Alejandro Manilla August 19, 2019

Comments for Test phase implementation on CS regulation

Requirement **7.1.1** The requirements of this Regulation shall not restrict provisions or requirements of other UN Regulations.	Interpretation This point claims that requirements can be extracted from the guidelines from other regulations.
	Comments This requirement was not possible to evaluate, since OEMs didn't apply any guideline/requirement from other UN Regulations.
Requirement **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	Interpretation This point wants to remark the usage of annexes B and C to identify risk and mitigations.
	Comments OEMS prefers to apply their own assessment methodologies and risk and mitigations databases when performing the analysis. However we think that is necessary to have Annexes B and C for a first reference. The usage of other methods is viable if are applied correctly and follow similar steps.
Requirement **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.	Interpretation Technical service will confirm the correct implementation of the CSMS with the evidences required during section 7 and a final audit. Handbook with the standard processes might be used as evidence.
	Comments OEMs are still working defining a handbook process for the CSMS, the overview presented was correct, and we think that OEMs can perfectly define and end a full handbook process that will comply with the CSMS requirements.

Requirement	Interpretation
7.2.2 *The Cyber Security Management System shall cover the following aspects* **7.2.2.1** The vehicle manufacturer shall demonstrate to an Approval Authority or Technical Service that their Cyber Security Management System considers the following phases: --> Development phase; Production phase; Post-production phase.	[7.2.2.1] can be evidenced with [7.2.2.2] points if it is properly linked. Demonstrate how handle CS during the lifetime of the vehicle for the phases mentioned, comment activities planned. This requirement can be mapped through ISO21434.
	Comments Conflict defining post-production phase, it means after the end of production until a timeframe not specified yet, subject to other legal requirements. Recommended monitoring activities to evidence activities on post-production phase, this can be evidenced in [7.2.2.2.g]. Phases should be defined, and specified in the regulation, special confusion detected in post-production phase This was already noticed and exposed during coordination meeting.
Requirement **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:	Interpretation 7.2.2.2 is covered by the next points and can be used also to evidence 7.2.2.1 if properly linked.
	Comments -
Requirement **7.2.2.2.a** The processes used within the manufacturer's organization to manage cyber security.	Interpretation Not cybersecurity of the entire information security management system of the organization, focus on the relevant processes for the cybersecurity of the vehicle types. Overall cybersecurity strategy, principles and organization structure. Take in account the phases mentioned in 7.2.2.1.
	Comments Overall cybersecurity strategy and organization is already clear from an organization point of view from the OEMs, minor details needs to be take into account to focus on vehicle type security and link it correctly

Requirement	Interpretation
7.2.2.2.b The processes used for the identification of risks to vehicle types;	No interpretation required
	Comments OEMs can use own methodology to perform Risk Assessments, if no specific methodologies are detailed. Then we suggest adding steps/parameters to cover to ensure that the methodology of risk assessment applied is valid, and we are able to get the same conclusions. ISO21434 draft has already explanation detail on risk assessment.
Requirement **7.2.2.2.c** The processes used for the assessment, categorization and treatment of the risks identified	**Interpretation** In these points is expected to review the Threat Analysis Risk Assessment of the system implemented by the manufacturer and the processes to treat the risks identified. - Overall system description with: definition of the system functions, boundaries and interactions with other systems, vehicle architecture, and operational environment of the system. - Critical points and risk level of the systems related to cybersecurity - Identification of the possible assets, threats and vulnerabilities. The method to apply the TARA is open, recommended use methodologies described in SAEJ3061/ISO 21434. Specify the processes of the methodology applied and reference it.
	Comments OEMs can use own methodology to perform Risk Assessments, if no specific methodologies are detailed. Then we suggest adding steps/parameters to ensure that the methodology of risk assessment applied is valid, and we are able to get the same conclusions. ISO21434 draft has already explanation detail on risk assessment.

