

## **Questions and Answers/Comments derived from the Workshop on the implementation of UN Regulation No. 155 (Updated, 13 January 2023)**

### **I. Context**

1. UN Regulation No. 155 was established to support vehicle cyber security. This regulation is rather unique in the framework of the 1958 Agreement and also in the field of cyber security. The regulation makes the vehicle manufacturer responsible for ensuring cybersecurity throughout the supply chain and the lifecycle of the vehicle. It requires addressing two types of requirements, those related to the cyber security management and those related to the type approval.

### **II. Specificities**

2. The regulation does not provide a high level of details on the way to evidence the compliance with the requirements. The regulator chose to provide guidance in a guidance document instead of inserting them in the regulation. This choice has an importance in the context of the mutual recognition obligation of type approvals according to the provisions of the 1958 Agreement. The regulator therefore inserted in the regulation the obligation for the approval authorities to exchange information, via the Database for the Exchange of Type Approval (DETA) on the assessment method used in the context of this regulation.

### **III. Workshop on the implementation of UN Regulation No. 155**

3. The Working Party on Automated/Autonomous and Connected Vehicles (GRVA) agreed to organize a workshop on the implementation of UN Regulation No. 155 and the first meeting was organized in 2021, see ECE/TRANS/WP.29/GRVA/10, para. 43. GRVA approved further workshops. To date the expert from NTSEL (Japan) and the secretariat organized 11 workshops.

4. The purpose of these workshops was to gather the approval authorities and technical services that are applying the Regulation. approval authorities of CPs exchanged views on the implementation for fulfilment of the requirements of the Regulation.

5. This document captures and summaries discussions in the workshops in the form of a Q&A. Answers or comments which have been agreed by the workshop so far are summarised as the table below.

### **IV. Questions gathered and discussed**

Categories	Questions	Answers (Comments) – under development
CSMS scope/assessment	How much detail manufacturers' documents should be assessed?	The assessment should entail enough detail to be confident to state that the CSMS is compliant with all relevant requirements of UN R155 and implemented. Harmonization of auditing/assessing manufacturer could be part of future work.
	How the steps to Audit is configured?	Other standards on management systems, such as the ISO/IEC 27000-series or ISO/PAS 5112 etc. could be used as reference.
	How to assess Stage-2-OEM?	Depending on the impact of the changes made by the Stage-2-OEM. The Stage-2-OEM must

	<p>explain the changes made and why they are not CSMS relevant.</p> <p>Three categories have been defined:          Cat. A - UN R155 CSMS for the Stage-2-OEM not required:          Changes which are not cyber relevant and do not relate to the E/E Architecture of the Stage-1-OEM (e.g. by adding pure hardware or devices which are not connected to the E/E Architecture of the Stage-1-OEM).</p> <p>Cat B - UN R155 CSMS might (not) be required: Changes are cyber relevant or related to the E/E Architecture but only with "read-access". Stage-2-OEM has to explain based on a risk assessment why the changes are not relevant.</p> <p>Cat. C - UN R155 CSMS required:          Changes are cyber relevant or related to the E/E Architecture with "read/write" access to the E/E Architecture.</p> <p>For cyber relevant modifications, elements given to the type approval authority/technical service should include information regarding interface between manufactures at each stage.</p> <p>Note: Type approval for multi stage vehicles regarding UN R155 needs to be further explored.</p>
How to assess outsourcing/suppliers?	The manufacturer must demonstrate that the cyber security interface agreement with its suppliers is in place, and how all the relevant items, such as testing, are put under control (documentation / audits).
One or more certificates for one applicant (legal person)?	Manufacturer can have one or more CSMSs. The scope of each CSMS and its CoC has to be defined.
For how long the OEM shall maintain cybersecurity?	The manufacturer must manage the cybersecurity risk until the vehicle is end of life. The strategy must define the conditions for end of life and how cybersecurity risks will be mitigated in the event that software update is no longer provided.
Is it required to have agreements/arrangements for cybersecurity with service providers across all geographies implementing UN R155?	Agreements with service providers do not need to extend to all UN R155 geographies as long as the same level of security is guaranteed (e.g. by disabling the relevant interface)
What should be the depth of review of Information security items for CSMS	The OEM must convince the TS (in audit and test). This might be also by explaining the own strategy, in giving evidence of

