United Nations ECE/TRANS/WP.29/GRVA/2024/5

Economic and Social Council

Distr.: General
1 November 2023

Original: English

Economic Commission for Europe

Inland Transport Committee

World Forum for Harmonization of Vehicle Regulations

Working Party on Automated/Autonomous and Connected Vehicles

Eighteenth session
Geneva, 22-26 January 2024
Item 5(a) of the provisional agenda
Connected vehicles:
Cyber security, software updates and over-the-air issues

Proposal for amendments to the Interpretation Document for UN Regulation No. 155 (Cyber security and cyber security management system)

Submitted by the experts from France, Italy, the United Kingdom of Great Britain and Northern Ireland, and the International Motorcycle Manufacturers' Association*

The text reproduced below was prepared by the experts from France, Italy, the United Kingdom of Great Britain and Northern Ireland, and the International Motorcycle Manufacturers' Association. The proposal aims to align the interpretation document with the concurrent amendment proposal for UN Regulation No. 155, extending the scope of the Regulation. The modifications to the existing text of the interpretation document are marked in bold for new characters.

* In accordance with the programme of work of the Inland Transport Committee for 2024 as outlined in proposed programme budget for 2024 (A/78/6 (Sect. 20), table 20.5), 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

Section E, sub item (h), amend to read:

"(h) For type approvals first issued before 1 July 2024 **(or 1 July 2029 for vehicles of Category L)** and for each extension thereof, the criteria that the Approval Authority will apply to assess if cyber security was adequately considered during the development phase of the vehicle type to the effect that it results in an equivalent cybersecurity performance; "

Section Y, amend to read:

"Y. Paragraphs 7.3. to 7.3.1.

"7.3. Requirements for vehicle types

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 of vehicles **of Categories M, N and O** first issued before 1 July 2024**, and for type approvals of vehicles of Category L first issued before 1 July 2029**, 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 **(or 1 July 2029 for vehicles of Category L)**, 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 **(or 1 July 2029 for vehicles of Category L)** 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 **(or 1 July 2029 for vehicles of Category L)** 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 **(or 1 July 2029 for vehicles of Category L)**."

Section AB, amend to read:

"AB. Paragraph 7.3.4

"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 of vehicles of Categories M, N and O first issued before 1 July 2024**, and for type approvals of vehicles of Category L first issued before 1 July 2029**, 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 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 5, 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 5 being "not relevant or not sufficient", but also may present a rationale, that another mitigation other than the ones listed in Annex 5 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.

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 **(or 1 July 2029 for vehicles of Category L)**, 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 **(or 1 July 2029 for vehicles of Category L)** 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 1 July 2024 **(or 1 July 2029 for vehicles of Category L)** 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:

(d) ISO/SAE 21434:2021 describes the determination of risk and the deduced cybersecurity goals and cybersecurity concept based on the identified risks. The results are documented in “[WP-09-03] Cybersecurity goals” and “[WP-09-06] Cybersecurity concept”;

(e) 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:

(f) 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. "

Paragraph 5.1.3., amend to read:

"5.1.3. Auditing requirements

In this chapter auditing requirements shall be listed. These shall be the evidence deemed sufficient by the approval authority to prove that all requirements as listed in paragraphs 7.2.2.1. to 7.2.2.5. are met by the manufacturer~~.~~ **(i**ncluding type approvals prior to 1 July 2024**, or 1 July 2029 for vehicles of Category L**).

Requirements should include the prospective rational to decide if cyber security was adequately considered during the development phase of the vehicle type."

II. Justification

This proposal reflects the concurrent proposal for amendment of UN Regulation No. 155 (document ECE/TRANS/WP.29/GRVA/2024/4), extending the scope of the Regulation to include all vehicles of Category L and giving appropriate lead time for vehicles of this Category when the vehicle type could not be developed in compliance with the manufacturer’s Cyber Security Management System.