Submitted by the expert from FIGIEFA

Informal document **GRVA-05-17**
5th GRVA, 10-14 February 2020
Agenda item 5(a)

Proposal for amendments to the draft Regulations on Cyber Security and Software Updates

(Proposal for amendments to ECE/TRANS/WP.29/GRVA/2020/2, /3 and /4)

The modifications to the existing text of the proposed Recommendation on Cybersecurity are marked in **bold** for new text and strikethrough for deleted text.

Amendment to the draft Cybersecurity Regulation

1.Scope

*Insert **new** paragrph 1.4., to read:*

"1.4. This Regulation is without prejudice to national or regional legislation governing the development and installation/system integration of replacement parts and components with regards to cybersecurity. This may include provisions that the vehicle manufacturer shall make available to the authorised replacement part manufacturers the relevant cybersecurity goals, specifications and requirements for product development including validation and authentication procedures. This may also include provisions that the vehicle manufacturer shall make available to the independent repairers and parts distributors, the relevant cybersecurity specifications, requirements and necessary means for installation and activation of authenticated replacement parts."

Justification for the amendment to cybersecurity regulation

1.Scope

Development requirement justification

The introduction of the cybersecurity regulation introduces regulatory requirements for the vehicle manufacturers and suppliers for the development of their CSMS and vehicle type. Such requirements will also be applicable to the authorised replacement part manufacturers who develop replacement parts and components. To ensure that the replacement parts and components comply with the implementation of the cybersecurity requirements of the vehicle manufacturer and their contracted suppliers, the vehicle manufacturer shall provide the relevant cybersecurity information (cybersecurity goals/specifications/requirements) to the authorised replacement part manufacturer. The absence of such a provision would mean that the part manufacturers does not have the required cybersecurity related information to develop, install and activate their products. This will lead to an unacceptable situation where the replacement parts developed by independent manufacturers does not have the required cybersecurity capabilities compared to the products developed by contracted suppliers of the vehicle manufacturers. This would further result in these aftermarket products becoming the weakest link in the cybersecurity of the whole vehicle, ultimately becoming an easy "attack interface" which can be exploited by the attackers, thereby compromising the security of the whole vehicle.

The current draft ISO/SAE 21434 standard defines Cybersecurity Interface Agreements (CIAs) for Development which are used for communicating the required cybersecurity activities across the supply chain including internal and external suppliers. Information shared through such interface agreement ensures that the required relevant cybersecurity information is exchanged across the supply chain without any intellectual property rights being violated. The respective replacement part manufacturers would need to obtain this information to ensure that the parts and components developed by them have the possibility to have the same level of security as that of the contracted suppliers. This is imperative also in the light of the block exemption principle for the IAM to develop products of comparable/equal quality with respect to cybersecurity as that of the original equipment manufacturer.

Installation/system integration requirement justification

The introduction of the cybersecurity regulation introduces regulatory requirements for the vehicle manufacturers and suppliers for the installation/production phase of the CSMS and vehicle type. Such requirements will also be applicable to the independent repairers and parts distributors who facilitate repair and maintenance operation. To ensure that the independent repairers and parts distributors have the necessary information to perform the repair and maintenance operation, it is also required that the vehicle manufacturer and their contracted suppliers provide relevant production/installation/activation related cybersecurity information to the respective parties. The absence of such a provision would mean that the independent repairers and parts distributors do not have the required cybersecurity related information to perform the repair and maintenance operation. This will lead to an unacceptable situation where the independent repairers and parts distributors do not have the possibility anymore to perform their core business activity. This would further result in threatening the very existence of these independent repairers and parts distributors and will provide the other automotive operations a monopolistic advantage in terms of repair and maintenance activities, which is also in violation of the competition law.

The current draft ISO/SAE 21434 standard defines Cybersecurity Interface Agreements (CIAs) for Production which are used for communicating the required cybersecurity activities across the supply chain including internal and external suppliers. Information shared through such interface agreement includes methods to confirm that the cybersecurity requirements for post-development like verification, validation, inspection, coding or configuration and calibration checks and related compatibility checks while performing system integration/ installation/ activation. This ensures that the required relevant cybersecurity information is exchanged across the supply chain without any intellectual property rights being violated. The respective independent repairers and parts distributors would need to obtain this information to ensure that the repair and maintenance activities still have the possibility to continue their operation in light of the new cybersecurity requirements.

Amendment to the draft Software Update Regulation

1. Scope

*Insert **new** point 1.2., to read:*

"1.2. This Regulation is without prejudice to national or regional legislation governing the installation of software updates which includes provisions for the vehicle manufacturers and the contracted suppliers to provide the independent repairers and parts distributors, the relevant specifications, requirements and necessary means for the software updates of the authenticated replacement parts and components of the vehicle type."

Justification for the amendment to software update regulation

Paragraph *1.2., **new** point:*

This point is introduced to align with the introduction of point 1.4 in the cybersecurity regulation for replacement parts and components. The respective independent repairers and parts distributors that have the capability to perform software updates for the authenticated replacement parts and components, needs to obtain relevant information from the vehicle manufacturer and their contracted suppliers. This includes information regarding interdependencies and configurations to ensure that the updates performed by the independent repairers are compatible with the systems developed by the vehicle manufacturer and their suppliers. This is important especially with the introduction of the CS regulation, that the security patches developed for the replacement parts and components must be compatible with the vehicle environment and independent repairers have the capability to perform and verify the same.