European Agricultural Machinery

CEMA

Brussels, 23/01/2023

In response to the Public Consultation on the CRA,

The Cyber-Resilience Act (CRA)
CEMA position to deliver on cybersecurity

In case the scope of the essential requirements is not clarified and, linked to that, **a more realistic timeline for non IT products** is provided, it is impossible to become compliant with the whole fleet overall, and quality of implementation will suffer. We want to deliver with proven and validated high quality adaptations, preferably following a **domain specific standard as guidance** for all companies, including the many SMEs.

Introduction

CEMA welcomes the initiative of the Cyber-Resilience Act. After a first assessment the conclusions remain that the Cyber-Resilience Act (CRA) will create a level playing field, creating a harmonised set of rules and requirements for all digital products in Europe. The CRA follows the New Legislative Framework (NLF) principles for placement on the EU market, as a horizontal legislation on cybersecurity for products, similar to the Machinery Directive for occupational safety. It gives clear responsibilities in the whole supply chain, for both OEM and suppliers, and through the principle of first placement on the EU market it clarifies these responsibilities even further, also in relation to imports. A supplier of a product with digital elements, placed on the EU market as component for integration, has to make his own assessment and put the CE marking, while the integrator is responsible for the product as a whole. When integrating outside of the EU these components, being products with digital elements themselves, the manufacturer of the final product has the full responsibility, and has to comply with the essential requirements of Annex I, when placing his product on the EU market, and for a defined period after placement on the market.

As agricultural vehicles and machinery are not products of Annex III for critical products, manufacturers can make use of self-certification. This lean approach is necessary to accommodate for the very large portfolio.

The following is presenting an insight in how the CRA affects agricultural vehicles and machinery, and which lead to CEMA's main concerns being the timeline for implementation and the missing clarity of scope.

CEMA aisbl - European Agricultural Machinery
Bluepoint, Bld A. Reyers 80, BE-1030 Brussels
T +32 (0)2 706 81 73
secretariat@cema-agri.org - www.cema-agri.org

Complete transition of vehicle/machine architecture to comply with CRA requires a staggered implementation

Being involved into Cybersecurity discussions at the level of UNECE, that involves the automotive industry, our industry has done a full assessment on what is requested, has understood its own needs, and is well positioned to evaluate the necessary vehicle/machinery changes and the timeline associated with CRA's introduction.

The CRA currently only talks of essential requirements without having identified the necessary and suitable standards neither for the critical products nor for the overall machinery industry, including the agricultural machinery/vehicles industry. The automotive sector is much more advanced on the matter with a much more worked out set of requirements. The expertise and knowledge gained should certainly be used as source to develop requirements for the industrial sectors. However, each sector has its ecosystem, its particularities and its capabilities, and needs time to adapt to new requirements, based upon proper assessment of these particularities and also its legacy. Our industry cannot be forced to take over existing standards or essential requirements from other sectors (e.g. IT) without adaptation. Such adaptations should be done with our own experts.

We would like to refer to the ongoing work within ISO TC23 (agricultural vehicles/machines) SC19 (electronics) on an ISO New Work Item Proposal initiating a new standard on cybersecurity. By mid 2026, this new standard will be applicable to our industry. It is important that such standard can be harmonised under the CRA.

The Agricultural industry Electronics Foundation (AEF – see https://www.aef-online.org/home.html), within its Expert team 'SEC' for Cybersecurity has assessed the challenges and in particular in relation to the hard-and software changes necessary to comply with the CRA.

The review of the CRA requirements revealed that it requires many different changes with different amounts of time and effort to realize.

There are some easier to implement process **updates to the existing development processes**. But it involves as well **software updates to the machine software**, which needs to be implemented across dozens of machine platforms and merged with platform update schedules. Finally, and dependent on how the scope of the CRA must be interpreted, we expect that **machine electronics hardware updates and machine network architecture updates** are necessary. The effort to realize these hardware and architecture changes is considerably higher.

Also to be mentioned is that the turnover of HW / SW architecture and platforms needs to be verified and validated within 2-3 planting and harvesting seasons.
Therefore the implementation of cybersecurity in a too short period of time would lead to a higher potential risk of being error-prone.

CEMA aisbl - European Agricultural Machinery
Bluepoint, Bld A. Reyers 80, BE-1030 Brussels
T +32 (0)2 706 81 73
secretariat@cema-agri.org - www.cema-agri.org

The size and scope of the hardware, architecture, and software changes presents a complexity of a higher order. Combined with the quality challenges for our products a longer time is required to prove-out this new technology. Due to the large portfolio of our industry, there is a need for an application of the CRA per model would take around **8-10 years** to make the entire new fleet (all new vehicles placed on the market) compliant with the requirements.

Therefore, as a minimum the **introduction of the CRA for complex products** like agricultural vehicles and machinery should be **postponed until the earliest 2030**. That would be approx. 4 years after the introduction of the domain specific standard and 6 years after the publication of the CRA. Any earlier deadline would mean a forced introduction with the associated problems of finding experts, increased costs or possible hinder the market access. We like to remind that the implementation of the Cybersecurity requirements for all new cars and trucks is in 2024, 8 years after the start of the discussions on the Regulation.

The urgency of the CRA and its ambitious implementation date, in particular on critical products and highly- critical products is understood and seems to be on request from the industry itself. However a staggered approach that first focusses on those critical products/components and then on the end product, in which they are built, in is a necessity.

Our assessment is based on the worst case, most stringent interpretation of the essential requirements. A further clarification of the requirements would be most welcome and could reduce the workload and the necessary time for implementation.

We like to raise in addition one small proposal for correction, which is that it would more clearly stated that any component, being a product with digital elements itself, for use as spare part in another product with digital elements, is not in scope, if this to-be-repaired product is placed on the market prior to the implementation date of the CRA.

Conclusions

The agricultural vehicles and machinery industry can be considered a frontrunner of the off-road and similar industrial sectors concerning cybersecurity, and had already identified the need for common cybersecurity measures for all our key enabling technologies. We fear that the CRA proposal with an application date of 24 months, and with a lack of clarity on how to interpret the essential requirements, is too short for many industrial machinery sectors. We also fear that a large part of this industry has very diverging understanding on how to implement the CRA essential requirements to their respective businesses.

Our interpretation is that the Cyber-Resilience Act allows manufacturers to develop **domain specific standards**, based on a risk assessment, just like the Machinery Directive. Though the Act does not implicitly exclude this possibility, a clarification in the text could make clear the scope of work for both experts developing horizontal and more domain specific standards.

The timeline is a more pressing issue. While it can be called ambitious for some critical products with digital elements, for highly complex vehicles, used in a versatile and high

CEMA aisbl - European Agricultural Machinery
Bluepoint, Bld A. Reyers 80, BE-1030 Brussels
T +32 (0)2 706 81 73
secretariat@cema-agri.org - www.cema-agri.org

demanding environment like in the agricultural industry, this timeline is impossible to achieve. Given

- the large number of models,
- the dependence on suppliers to provide information on their products with digital elements to be integrated into the final machine,
- the uncertainty on how to apply the essential requirements,
- the necessary quality checks to be done and
- that our domain specific standard is in draft but only to be out by 2026 expectedly,

there is a high need for a staggered approach of implementation for the huge amount of products in scope of the CRA. We call upon legislators for their support to obtain an implementation date in 2030, at the earliest, for final products.

****

ABOUT CEMA

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.

CEMA aisbl - European Agricultural Machinery
Bluepoint, Bld A. Reyers 80, BE-1030 Brussels
T +32 (0)2 706 81 73
secretariat@cema-agri.org - www.cema-agri.org