	Annex 5 threats/mitigations especially, threats 1.1, 1.2, 1.3, 2.1, 3.1, 3.2, 3.3, 3.4, 3.5, 15.1, 15.2, 16.2, 19.3, 20.2. ?	competence of own staffs who are responsible for these (and other) items, of doublechecking (supplier by the OEM or OEM-developing department or other neutral department etc.).
	How to handle different production sides within the scope of CSMS?	All production sites/plants relevant for UN R155 should be within the scope of CSMS.
	What is minimum criteria on reasonable timeframe?	As a future work, the workshop agreed to develop consensus reasonable timeframe accumulating experiences.
Testing	What is the purpose of test by technical service?	The technical service is expected to assess the submitted documentation of the tests carried out by an OEM to verify the implementation of the OEM's cybersecurity management system during vehicle development. The purpose of testing during vehicle type approval is not to discover new vulnerabilities, but to check the adequacy of the OEM's mitigation measures and give confidence in the testing carried out by the manufacturer during development.
	How many tests? Chosen on what basis?	There is no maximum or minimum recommended number of tests (in the regulation) for the technical services to consider, as each test assessment will depend on the complexity of the OEM's mitigation measures as stated in their technical documentation. Hence technical services may decide to choose to verify any number of an OEM's declared mitigation measures that it deems appropriate, as long as this is in line with the purpose stated in "What is the purpose of test by technical service?" of this table. Any requirements in the approval authority's Method and Criteria document should be taken into account.
	How will the sensitive information related vehicle type be treated?	See "How to handle non-critical elements?" of this table.
	Destructible test methods allowed?	Destructible test methods will not be restricted by type approval authority or technical service. However, the purpose of tests for vehicle type approval is not intended to discover another vulnerability and results of the tests should be reviewed in the perspective of CSMS compliance.
	How much effort (time) shall be spent (in particular on pen-testing)?	Not to specify the number but answer in line with "What is the purpose of test by technical service?" and "How many tests? Chosen on what basis?" of this table.
Homologation process	What communication between the technical	Breadth and depth of communication with the technical service shall be defined ad hoc and may not need to be constrained by precise

	service and the type approval authority?	guidelines. However, a type approval authority wishing to give specific guidance on information exchange may do so within their Method & Criteria document.
	Certificates / approval for suppliers	Certificates to suppliers is not in the scope of this regulation. It is the responsibility of each OEM to specify what methods, standards and associations are applicable to their suppliers.
	Acceptance of foreign Certificates (for CSMS/SUMS) for the type approval	Contracting Parties may, for example by bilateral or by reciprocal agreement, recognize another contracting party's Certificate of Compliance for some or all elements of the Cyber Security Management System. <Introduction of guidance in § K. of the interpretation document regarding § 6.1. of the Regulation> This amendment was proposed in the light of discussing specific scenarios, such as joint ventures, which involve several OEMs and authorities.
	Approval with withdrawn or expired certificate	The CSMS CoC must be valid at the time of signing the UN R155 communication file.
	Extensions for vehicles with approvals under transitional provisions of UN R155	See amendment of the interpretation document. ECE-TRANS-WP29-2022-061e
Risk Assessment	How to handle non-critical elements?	It should be noted that 'non-critical element' is not a defined term in UN R155. Hence, technical services should ensure that OEMs identify non-critical elements within their submitted documentations. Cyber relevant but non-critical elements should also be protected if deemed necessary by the outcome of the threat analysis and risk analysis.

## V. Follow up

6. The participants of the workshop propose the following activities in coming meetings:
  - (a) To complete the table of Q&A(C)
  - (b) To draft a proposal to amend the current official documents ([UN R155 and] its interpretation document) to address the identified issues regarding certification of CSMS and approval of types for UN R 155