Submitted by the experts
from OICA and CLEPA

Informal document **GRVA-06-07**
6th GRVA, 3-4 March 2020,
Agenda item 4

Suggestion for amendments of ECE/TRANS/WP.29/GRVA-05-05-Rev.1
(Draft new UN Regulation on uniform provisions concerning the approval of vehicles with regard to cyber security and of their cybersecurity management systems)

The additions and deletions are shown in **bold** text to facilitate identification of these proposed changes.

Paragraph 1.1. amend to read:

1.1. This Regulation applies to vehicles, with regard to cyber security, of the categories M, N, [~~O,~~ R, S and T].

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

Paragraph 5.1.3. amend to read (in order to align it with 7.3.x):

5.1.3. The Approval Authority or Technical Service shall refuse to grant the type approval with regard to cyber security where the vehicle manufacturer has not fulfilled one or more of the requirements referred to in paragraph 7.3., notably:

(a) the vehicle manufacturer did not perform the exhaustive risk assessment referred to in paragraph 7.3.3.; including where the manufacturer did not consider all the risks related to threats referred to in Annex 5, Part A;

(b) the vehicle manufacturer did not **protect** ~~**ensure that critical elements of**~~ the vehicle type ~~**are protected**~~ against risks identified in the vehicle manufacturer's risk assessment **or proportionate mitigations were** ~~**and the vehicle manufacturer did**~~ **not implemented** ~~**the relevant mitigations**~~ as required by paragraph 7.3.4.;

(c) the vehicle manufacturer did not **put in place** ~~**ensure that**~~ appropriate and proportionate measures ~~**have been put in place**~~ to secure dedicated environments on the vehicle type (if provided) for the storage and execution of aftermarket software, services, applications or data;

(d) the vehicle manufacturer **did not perform, prior to the approval,** ~~**has not performed**~~ appropriate and sufficient testing to verify the effectiveness of the security measures implemented ~~**and the outcome of those tests**~~.

Paragraphs 5.3.1 to 5.3.4

Requirements for a peer review between approval authorities are supported by OICA/CLEPA. This peer review shall be decoupled from a single UN type approval regulation.

The perception of a too high abstraction level of this draft UN Regulation is not shared by the experts from OICA/CLEPA.

The protection against cyberattacks and criminal activities cannot be validated by a list of specific pass/fail criteria. This is the reason why a thorough risk analysis is required as proof.

The applicability of the draft Regulation has been confirmed during the test phase and corrections have been made.

A similar level of abstraction will be used in other future regulations, e.g. for the validation of automated driving, and solutions have to be found as well.

Potential solutions:

- *The risk analysis is not high level but a very detailed specific piece of engineering judgement which shall be checked for its comprehensiveness by competent technical services following consensus standards (e.g. ISO/SAE 21434).*
- *Extension of existing peer reviews (e.g. TAAM Type Approval Authorities Meetings, TAAEG Type Approval Authorities Expert Group, or the "Forum") to the UN level, similar to GRSP "TSG Technical Service Group for Child Restraint System R44 & R129".*
- *Integration of mandatory peer reviews in the Schedule 2 of 1958 Agreement "Assessment, designation and notification of technical services / Standards which the technical services, referred to in Part one of this Schedule, shall comply with".*
- *Creating a new schedule in the 1958 Agreement.*

As a consequence, the experts of OICA and CLEPA actively support the proposals by Japan and France for deletion of paragraphs 5.3.1 to 5.3.4.

Paragraphs 7.2.2.2. to 7.2.2.4. amend to read:

7.2.2.2. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System ensure security is adequately considered, including risks and mitigations listed in Annex 5. This shall include:

(a) The processes used within the manufacturer's organization to manage cyber security;

(b) The processes used for the identification of risks to vehicle types. Within these processes, the threats in Annex 5, Part A, and other relevant threats shall be considered;

(c) The processes used for the assessment, categorization and treatment of the risks identified;

(d) The processes in place to verify that the risks identified are appropriately managed;

(e) The processes used for testing the cyber security of a vehicle type;

(f) The processes used for ensuring that the risk assessment is kept current;

(g) The processes used to monitor for, detect and respond to cyber-attacks, cyber threats and vulnerabilities on vehicle types and the processes used to assess whether the cyber security measures implemented are still effective in the light of new cyber threats and vulnerabilities that have been identified.

(h) The processes used to provide relevant data to support [analysis / investigation] of attempted or successful cyber-attacks.

7.2.2.3. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that, based on categorization referred to in paragraph 7.2.2.2 (c) and 7.2.2.2 (g), cyber threats and vulnerabilities which require a response from the vehicle manufacturer shall be **treated** ~~**mitigated**~~ within a reasonable timeframe.

7.2.2.4. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that the monitoring referred to in paragraph 7.2.2.2 (g) shall be continual. This shall:

(a) Include vehicles after first registration in the monitoring;

(b) Include the capability to analyse and detect cyber threats, vulnerabilities and cyber-attacks from **available relevant data** ~~**vehicle data and vehicle logs**~~. This capability shall respect paragraph 1.3. and the privacy rights of car owners or drivers, particularly with respect to consent.

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, if the vehicle manufacturer can demonstrate that the vehicle type could not be developed in compliance with the CSMS, because it was fully developed ~~**before**~~ **latest until [48 months]** after entry into force of this Regulation, then the vehicle manufacturer shall demonstrate that cyber security was adequately considered during the development phase.

Paragraph 7.3.4. amend to read:

7.3.4. The vehicle manufacturer shall protect ~~**critical elements of**~~ the vehicle type against risks identified in the vehicle manufacturer's risk assessment. **For the risks identified, the vehicle manufacturer shall consider the mitigations referred to in Annex 5, Part B** ~~**and C**~~**. Appropriate mitigations shall be implemented to protect the vehicle type.** ~~**Proportionate mitigations shall be implemented to protect such elements. 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, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented.**~~

Paragraph 7.3.7. amend to read:

7.3.7. The vehicle manufacturer shall implement measures for the vehicle type to:

(a) detect **and respond to** ~~**prevent**~~ cyber-attacks against vehicles of the vehicle type;

(b) support the monitoring capability of the vehicle manufacturer with regards to detecting threats, vulnerabilities and cyber-attacks relevant to the vehicle type;

~~**(b) provide data forensic capability to enable analysis of attempted or successful cyber-attacks.**~~

(c) provide relevant data to support [analysis / investigation] of attempted or successful cyber-attacks.