|  |  |
| --- | --- |
| **New amendments submitted by the experts from**  **CITA, EGEA, FIA, FIGIEFA, ETRMA** | 17th TFCS, 21st-23rd January 2020 Agenda item IV |

**Proposal for a Recommendation on Cyber Security**

**(ECE-TRANS-WP29-GRVA-2020-03e)**

**(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-2020-03e) are marked in **bold** for new text and strikethrough for deleted text.

Proposed amendments

**2. Definitions**

*Point 2.7.* ***amend*** *to read:*

2.7. “Post-production phase” refers to the period **in** **~~after~~** which a vehicle type is no longer produced **until the end-of-life of all vehicles under the vehicle type**.[[1]](#footnote-1) Vehicles incorporating a specific vehicle type will be operational during this phase but will no longer be produced. The phase ends when there are no longer any operational vehicles of a specific vehicle type **the vehicles have been dismantled and its components recycled.**

*Insert* ***new*** *point 2.14, definition of HMI, used in amendments 3.2.5 and 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[[2]](#footnote-2).**

*Insert* ***new*** *point 2.15, definition of Aftermarket, used in paragraph 7.3.5 and 9.6, definition already included in the cybersecurity resolution*

**2.15.** **"Aftermarket" means the secondary market of the automotive industry, like repairers who provides repair and maintenance services for vehicles, independent operators who are directly or indirectly involved in the repair and maintenance of vehicles, and include repairers, manufacturers or distributors of diagnostic and repair equipment, tools or spare parts, or lubricants as well as publishers of technical information, remanufacturers, automobile clubs, roadside assistance operators, fleet management solution providers, operators offering inspection and testing services, operators offering training for installers, manufacturers and repairers of equipment for electric and alternative-fuel vehicles and independent service providers~~.~~**

**3. Application for approval**

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

**3.2.4.** [**The documentation package shall contain the security relevant descriptions how confidentiality, integrity and availability shall be ensured including of any IT security relevant functionality of security relevant components, at a minimum for 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.

**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 7.1.4., to read:*

**7.1.4. "The vehicle manufacturer shall put in place an incident response policy that shall be applied during the vehicle’s lifetime. The associated incident response plan shall be submitted to the approval authority at approval. "**

*Point 7.3.3.* ***amend*** *to read:*

7.3.3. The vehicle manufacturer shall demonstrate to the satisfaction of the Approval Authority or its Technical Service the risk assessment for the vehicle type and how the risks have been treated/managed. The risk assessment shall consider the systems of the vehicle type and their interactions. The risk assessment shall further consider interactions with any external system **without prejudice to the principle laid down under point 1.3. of this Regulation.”**

*Point 7.3.5.* ***amend*** *to read*:

7.3.5.The vehicle manufacturer shall demonstrate to the satisfaction of the Approval Authority or its Technical Service 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 **without prejudice to the principle laid down under point 1.3. of this Regulation.”**

*Insert* ***new*** *point 7.3.8., to read:*

**7.3.8.** **The vehicle manufacturer shall be responsible for the vehicle’s security over its lifetime until its end-of-life.**

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

**7.3.9** [**The manufacturer may apply for an exemption for the requirement laid down in point 7.3.8. The approval authority may grant the exemption where all of the following conditions are met:**

**National or regional regulation defined a specific time period for full cybersecurity support by the vehicle manufacturer, commencing from the time when production of the vehicle type was definitively discontinued after a minimum period of 10 years;**

**Two years before the vehicle manufacturer submits the request for exemption to the approval authority, all security relevant documentation and information, including all source codes and software descriptions shall be transferred to an authorised party. This authorised party shall become responsible for the vehicle’s security at the approved date by ensuring regular hardware and software updates, until the vehicle’s end-of-life.**

**The type-approval shall definitely end at the approved date referred to under point (b).]**

*Insert* ***new*** *point 7.3.10., to read:*

**7.3.10. [The authorised party referred to in point 7.3.9.b shall be subject to the same obligations and shall be entitled to have the same rights than the vehicle manufacturer**.  **The process to apply for authorisation and be granted approval to take over the vehicle security responsibilities shall be regulated in regional or national approval legislation.]"**

*Insert* ***new*** *point 7.3.11., to read:*

**7.3.11. "** **The vehicle manufacturer shall demonstrate to the satisfaction of the Approval Authority or its Technical Service that critical parts of the vehicle security system are designed to be replaceable over the lifetime of the vehicle.**

Justification

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

*Point 2.7,* ***amend***

The current definition of post-production phase is updated to be in alignment with amendment 7.3.8, and consequently with amendments 7.3.9 and 7.3.10. The amendment text has been referenced from regulation R133.

