Submitted by the expert
from Germany

Informal document **GRVA-16-26**
16th GRVA, 22-26 May 2023
Provisional agenda item 5(a)

# Comparison between UN Regulation No. 155 and the EU Cyber-Resilience Act with regard to CSS requirements on agricultural and forestry vehicles

UN-R 155 is applicable only to certain categories of vehicles. In particular, agricultural and forestry vehicles are not covered by the regulation. For these vehicle categories, the EU Cyber Resilience Act (CRA) is therefore likely to apply. The following table compares the key requirements of both regulations. For the CRA, the draft version of 15.9.22 has been used.

| | UN-R 155 | CRA |
|---|---|---|
| Products affected | Vehicles of categories M, N, partly also O, L6, L7 | Products with digital elements that have a direct or indirect data connection to a device or network. |
| Management systems required | A cyber security management system (CSMS) is required by the manufacturer that includes a.o. processes for risk assessment, secure development, and vulnerability handling. | No formal management system required. Manufacturers can have a quality system approved to ensure the conformity of affected products (Annex VI). |
| Risk assessment | Identification, assessment, and mitigation of risks during product development is required as part of the CSMS. | An assessment of cybersecurity risks must be performed and must be taken into account during the development, manufacture and maintenance of the product. The risk assessment must be included in the technical documentation (Article 10). |
| Technical safety requirements | A number of threats are listed (with reference to the vehicle and back-end systems) to be considered in the risk assessment. Corresponding abstract countermeasures are also formulated (Annex 5). Concrete technologies or algorithms are not prescribed. | Basic abstract requirements for the cybersecurity of products are defined (Annex I). Concrete technologies or algorithms are not prescribed. The technical design of the security requirements is basically the responsibility of the relevant economic operator (usually the manufacturer). In doing so, the latter can, if necessary, rely on more concrete requirements from suitable harmonized standards, common specifications or within the framework of European schemes for cybersecurity certification. |
| Testing and certification | The CSMS is tested by a technical service and certified by the approval authority. Vehicle types are also tested by technical services and approved by the authority. | Depending on the type of product and the specific design of the regulation, the relevant economic operator (usually manufacturer) can choose between different conformity assessment procedures. Basically, there is a differentiation with regard to:<br>• Conformity assessment by the manufacturer (self-declaration) with or without harmonized standard or common specification,<br>• Conformity based on a type examination by a notified conformity assessment body |

| | | |
|---|---|---|
| | | and internal production control,<br>• Conformity on the basis of a quality assurance system approved by a notified body to ensure the conformity of products concerned, and<br>• conformity on the basis of a European cybersecurity certificate.<br>Issued or withdrawn approvals or type examination certificates must be reported to a notifying authority. |
| Reporting obligations | The OEM is required to report cybersecurity activities and new cyberattacks to the approval authority or technical service at least once per year.<br>The vehicle manufacturer shall also report and confirm to the Approval Authority or the Technical Service that the cyber security mitigations implemented for their vehicle types are still effective and any additional actions taken. | The manufacturer is obliged to report exploited vulnerabilities or incidents affecting the IT security of the product to ENISA within 24 hours of becoming aware of them. Furthermore, the product users must also be informed about this. |
| Fixing vulnerabilities | Processes must be implemented at the manufacturer's site to enable the remediation of threats and vulnerabilities in the product within a reasonable timeframe. | Manufacturers must be able to correct any vulnerabilities that occur over the expected service life, but over a maximum of five years, by means of security updates. |
| Market surveillance | Not regulated in UN-R 155. Technical services check the conformity of production at least every three years. | Each member state must appoint at least one market surveillance authority. This authority can request access to the internal technical documentation of the products and carry out tests. It can specify corrective measures in the event of risks being identified. If the measures are not implemented, the market surveillance authority can ban the sale. |