Submitted by the expert from CEMA

Informal document **GRVA-14-34**
14th GRVA, 26-28 September 2022
Provisional agenda item 5(a)

CEMA proposal for ROADMAP on CS & SUMS for Categories R, S and T

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.

With this document CEMA provides a roadmap towards the development of suitable requirements on Cybersecurity and Software update management for the agricultural machinery sector, both on content and timing for realising such requirements and the implementation. Arguments are brought forward for activating two New Work Items in standardisation and for establishing a new GRVA subgroup to assess requirements on Cybersecurity and Software Updates for agricultural vehicles.

The agricultural machinery sector: an introduction

Agricultural self-propelled and towed machinery and tractors are designed for farm and field work and will travel only occasionally on the road. The main goal of agricultural machinery producers is to deliver versatile, robust and reliable tools to work under all kinds of weather, soil and crop conditions. Due to the great built quality but also the limited resources within the sector, the average age of agricultural machinery and tractors is very high with in some countries reaching +35.
The design is often dictated by the field conditions and economic needs to perform more work per time unit with less labour and more energy efficient. In addition, for reasons of traction and reduction of soil compaction, tyres are a decisive factor in the design. As a result weight in total and per axle, and widths (up to 4.5 m are no exception for some mobile machinery) are often in need of special arrangements. Due to the design but also short distances travelled in rural areas, the maximum design speed and the speed limitation for agricultural machinery and tractors in many countries is 40 km/h. A German GDV study in 2010 found the average speed of tractors, when involved in accidents, to be 28 km/h, with main reasons of accident the high speed of other vehicles colliding into agricultural vehicles crossing a conjunction or turning left.

Tractors

The volumes of sales per type are very low, and types, variants, version are defined such to include as many vehicles as possible within one type. But even so, and looking only at tractor sales they are not comparable to the automotive sectors. Comparing tractors with heavy duty vehicles (category N):
In 2021, new HCV registrations totalled **240,346 units** (New heavy commercial vehicles 16t and over)
In 2021, new MHCV registrations totalled **289,316 units** (New medium and heavy commercial vehicles over 3.5t).
So overall you speak of a EU27 market of over **500.000** vehicles
For tractors the 2021 registrations were **170.000 units, and the volumes per type even for the best selling high-power tractors are a factor 20-30 lower than for trucks.**
The diversity of these tractor volumes is reflected in the European type approval legislation by the division over the following categories:
Category T1 : ‘normal’ tractors,
Category T2 : ‘narrow track’ tractors often used for specialty crops in very special conditions like narrow pathways, very steep fields, low overhanging plants like vineyards, orchards… These count for about 10 % of the sales often in very low volumes and produced by smaller companies with specialisation to niche products.
Category T3 : ‘small’ tractors mainly for municipal or garden use

Category T4.3 : ‘low clearance’ tractors for mountainous areas with low point of gravity due to lower ground clearance.
Category T 4.1 : ‘high clearance’ tractors, for vineyards, that are produced in very low volumes
Category T4.2 : ‘extra wide’ tractors. These are normal tractors but with the body structure exceeding 2.55 m

For Category T4.1 and T4.2 the manufacturer is not obliged to use EU type approval but can choose national approval, following national requirements.

From these categories only category T1 within the higher power classes is used for 3rd party haulage with R4 trailers.

Only category T vehicles, for safety & health related to use both **in-field and on-road**, are following requirements under EU type approval Regulation 167/2013.

Towed implements
There are two main categories being
Category R: agricultural trailers with as main distinction that the ratio between loaded and unloaded is higher than 3. There is a further categorisation in relation to weight (4 categories R1 to R4)
Category S: interchangeable towed equipment. They have dedicated functionalities to perform work in-field and have the ratio below 3. They are further categorised in relation to weight (2 categories S1 and S2 mainly in relation to the presence of brakes, with no brakes required under 3500 kg)

Overall they come in many different shapes and weights with >400 designations.
Towed implements are for safety and health essential requirements covered by the Machinery Directive, a New Legislative Framework (NLF) legislation, for safety in-field. The EU type approval legislation 167/2013 only applies for road circulation with main safety features related to braking and visibility, Many aspects are considered sufficiently covered from the Machinery Directive side, e.g. on ‘exterior projections’ in relation to possible injury of bystanders due to sharp edges.