*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 2.15,* ***new***

Definition of aftermarket, included from the resolution part, for consistency and clarity of use in the regulation text. The term aftermarket is used in requirement 7.3.4 and Annex 1 point 9.6 of the regulation.

*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[[3]](#footnote-3). 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)[[4]](#footnote-4), or an equivalent European cybersecurity certification scheme under the relevant European Cyber Security framework (Regulation (EU) No 526/2013 - Cybersecurity Act**[[5]](#footnote-5)** ).

*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.
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 7.1.4.,* ***new***

If state-of-the-art protection and the applied security by design was not sufficient and the risk increased over time then the manufacturer shall act as quick and effective as possible to resolve the security intrusion and raise the level of protection or address the attacks as swiftly as possible. A security incident response plan shall be submitted to the approval authority before the vehicle is placed on the market and shall contain the reaction of the manufacturer to restore security to the state-of-the-art level. Of course, this protection over the lifetime of the vehicle and keeping at a high level of security needs to remain affordable for consumer and society.

*Point 7.3.3 and 7.3.5,* ***amend***

Include “national/regional legislation”, as we expect this regulation not to overrule the requirements of any provision/requirements in a national/regional legislation as mentioned in the scope requirement 1.3 of this regulation.

1.3- Generic requirement to ensure data access and operational continuity in the wake of cybersecurity measures implemented by the vehicle manufacturer. Requirement 7.3.2 requires the vehicle manufacturer to perform risk assessment and consider vehicle systems and interactions between vehicle systems and external systems. Mitigation measures implemented as a result of considering these interactions should not hinder data access and operational continuity for the aftermarket players.

Requirement 7.3.6 requires the manufacturer to “secure” their dedicated environments on the vehicle type (if provided) for the storage and execution of aftermarket software, services, applications or data. Measures implemented to secure these dedicated environments should not hinder data access and operational continuity for the aftermarket players who uses these dedicated environments.

*Points* 7.3.8*,* 7.3.9*. and* 7.3.10*,* ***new***

This new point serves consumer protection. 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 may not deem it economically viable any longer to provide security hardware and software updates to maintain the vehicle approved at a state-of-the-art protection levels against hacking. In these cases, the consumer should have the choice from alternatives provided by other service providers that allow the vehicle to remain in circulation.

This needs to be the standard norm within the regulation (security until end of lifetime), unless there are regional/ national laws which defines the responsibility of the vehicle manufacturer for a period of “X” years. We should not totally neglect the idea that there may be regional/ national legislations or product liability regulations which may define this serviceability period within a time frame of “X” years. In such situations, the vehicle manufacturer needs to consider this timeframe and inform the approval authority about end of their responsibility.

Consumers may expect that the vehicle manufacturer takes care of the vehicle security remaining at a state-of-the-art level over the lifetime of the vehicle. If the vehicle manufacturer opts to abandon his customers after a minimum period of 10 years and not any longer wishes to supply security relevant hardware and software updates, then other authorised service providers like e.g. TIER I suppliers shall be given the possibility to take over this important responsibility to the benefit of society and the individual consumer. It is unacceptable that security, safety and environmental protection will be put at risk because of lacking security updates, but likewise it is also not acceptable when the consumer is not any longer in control of this highest personal investment and society would be exposed to unjustifiable economic losses. For automation and connectivity to achieve the utmost potential it has with regard to road safety, environmental protection and sustainability, the cyber security of vehicles must be ensured over their lifetime. Downgrading the vehicle to non-automation and non-connectivity may not be the answer.

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.

Furthermore, the authorisation process and which party is eligible and may be authorised to take over the important responsibility from the vehicle manufacturer to ensure security over the lifetime of the vehicle must be regulated at the regional or national level.

*Point 7.3.11.,* ***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 ensure fair competition and level playing field for aftermarket players in the automotive domain.

1. Source: UN Regulation 133 [↑](#footnote-ref-1)
2. Source: Definition of user interface: ISO 9241:110 [↑](#footnote-ref-2)
3. <https://www.commoncriteriaportal.org/cc/> v3.1. Release 5 [↑](#footnote-ref-3)
4. <https://www.sogis.eu/> [↑](#footnote-ref-4)
5. OJ L 165, 18.6.2013, p. 41–5 [↑](#footnote-ref-5)