Submitted by the experts from the Aftermarket coalition (EGEA, FIA, FIGIEFA and ETRMA)

Informal document **GRVA-05-16**
5th GRVA, 10-14 February 2020
Agenda item 5(a)

Proposal for a Recommendation on Cyber Security

(ECE/TRANS/WP29/GRVA/2020/2 & /3)

(Proposal for amendments– with tracked amendments)

The text reproduced below aims at proposing improvements to the text of the main text and Draft new UN Regulation on uniform provisions concerning the approval of cyber security. The modifications to the existing text of the proposed Recommendation on Cybersecurity (ECE/TRANS/WP29/GRVA/2020/2 & ECE/TRANS/WP29/GRVA/2020/3) are marked in **bold** for new text and strikethrough for deleted text.

Proposed amendments

2. Definitions

*Insert **new** point 2.14, definition of HMI, used in amendment 7.1.3*

2.14. Human Machine Interface (HMI) means all parts of an interactive system (software or hardware) that provide information and control that is necessary for the user to complete a certain task with the interactive system[1].

3. Application for approval

*Insert **new** point 3.2.4., to read:*

3.2.4. The documentation package shall contain the security relevant descriptions of how confidentiality, integrity and availability shall be ensured including any IT security relevant functionality of security relevant components, at a minimum for the principal security relevant vehicle components, namely the electronic device that monitors and controls the data flow to and from the vehicle, the device for the storage and execution of vehicle related services and the in-vehicle Human Machine Interface (HMI). The security evaluation certificate granting system and administrative provisions shall be regulated at regional or national level.

*Point 3.3.a. **amend** to read:*

3.3. "Documentation shall be made available in two parts:

(a) The formal documentation package for the approval, containing the material specified in Annex 1 **and in accordance with the documentation requirements referred to in point 3.2.4.,** which shall be supplied to the Approval Authority or its Technical Service at the time of submission of the type approval application. This documentation package shall be used by the Approval Authority or its Technical Service as the basic reference for the approval process. The Approval Authority or its Technical Service shall ensure that this documentation package remains available for at least 10 years counted from the time when production of the vehicle type is definitely discontinued.

[1] Source: Definition of user interface: ISO 9241:110

5.Approval

Insert ***new*** *point 5.5., to read:*

5.5. This regulation is without prejudice to other national and regional legislation defining additional minimum compliance criteria and processes for the CSMS and the vehicle type requirements in the cybersecurity regulation.

7. Specifications

Insert ***new*** *point 7.1.3., to read:*

7.1.3. The following principal security relevant vehicle components, namely the electronic device that monitors and controls the data flow to and from the vehicle, the device for the storage and execution of vehicle related services and the in-vehicle Human Machine Interface (HMI) shall be evaluated, validated and certified in accordance with Common Criteria v3.1. Release 5.

Insert ***new*** *point 7.3.9., to read:*

7.3.9. The vehicle manufacturer shall demonstrate to the satisfaction of the Approval Authority or its Technical Service that should critical elements of the vehicle that are designed as part of its security system become non secure, then they shall be upgradeable until the end of life of the vehicle.

The upgraded critical element of the vehicle shall satisfy the following conditions:

a) It shall be approved;

b) Risk Assessment for the upgraded component shall mitigate the security risk of the non-secure critical element.

Justification

Draft new UN Regulation on uniform provisions concerning the approval of cyber security

Background information on the need to secure the vehicle over the entire lifetime

Consumer protection shall be considered. In addition to safety and environmental protection consumers have the right to affordable transportation. It is of paramount importance that the consumer remains in control of scrappage of the vehicle and principally determines when it shall be taken out of circulation, providing the vehicle remains well maintained and fulfils all legal requirements for safety and environmental protection during the remaining time of its lifetime.

The consumer may not be forced to give up this principal control to communication providers, vehicle manufacturers or other commercial parties. Over their lifetime, vehicles may become non-compatible with the latest communication network or with other remote technologies. The vehicle manufacturer shall ensure state-of-the-art protection levels against hacking.

