Submitted by the expert of CEMA

Informal document **GRVA-15-45**
15th GRVA, 23-27 January 2023
Agenda item 5(a)

CEMA input for the evaluation of UN Regulation No. 155 and the EU Cyber-Resilience Act and the needs of the agricultural vehicle and machinery sector

CEMA represents the **European agricultural machinery industry** which comprises about 7,000 manufacturers, most of which are SMEs, producing more than 450 different types of machines with an annual turnover of about €40 billion (EU28 - 2016) and 150,000 direct employees. CEMA companies produce a large range of machines that cover any activity in the field from seeding to harvesting, as well as equipment for livestock management.

Introduction

It cannot be denied that with a more and more connected world there is a need for more product security. This is true for every aspect of the supply chain at the component and product level, but also from the design until and after production. For Agricultural vehicle/machinery becoming highly intelligent systems that can achieve field work autonomously and can communicate in autonomous mode information and task messages to the supervisor and to the implement (using TIM, Tractor-Implement Management including security features), a sufficient level of protection against cyber threats is crucial.

Agricultural vehicle/machinery sector is already included as important entities in the NIS2 (Network and Information Security). With the Cybersecurity Act, many of the ICT systems and services (cloud) that our industry is using, will be certified.

With ISO/SAE 21434 and the UN Regulation No. 155 came one of the first regulatory initiatives with detailed requirements on Cybersecurity as a perfect fit for the on-road sector.

As of 15 September 2022, a more generic legislation with cybersecurity requirements on products was published. Called the Cyber-Resilience Act, this legislation aims to make the whole manufacturing industry more resilient towards cyberattacks whilst protecting the network against harm and misuse of data.

In the following, CEMA is assessing what both files UN Regulation No. 155 and the Cyber-Resilience Act have to offer for the agricultural vehicle/machinery sector.

Our main needs as agricultural and off-road sector

Looking at the vehicle/machinery safety as outlined in EU type approval for agricultural vehicles and in the Machinery Directive (NLF) for agricultural machinery, the focus is on using suitable international

standards that are harmonized to EU legislations. Applying these standards result in performing the risk assessment for in-field, on-farm but also on-road applications. The specific standard requirements are fit for purpose, proportionate and can be adapted whenever required by our industry. These changes can be driven by new needs or general adaptation to the state of the art. **Consequently for cybersecurity, the development of a suitable standard is key for our industry.**

Producing very complex vehicle and machinery for many different applications, our sector is characterized by many platforms, many types and variants and low volumes. **Lean compliance rules with minimum cost and administration are important** to ensure proper access to the market and full deployment of the innovation potential. Any unnecessary cost can not be borne by manufacturers or small and very dedicated suppliers. due to the low volumes or wide portfolio. This is particularly true for the many SMEs in our sector. Finally, it will also negatively impact farmers and contractors, our customers.

As one of the few industrial sectors with such complex vehicles and machinery, we are very concerned with the drastic architectural changes necessary both to hardware and software, and the many interdependencies between these changes, which obliges a change-over per type, rather than gradual changes over all types in one go. To accommodate again for the many types and low volumes, a staggered approach is necessary with first focus on the high-end, higher volume types and only in a later stage the less advanced low volume types. **An adapted timeline for application of any legislation is therefore key for our sector.** As mentioned, in certain cases, market access is at risk.

Summary of main differences between UNECE R155 (R156) and the Cyber-Resilience Act (CRA) and proposal of the way forward.

Regarding **content**, despite similarities between both R155/ISO 21434 and the CRA, the CRA is less specific due to its broaden scope. CRA essential requirements will be supported by horizontal and vertical / sectorial standards providing the necessary details for the concrete implementation. As the assessment on existing standards and gap analysis by the European Commission is not done yet and the mandate for standardisation awaited, it is unclear with which type of standard the CRA will be supported. R155 is more specific and in particular on the risk management as outlined in annex V.

In terms of **scope**, the R155 is mainly addressing requirements to the manufacturer including the task of monitoring the supply chain, while in the CRA the suppliers of the components have their own responsibility. This is particularly of interest for small and medium sized enterprises, buying off-the-shell components and that have less leverage in the supply chain.

