United Nations ECE/TRANS/WP.29/GRVA/2022/17

Economic and Social Council

Distr.: General
13 July 2022

Original: English

Economic Commission for Europe

Inland Transport Committee

World Forum for Harmonization of Vehicle Regulations

Working Party on Automated/Autonomous and Connected Vehicles

Fourteenth session
Geneva, 26-30 September 2022
Item 5(a) of the provisional agenda
Connected Vehicles:
Cyber security and data protection

Proposal for a supplement to UN Regulation No. 155 (Cyber Security and Cyber Security Management System)

Submitted by the experts from SAE International*

The text reproduced below was prepared by the experts from SAE International. It aims at seeking clarification of the requirements of Annex 5, regarding the authentication of Global Navigation Satellite System (GNSS) messages. It is based on informal document GRVA-13-29. The modifications to the existing text of the Regulation are marked in bold for new or in strikethrough for deleted characters.

* In accordance with the programme of work of the Inland Transport Committee for 2022 as outlined in proposed programme budget for 2022 (A/76/6 (Sect.20), para 20.76), 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

Annex 5, Part B, first row of Table B1, amend to read:

Table A1 reference	*Threats to "Vehicle communication channels"*	*Ref*	*Mitigation*
4.1	Spoofing of messages (e.g. 802.11p V2X during platooning, GNSS messages, etc.) by impersonation	M10	The vehicle shall verify the authenticity and integrity of messages it receives **using appropriate mechanisms. Depending on the message type and capabilities, these may include cryptographic authentication and integrity checking; plausibility checking; use of a diversity of sources; and other appropriate means of providing assurance.**

II. Justification

1. The experts from SAE International noted the ambiguous language in Annex B of UN Regulation No. 155 (see more details in informal document GRVA-13-29) that has been interpreted within the automotive industry as putting a narrow requirement on implementations – specifically, a mandatory requirement that vehicles carry out cryptographic authentication of received GNSS messages.

2. This proposal includes amendments that are suggested to be more appropriate and, in practical terms, would lead to more resilient implementations than the interpretation-of-concern of the current wording would.