Improvements in road safety and environmental protection by automation and connectivity will only be reached by a high market penetration of automated and connected vehicles. The automated driving functions will prevent between 5.0% and 6.8% of insurance relevant damages in accidents 20 years after their launch in the EU market. A reduction of 1.9% for the heavy accidents will be reached after 20 years. This will only happen, if the IT security is guaranteed over the lifetime of the vehicle.

*Point 2.14, **new***

Definition of Human Machine Interface (HMI) from ISO 11064: Ergonomic design of control centres. For clarification this definition of HMI has been added from ISO 11064. A definition of HMI was deemed needed as it is one of the security-critical components on-board of a vehicle. The definition needs to provide clarity but should not restrict innovative ways to enable human machine interaction

*Point 3.2.4, **new***

In order to provide evidence and demonstrate to the approval authority that the security-by-design principles were applied, the vehicle manufacturer must provide the documents and information that are required by the Common Criteria certification and documentation scheme[2]. It is the intention that from the security analysis and mitigation measures the most relevant hardware devices and associated software is identified and to certify only these high risk devices like e.g. the electronic device that controls the dataflow to and from the vehicle, the device tasked with storage and execution of aftermarket software, services, applications or data, or, the Human Machine Interface devices used for bi-directional communication between authorised remote operator and vehicle occupants.

For the EU, it would mean that in support of the security requirements of confidentiality, integrity and availability, evidence needs to be provided by the manufacturer and be submitted in the documentation package. Any IT security relevant functionalities of relevant security components must be evaluated, validated and certified in line with ISO 15408:2009, applying the mutual recognition agreement of information technology security evaluation certificates of the Senior Officials Group on Information Systems Security (SOG-IS)[3], or an equivalent European cybersecurity certification scheme under the relevant European Cyber Security framework (Regulation (EU) No 526/2013 - Cybersecurity Act[4]).

*Point 3.3.a **amend***

Besides the documentation package relevant for the Cyber Security Management System laid down in Annex A, also the Common Criteria documents and certificates have to be supplied to the approval authority as a solid basis for assessment and approval.

*Point 5.5, **new***

The CS/OTA regulation, in its current state, does not define any objective, fail criteria/minimum compliance criteria for the requirements. While adopting the CS/OTA regulation in its current state, national/regional authorities must ensure that such process descriptions are considered along with the CS/OTA regulation. An initial attempt to identify such process requirements can be found in the document "UNECE_Cybersecurity_process_description", submitted along with this proposal document. These process requirement gives guidance on how

1. Cybersecurity needs to be evaluated for the vehicle type by the approval authority
2. Annex B and Annex C of the Cybersecurity resolution document needs to be considered and taken forward for vehicle approval process.

[2] https://www.commoncriteriaportal.org/cc/ v3.1. Release 5

[3] https://www.sogis.eu/

[4] OJ L 165, 18.6.2013, p. 41–5

3. How this list can be maintained as a living document which does not lose its relevance in the in the wake of identifying new and evolving cyber threats, vulnerabilities, risks and mitigation measures
4. How RXSWIN can be effectively used for security updates. RXSWIN helps us to have an identifier for type approval relevant software updates. Once the cybersecurity regulation is formally adopted by WP29, cyber security updates also becomes type approval relevant, and will need to be managed using the RXSWIN.

*Point 7.1.3., **new***

This point sets out the obligation for the manufacturer to apply Common Criteria to all high risk components and relevant software, namely the electronic device that monitors and controls the data flow to and from the vehicle, the device for the storage and execution of vehicle related services and the in-vehicle Human Machine Interface (HMI). These 3 components are identified as the minimum set of principal security relevant vehicle components. However, if the manufacturer identifies additional components which requires this level of security, the Common Criteria approach can be extended for these components. The obligation does not affect each and every component of the vehicle but only those that in the risk assessment were identified as vulnerable to security system breaches and attacks.

*Point 7.3.9., **new***

Vehicles should have the provision to be kept at the required security level over their lifetime by replacing affected security-critical software and hardware components to ensure continued compliance with the vehicle manufacturer’s cybersecurity type approval. This will help support fair competition and a level playing field for aftermarket players in the automotive domain.

***