R155 is applicable to agricultural vehicle (categories R&S and T) but not to non-road mobile machinery. Its strong link with on-road safety makes it unclear to what extent it can cover specific in-field, on-farm vehicles. For the moment, in the CRA, all agricultural vehicles and machinery are in scope. The Commission has decided to exclude only those sectors subject to other EU legislations offering similar requirements. The EU type approval for agricultural vehicles covered by Regulation 167/2013 does not include cybersecurity requirements. Therefore, due to the time frame, an exclusion of agricultural vehicles in the CRA is not possible during the ongoing political negotiations. We would like to note that such exclusion must not to be completed necessarily before the CRA entry into force (expected in 2024). In the CRA, article 2 point 4 already states the criteria under which further exclusions are possible and the Commission is empowered to adopt delegated for such exclusion. It is very likely that before such exemption is granted the CRA is already applicable and implemented for our vehicles and machinery. The possible misalignment of requirements between an agricultural vehicle and an

agricultural machine, as a result of application of different legislations, is worrisome for manufacturers, most of whom are producing both.

As platform for discussing specifics of the agricultural sector, UNECE WP.29 GRVA have indicated their willingness to engage. It is however unclear how far the R155 requirements can be adapted and take adequately into account the future needs of our sector with slower pace of change than the automotive industry. The CRA on the other hand is specifically designed to cover many different industries allowing not only the development of industry specific standards, but offers flexibility in the implementation of standard revisions, and thus ensuring a good working of the internal market.

On compliance, similar to the R155, the application of the CRA requirements is risk based. But the CRA works with self-certification for products that have a core-functionality different from stated in Annex III, like agricultural vehicle/machinery. Any 'critical' product integrated as a component into a vehicle as defined in CRA Annex III, must be third party certified except if class I 'critical' products are in compliance with a harmonized standard. The R155 is fully integrated into the vehicle type approval with associated third party certification and homologation of cybersecurity features and processes in and around the vehicle.

The CRA reporting process is triggered when an active exploitable vulnerability has been identified. In comparison the reporting within the R155 is yearly and there are audits involved.

With the CRA, our sector would limit the heavy burden on critical components and beneficiate from a lean framework for the compliance of the vehicle as a whole.

Currently, **timing for implementation** remains critical for both legislations. For the reasons outlined in our roadmap at the 14th GRVA meeting, a timing beyond 2030 would be more suitable to allow a staggered introduction of the architecture changes. It would be a minimum of 4 years after the publication of the agricultural standard which is expected in April 2026. It must be reminded that it took 8 years between the initiation of the regulatory work in 2016 and the application of R155 for on-road vehicles in 2024. The start of the regulatory work for our sector started officially with the CRA in 2022.

The discussions on the CRA are just started and it is acknowledged by most of the industry sectors that the assumed implementation date of 2026 is very ambitious. Although there is a consensus for the so called critical products that such deadline is desirable, the impact on a vehicle integrating those critical products as components was never assessed. The introduction of a staggered scope to accommodate the supply chain will be up for discussion.

For the future, once decisions are made and the regulatory horizon is clear, we would like to emphasize that one single and common approach for all our vehicles and machines would be preferred. One standard adapted to the needs of our industry, reflecting the state of the art, with suitable timelines would be preferred too. The CRA does accommodate on most accounts. Given the recent discussions at the UNECE GRVA meetings, we put the question to the contracting parties if such sector specific approach can be realized as well regarding the technical details, conformity requirements and implementation dates within UNECE.

Summary

There are two initiatives on cybersecurity impacting agricultural vehicle categories T and R&S. These categories are in scope of the Cyber-Resilience Act and discussions are ongoing in the WP.29 GRVA to

decide if they should be in scope of the UN Regulation No. 155 as well. Agricultural machinery like combine harvesters or self-propelled forage harvesters, that do not belong to the categories T and R&S, are in scope of the CRA. Given that the European commission will only exclude from the CRA those sectors that have cybersecurity requirements in presently applicable EU legislation, there is little potential for such exclusion on the short term

Overall looking at our industry needs on flexibility for implementation, a lean approach for the product certification, light reporting administration, and freedom in the drafting and revising of the technical specifications in standards, the CRA seems to accommodate our industry the best at this stage. It also accommodates for all our vehicle and machinery.

Again, industry emphasizes the strong need for more lead time to make the transition in architectures on the whole portfolio, which is still a serious concern in the CRA. However, it is too soon to make any conclusions on the final consensus as a result of the political discussions which have just started.

We call upon contracting parties not to jump to any conclusions in short term until all facts and options are clear. We want to engage together within the GRVA to collect and evaluate all these facts and options to find the most suitable cybersecurity set of rules for agricultural vehicle and machinery.
