United Nations ECE/TRANS/WP.29/GRVA/2024/4

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 a supplement to 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[1*]

The text reproduced below was prepared by the expert from France, Italy, the United Kingdom of Great Britain and Northern Ireland, and the International Motorcycle Manufacturers' Association. The proposal aims to extend the scope of UN Regulation No. 155 to include all vehicles of Category L. The modifications to the existing text of the Regulation are marked in bold for new or strikethrough for deleted 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

Paragraph 1.1., amend to read:

"1.1. This Regulation applies to vehicles, with regard to cyber security, of ~~the~~ Categories **L,** M ~~and~~**,** N **and O, if fitted with at least one electronic control unit.**

~~This Regulation also applies to vehicles of Category O if fitted with at least one electronic control unit~~."

Paragraph 1.2., shall be deleted:

"~~1.2. This Regulation also applies to vehicles of the Categories L_6 and L_7 if equipped with automated driving functionalities from level 3 onwards, as defined in the reference document with definitions of Automated Driving under WP.29 and the General Principles for developing a UN Regulation on automated vehicles (ECE/TRANS/WP.29/1140).~~"

Paragraphs 1.3. (former) and 1.4., renumber as paragraphs 1.2. and 1.3.

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 **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."

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 **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."

II. Justification

1. The purpose of UN Regulation No. 155 is to offer an international framework for the type approval of road vehicles with regard to cyber security. Therefore, GRVA should strive to offer the broadest scope possible to its Contracting Parties, and to allow manufacturers of vehicles of any relevant category to apply for a type approval.

2. During the previous sessions of GRVA and of its informal working group on cyber security and software updates, no technical argument was put forward to justify the exclusion of vehicles of Category L from the scope of the Regulation. Not including this category thus forces Contracting Parties and regional organisations to use national or regional laws on cyber security for this category of vehicles. This could lead to unique requirements and a level of divergence that could be onerous on the industry.

3. Similarly to what was granted to Categories M and N in the original version of the Regulation (paragraphs 7.3.1. and 7.3.4.), an adequate lead time is necessary for manufacturers of vehicles of the category introduced in this proposal to demonstrate adequate cybersecurity measures for the approval of vehicle types whose development phase started prior to the implementation of the manufacturer's Cyber Security Management System. Category L vehicles that were already in scope of the Regulation have been included in this lead time to simplify the drafting and remove reference to levels of automation. As the provisions still require demonstration that cyber security was adequately addressed and any alternative mitigations are appropriate, no issues are foreseen in allowing additional time in this case.