for the vehicle type;

|  |
| --- |
| Q: Any guidance required for how to evidence this requirement? Q: If relevant, what type of evidence would show compliance? |
| Answer to Q: |
| **9.4. Documents for the vehicle type to be approved describing the outcome of its risk assessment** |

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

|  |
| --- |
| Q: Any guidance required for how to evidence this requirement? Q: If relevant, what type of evidence would show compliance? |
| Answer to Q: |
| Delete as this is included in 9.4.Clarification – “non-type approved” was referring to systems approved under other regulations.  |

1. The components of those systems that are relevant to cyber security;

|  |
| --- |
| Q: Any guidance required for how to evidence this requirement? Q: If relevant, what type of evidence would show compliance? |
| Answer to Q: |
| Delete as this is included in 9.4. |

1. The interactions of those systems with other systems within the vehicle type and external interfaces;

|  |
| --- |
| Q: Any guidance required for how to evidence this requirement? Q: If relevant, what type of evidence would show compliance? |
| Answer to Q: |
| Delete as this is included in 9.4. |

1. The risks posed to those systems that have been identified in the vehicle type’s risk assessment;

|  |
| --- |
| Q: Any guidance required for how to evidence this requirement? Q: If relevant, what type of evidence would show compliance? |
| Answer to Q: |
| Delete as this is included in 9.4. |

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

|  |
| --- |
| Q: Any guidance required for how to evidence this requirement? Q: If relevant, what type of evidence would show compliance? |
| Answer to Q: |
| **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**

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

|  |
| --- |
| Q: Any guidance required for how to evidence this requirement? Q: If relevant, what type of evidence would show compliance? |
| Answer to Q: |
| **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.**Clarification – it is the vehicle type being approved, hence suggested amendment. Note: tests on the vehicle type may be described in terms of the testing done as a whole and on parts (for example critical elements) to provide evidence backing claims of the OEM for the vehicle type. To be reviewed in the test phase if further clarification is needed. |

12.8.2 The number of the CSMS Certificate of Compliance

|  |
| --- |
| Q: Any guidance required for how to evidence this requirement? Q: If relevant, what type of evidence would show compliance? |
| Answer to Q: |
| **9.3. The number of the CSMS Certificate of Compliance** |

**9.8. Description of integration of supply chain with respect to cyber security. It includes hardware and software.**

Annex 2

 Communication form

COMMUNICATION

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

issued by : Name of administration:

......................................

......................................

......................................



concerning: 2/ APPROVAL GRANTED

 APPROVAL EXTENDED

 APPROVAL REFUSED

 APPROVAL WITHDRAWN

 PRODUCTION DEFINITELY DISCONTINUED

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

Approval No. ………..

*Copied from Annex 4 UN R-46*

**Extension No.: ..........................................**

**1. Make (trade name of manufacturer): ...........................................................................**

**2. Type and general commercial description(s) ................................................................**

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

**3.1. Location of that marking: .............................................................................................**

**4. Category(ies) of vehicle: ………………………………………………………………**

**5. Name and address of manufacturer / manufacturer’s representative: .............................................................................**

**6. Name(s) and Address(es) of the production plant(s) ..........................................................................**

**7. Number of the certificate of compliance for cyber security management system: …**

**8. Technical Service responsible for carrying out the tests:..............................................**

**9. Date of test report: ........................................................................................................**

**10. Number of test report: ...................................................................................................**

**11. Remarks: (if any).**

**12. Place: ............................................................................................................................**

**13. Date: .............................................................................................................................**

**14. Signature: ......................................................................................................................**

**15. The index to the information package lodged with the Type Approval Authority, which may be obtained on request is attached.**

Annex 3

 Arrangement of approval mark

Model A

(See paragraph 4.2 of this Regulation)



xxx

 a = 8 mm min.

 The above approval mark affixed to a vehicle shows that the road vehicle type concerned has been approved in the Netherlands (E 4), pursuant to Regulation No. xxx, and under the approval number 002492. The first two digits of the approval number indicate that the approval was granted in accordance with the requirements of Regulation No. xxx **as amended by the 00 series of amendments.**

Annex 4

 Model of CSMS ~~Certificate~~ Certificate of Compliance

**CERTIFICATE OF COMPLIANCE FOR CYBER SECURITY MANAGEMENT SYSTEM(S)**

WITH REGULATION No. [Cyber Security Regulation] xxx

No. [Reference number]

[……. Approval Authority]

Certifies that

Manufacturer or manufacturer’s representative: ...............................................................................................

Address(es) of the manufacturer or manufacturer’s representative: ..................................................................

complies with the provisions of paragraph **7.2.** of Regulation No. xxx

Checks have been performed on:

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

Number of report:

The certificate is valid until […..date]

Done at [……Place]

On […….Date]

[………….Signature]

**Attachments: description of the Cyber Security Management System(s) by the manufacturer.**