Requirement	Interpretation
7.2.2.2.c The processes used for the assessment, categorization and treatment of the risks identified	In these points is expected to review the Threat Analysis Risk Assessment of the system implemented by the manufacturer and the processes to treat the risks identified. - Overall system description with: definition of the system functions, boundaries and interactions with other systems, vehicle architecture, and operational environment of the system. - Critical points and risk level of the systems related to cybersecurity - Identification of the possible assets, threats and vulnerabilities. The method to apply the TARA is open, recommended use methodologies described in SAEJ3061/ISO 21434. Specify the processes of the methodology applied and reference it.
	Comments From our interpretation right now, methodology explained by OEMs covers the requirement but needs to be deep explained and provide documentation of the method parameters and how to calculate it. Ex. Table of severity, parameters take into account for likelihood, etc.
Requirement	Interpretation
7.2.2.2.d The processes in place to verify that the risks identified are appropriately managed	Provide the processes to manage appropriately the risks and the residual risks.
	Comments IDIADA suggest the documentation of how this process is managed in all the phases. Also, clarify assumptions when a threat is not dependent directly to OEMs or it is not feasible to be mitigated by OEMs.

Requirement	Interpretation
7.2.2.2.e The processes used for testing the security of the vehicle type throughout its development and production phases;	Appropriate cybersecurity capabilities and processes for testing the system throughout the development and production phases. - For development phase --> Strategies, rules and cybersecurity processes for testing system design, SW/HW development, integration and the processes to document the results of the tests mentioned. Also demonstrate the capability to perform the tests. - For production phase --> Processes for testing requirements, configuration, controls, specifications on production plan that are in accordance with the development phase and the processes to document the results of the tests mentioned.
	Comments Doubts find by OEMS on when is required perform testing, if during all the phases, or only with the final version of the vehicle type/components.
Requirement **7.2.2.2.f** The processes used for ensuring that the risk assessment is kept current.	Interpretation No interpretation required
	Comments OEMs didn't identify difficulties to reach this requirement, we encourage to follow ISO21434 that provides guidelines for the TARA and to keep it updated.
Requirement **7.2.2.2.g** The processes used to monitor for, detect and respond to cyber-attacks on vehicle types.	Interpretation These points shall demonstrate platforms to: - Inform about the vulnerabilities/threats discovered and how to mitigate them. Improvements and knowledge implemented recursively in the production - Monitoring and response to incidents in post-production - Collect the information in order to apply the knowledge and mitigations to the already registered vehicles and for vehicles not yet registered too.
	Comments Processes to detect and respond are defined, but monitoring vehicles is still under development.

Requirement	Interpretation
7.2.2.2.h The processes used to identify new and evolving cyber threats and vulnerabilities to vehicle types	No interpretation required
	Comments Deep definition on evolving threats may be required.
Requirement **7.2.2.2.i** The processes used to appropriately react to new and evolving cyber threats and vulnerabilities.	Interpretation Demonstrate processes to identify new threats and how to react to unexpected new vulnerabilities not contemplated in the TARA.
	Comments Respond methodologies are already defined in 7.2.2.2.g, same approach is followed by OEMs in evolving cyber threats and known threats are detected and needs a response.
Requirement **7.2.2.3** The vehicle manufacturer may refer to [the Recommendation / Resolution on cyber security] when describing the processes, they have employed.	Interpretation Citation of the recommendations followed in the processes used in the CSMS.
	Comments We suggest link the methods explained by the OEMs with the standard and guidelines like ISO21434, SAEJ3061, annexes of the regulation, etc. Right now OEMs are not linking their methodologies described with the ones depicted in the recommended references.
Requirement **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.	Interpretation Manufacturer is responsible that the suppliers follow the requirements for the CSMS. If needed, the manufacturer might audit the evidences presented by the suppliers.
	Comments Hard to demonstrate right now in the implementation phase, but the OEMs have the clear idea on how to proceed with this requirement.

