United Nations ECE/TRANS/WP.29/GRVA/2021/21

Economic and Social Council

Distr.: General
12 July 2021

Original: English

Economic Commission for Europe

Inland Transport Committee

World Forum for Harmonization of Vehicle Regulations

Working Party on Automated/Autonomous and Connected Vehicles
Eleventh session
Geneva, 27 September – 1 October 2021
Item 5 (a) of the provisional agenda
Connected vehicles:
Cyber security and data protection

Proposal for amendments to UN Regulation No. 155 (Cyber Security and Cyber Security Management System) and the corresponding Interpretation Documents

Submitted by the experts from the Informal Working Group on Cyber Security and Over-The-Air issues (Software updates)*

The text reproduced below was prepared by the experts from the Informal Working Group on Cyber Security and Over-The-Air (OTA) issues (Software updates). It contains an amendment proposal to UN Regulation No. 155 that is aimed to be adopted as Supplement 1 to original version of the Regulation. Amendments to UN Regulation No. 155 and to the Interpretation Document for UN Regulation No. 155 (ECE/TRANS/WP.29/2021/59) are marked in bold for new or strikethrough for deleted characters.

* In accordance with the programme of work of the Inland Transport Committee for 2021 as outlined in proposed programme budget for 2021 (A/75/6 (Sect.20), para 20.51), the World Forum will develop, harmonize and update UN Regulations in order to enhance the performance of vehicles. The present document is submitted in conformity with that mandate.

I. Proposal

A. Amendments to UN Regulation No. 155

Paragraph 7.3.1., amend to read:

"7.3.1. The manufacturer shall have a valid Certificate of Compliance for the Cyber Security Management System relevant to the vehicle type being approved.

However, for type approvals ~~prior to~~ **first issued before** 1 July 2024 **and for each extension thereof**, 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."

Paragraph 7.3.4., amend to read:

"7.3.4. The vehicle manufacturer shall protect the vehicle type against risks identified in the vehicle manufacturer's risk assessment. Proportionate mitigations shall be implemented to protect the vehicle type. The mitigations implemented shall include all mitigations referred to in Annex 5, Part B and C which are relevant for the risks identified. However, if a mitigation referred to in Annex 5, Part B or C, is not relevant or not sufficient for the risk identified, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented.

In particular, for type approvals ~~prior to~~ **first issued before** 1 July 2024 **and for each extension thereof**, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented if a mitigation measure referred to in Annex 5, Part B or C is technically not feasible. The respective assessment of the technical feasibility shall be provided by the manufacturer to the approval authority."

B. Amendments to the Interpretation Documents for UN Regulation No. 155 (ECE/TRANS/WP.29/2021/59)

Part A, 3, paragraph Y. paragraphs 7.3. to 7.3.1., amend to read:

"7.3.1. The manufacturer shall have a valid Certificate of Compliance for the Cyber Security Management System relevant to the vehicle type being approved.

However, for type approvals ~~prior to~~ **first issued before** 1 July 2024 **and for each extension thereof**, 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.

For existing architectures that were developed before CSMS certification, it may not have been possible to develop the architecture in full compliance with that CSMS.

Therefore, for type approvals before 1 July 2024, the provision for "adequate consideration" of cyber security applies but only to the development phase. The production and post production phases of those types must be in full compliance with the certified CSMS.

Further technical modifications/updates leading to extensions of the existing type after 1 July 2024 should be performed as much as possible according to the processes defined in the CSMS for the development

phase. Where there is deviation from the processes defined in the CSMS this should be explained and justified to the technical service or approval authority and the responsibility for the deviation assumed by the vehicle manufacturer at an appropriate management level.

For modifications or updates the Technical Service/Approval Authority may confirm that extensions can be issued after 1 July 2024 based on the method and criteria published to UNECE, in line with paragraph 5 of UN Regulation No. 155.

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

The following could be used to evidence the validity of the CSMS certificate:

(b) The Certificate of Compliance for CSMS to demonstrate it is still valid;

(c) Confirmation that the CSMS is appropriately applied to the vehicle type and any information required to provide assurance.

(d) Information on how updates or extensions are managed within the CSMS for any update to type approvals before 1 July 2024."

Part A, 3, paragraph AB. paragraph 7.3.4., amend to read:

"7.3.4. The vehicle manufacturer shall … another appropriate mitigation is implemented.

In particular, for type approvals ~~prior to~~ **first issued before** 1 July 2024 **and for each extension thereof**, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented if a mitigation measure referred to in Annex 5, Part B or C is technically not feasible. The respective assessment of the technical feasibility shall be provided by the manufacturer to the approval authority."

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 … that interact with the vehicle.

The technical mitigations … to allow the adoption of new or improved defensive technologies.

For existing architectures that were developed before the enforcement of UN Regulation No. 155, it may not have been possible to develop the architecture so that all mitigations in Annex 5, part B and C were implemented. Therefore, for approvals first issued before 1 July 2024, other appropriate mitigations for identified cyber security risks are permitted.

Further technical modifications/updates leading to extensions of those existing types after 1 July 2024 should be performed as much as possible in accordance with Annex 5. This should consider the risks and confirm they continue to be managed or reduced. Where there is deviation from Annex 5 this should be explained and rationalised.

For modifications or updates the Technical Service/Approval Authority may confirm that they consider the risks are appropriately managed, including any deviations, and may confirm that extensions can be issued after 1st July 2024 based on the method and criteria published to UNECE, in line with Chapter 5 of UN Regulation No. 155.

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.

Examples of documents/evidence that could be provided

The following standards may be applicable:

…

(iii) the reason, if mitigation measures are determined to be unnecessary."

II. Justification

1. The Informal Working Group on Cyber Security and OTA issues (Software Updates) discussed at its twenty-second session a request for clarification on the transition clauses specified in paragraph 7.3.1. and 7.3.4. with regards to the extension of type approvals first issue before 1 July 2024 and applied for such extension after that date.

2. The Informal Working Group concluded to provide amendments to (a) the UN Regulation No. 155 (Cyber Security and Cyber Security Management System), see part A of the proposed amendments and (b) the respective Interpretation Documents for UN Regulation No. 155 (ECE/TRANS/WP.29/2021/59), see part B of the proposed amendments, in order to clarify under which circumstances extensions are possible and which additional information is expected to be provided by the vehicle manufacturer applying for approval.

3. Additionally, numbering issues of paragraph Y and AB of Part A, 3 of the Interpretation Documents for UN Regulation No. 155 have been corrected.