Submitted by the experts from FIGIEFA

Informal document **GRVA-06-04**
6th GRVA, 3-4 March 2020
Agenda item 4

Proposal for amendments to ECE/TRANS/WP.29/GRVA/2020/3 & GRVA-05-05-Rev.1

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 for Cybersecurity Regulation

Paragraph 1.4., amend to read:

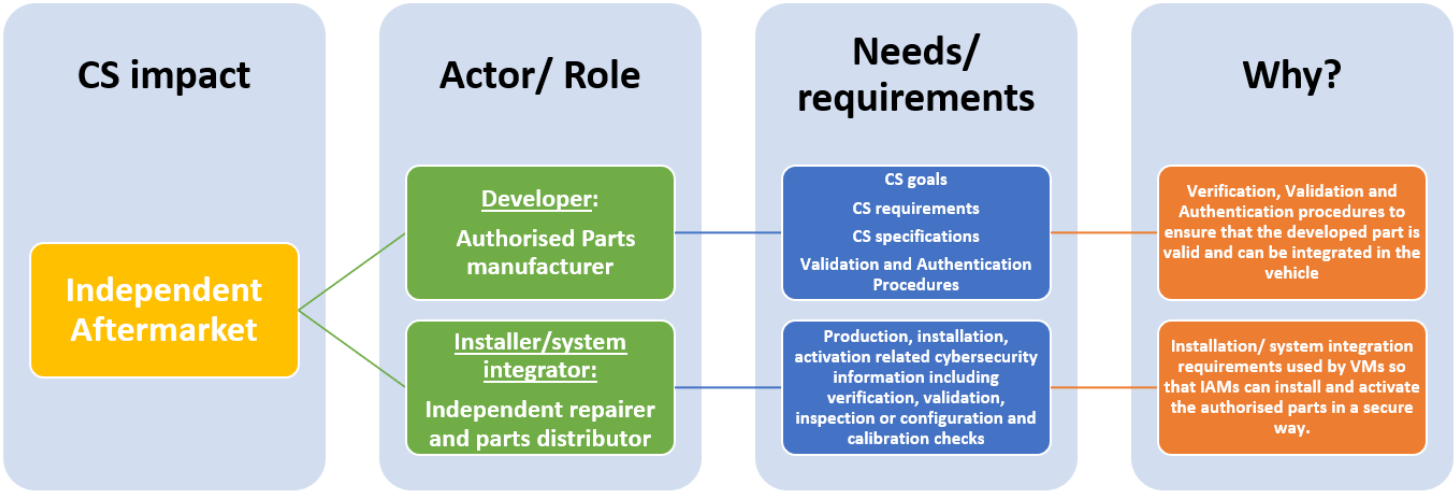
"1.4. This Regulation is without prejudice to other UN Regulations, national or regional **legislation** ~~regulations~~ ~~dealing with~~ **governing** the development and **installation/system integration of** replacement ~~of~~ parts and **components** ~~systems~~, physical and digital, with regards to ~~ensure their compatibility with~~ cybersecurity"

Amendment for Interpretation Document

Paragraph 1.4., amend to read:

"1.4. 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 amendments



Additional clarification

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. To ensure that the replacement parts and components comply with 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. Otherwise the part manufacturers do not have the required cybersecurity related information to develop, install and activate their products, leading to an unacceptable situation where the replacement parts do not have the required cybersecurity capabilities compared to the products developed by contracted suppliers of the vehicle manufacturers. The aftermarket products may then become the weakest link in the cybersecurity of the whole vehicle, an easy "attack interface" which can be exploited, 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. This ensures that 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 parts and components developed by them 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 cybersecurity regulation introduces regulatory requirements for 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, it is also required that the vehicle manufacturer and their contracted suppliers provide relevant production/installation/activation related cybersecurity information to the respective parties. Otherwise, independent repairers and parts distributors will not have the required cybersecurity related information to perform the repair and maintenance operation which is their core business activity, threatening their very existence. This 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. This 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 considering the new cybersecurity requirements.