Requirement	Interpretation
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.	Assuming the CSMS is valid, the manufacturer shall list the cybersecurity requirements each vehicle type has to fulfil to be approved. The technical service shall evaluate if the requirements are relevant to the vehicle type and there are no other relevant requirements omitted by the manufacturer.
	Comments Is not possible to extract conclusions of this point, since no specific vehicle type is evaluated. Generally, most of the requirements in vehicle type are hard to evaluate in the current level, the idea of the requirements to provide is mostly clear, but vehicle/systems needs to be further developed to be able to do a deep analysis. Clear definition of vehicle type is required, what changes on the architecture leads to a new vehicle type.
Requirement **7.3.2.a** Collect and verify as appropriate information required under this regulation, through the full supply chain;	**Interpretation** The technical service will evaluate if the manufacturer has evidences about how the suppliers deal with cybersecurity requirements. Check if suppliers have exchanged cybersecurity risk information and mitigations to the manufacturer. Check how supplier and manufacturer did the exchange of cybersecurity related information.
	Comments This point is not clear enough about which are the suppliers that are affected. IDIADA proposes only EE components suppliers are affected and how they deal with cybersecurity shall be evaluated. At the end full vehicle integrated should be also evaluated.

Requirement	Interpretation
7.3.2.b Document appropriate design and test information:	No interpretation required.
	Comments Test depends also on risk assessment, that is covered by the points 7.3.3-7.3.6. At the moment the information received is generic and cannot be applied for a specific vehicle type.
Requirement	Interpretation
7.3.2.c Implement appropriate security measures in the design of the vehicle type.	The technical service will evaluate if the security measures related to the design of the vehicle type are implemented and it includes reference to the assumptions made about external systems interacting with the vehicle. Manufacturer shall document and demonstrate how implements the security measures related to the design of the vehicle type and the vehicle systems. Annex C is proposed to be considered as reference, but it is assumed it could be supported with other evidences as it is not exhaustive enough.
	Comments Provide information of how to deal with Cybersecurity in global, but it is not depicted in detail in the design. We recommend providing the details of the security measures in an architecture schematic. F.E, remark the usage of Firewalls, IDS, secure protocols communications, cryptographic algorithms, where are placed the HSMs, OTA procedures, etc.

Requirement	Interpretation
7.3.3 The vehicle manufacturer shall demonstrate the risk assessment for the vehicle type in terms of the vehicle systems, the interactions of the different vehicle systems and the entire vehicle.	The technical service will validate the evidences related to risk assessment for a specific vehicle type to confirm the application of it. This risk assessment shall include the interaction with other internal and external systems that are relevant for the vehicle type.
	Comments Specific risk assessment for a specific vehicle type was not provided, but examples of the appliance of the risk assessment were showed by the OEMs.
Requirement	**Interpretation**
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.	The documentation shall demonstrate why an element is catalogued to critical and how are defined the security measures needed in order to protect them. The documentation shall include how the previous measures are provided against risks exposed in the points commented in the CSMS part and related to risk assessment. Suggested documentation: Annex B and C.
	Comments OEMs provide information about the Risk Assessment method but not information related to a specific vehicle type and the identification of critical items. IDIADA considers that this point can be covered in a future because OEMs showed the idea to perform it in a real scenario after the test phase.
Requirement	**Interpretation**
7.3.5 The vehicle manufacturer shall demonstrate how it has 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.	The technical service will evaluate the risk assessment and mitigation related to the storage and execution of aftermarket software, services, applications or data.
	Comments OEMs demonstrate the capabilities to reach the requirements, minor details on deeper documentation were required.

Requirement	Interpretation
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.	The technical service will evaluate how the manufacturer has tested the security mitigations applied. The manufacturer shall justify the methodology used and why it is expected to be valid. The result of the tests performed that take in account the critical points identified in the threat analysis risk assessment. The manufacturer shall demonstrate the affirmation exposed in the documentation about successful outcomes. For this point, the manufacturer must apply the point 7.2.2.2.e for the vehicle type as described in the delivered CSMS
	Comments Define some text examples may be required to provide fine evidence. Documentation was required. OEMs are not able to show this type of tests since vehicle type is not developed yet. Process, generic examples, and test definitions were explained.