Although it concerns more and more highly versatile intelligent systems that can operate field tasks autonomously and can communicate autonomously for information and tasks message exchange with the tractor (using TIM, Tractor-Implement Management including security features), the systems for in-field are shut down for on-road travel at higher speeds. This avoids that systems are activated by accident or technical problem, and create additional risks like e.g. bystanders getting hurt by unintentional deployment of a sprayer boom. More and more the aspect of cyber risks also play. This shut down is done by a physical switch between road and in-field use for self -propelled machinery and towed implements (from the cabin of the tractor). This is the responsibility of the operator, although often it is linked to exceeding a certain speed, as road speed is much higher than in-field speed.

Relationship tractors -towed implements for on-road travel: scenario to consider for requirements on cybersecurity and software updates.
The tractor is considered the intelligent-power hub that can deliver energy in different forms (traction, mechanical transmission, pneumatic/hydraulic pressure, electric power) for optimal performance in-field. Also on road the tractor will be the instrument for the driver to control the combination and prevent any risk of accidents.

It is expected that neither tractor nor tractor-implement combination will be travelling on public road autonomously for the coming decade, awaiting the implementation within the automotive sectors and a better understanding on the safety risks, and required safety features for agricultural machinery and vehicles. Though cybersecurity measures are beneficial for all vehicles, most recent studies focused on (semi-) automated smart cars, due to the extended ecosystem in which these smart vehicles would take autonomous decisions and autonomously communicate within the ecosystem (e.g. the ENISA study on ‘good practices for security of smart cars’ from November 2019).
It is expected that for the foreseeable future, V2V and V2X will be limited to in-field communication for agricultural vehicles. In the past, efforts were done in collaboration with ETSI to develop tractor to vehicle communication through a one M2M standard, where vehicles would be warned upfront for the presence of an agricultural vehicle entering/crossing a road. Deployment was never achieved, with no interest from the automotive side to engage.

No smart functionalities ADAS or ADS will be taken over in the foreseeable future with full control still with the driver and with currently limited electronic supporting systems (< 5 % of T1 tractors have ABS).

Given the facts above, **the scenario (scope), when considering the necessary requirements on cybersecurity and software updates under EU type approval is:**

- **for tractor and tractor-implement combination;**
- **when travelling on-road;**
- **with on-road no V2V communication, and no V2X communication with other smart systems like in relation to traffic;**
- **no assistance systems present for road circulation**
- **with the driver in control and**
- **the (smart) control systems for in-field use of the towed implements shut down.**

If for tractors this should be expanded to in-field operations, the necessary experts must be assigned.

Note: in relation to on-road accidents with agricultural vehicles, mainly tractors, for many years fatal accidents with agricultural machinery remain at about 1 % of the total EU fatal accidents. To what extent breaches and errors in relation to CS and SU will impact the risks and the accident rate, should be assessed.

The EU legislation and standards on Cybersecurity and Software Updates

In the introduction we touched upon the applicable EU legislation in relation to safety. In what follows there is an attempt to provide a more extensive overview of the existing, new and upcoming European legislation, both horizontal legislation and vertical/sectoral.

EU legislation on cybersecurity

- **Cybersecurity act**/Reg – for the first time with this Regulation are EU wide rules introduced, for the cybersecurity certification of ICT products, processes and services
- **NIS2** (Network and Information Security) is about a high common level of cybersecurity in the EU. This revision strengthens the security requirements, addresses the security of supply chains, streamlines reporting obligations, and introduces more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU. The NIS2 expected to be published autumn 2022 would include also machinery manufacturing as of mid-2024. Concerns were raised by many sectors on the possible additional administrative cost it would generate
- New Legislative Framework legislation (NLF) Radio Equipment Directive (**RED**): threat of hacked products to corrupt the internet/ hack servers. To work on suitable standards there is a CEN-CENELEC-ETSI collaboration.
- NLF: **Machinery Regulation**: linked to safety of the product and as essential security requirement being noted the ‘protection against corruption’. This includes proper design, protection and logging to ensure that for critical hardware and software, the communication with the machinery product does not lead to a hazardous situation, accidental or intentional corruption is prevented, software installed is clearly identifiable, and evidence of a legitimate or illegitimate intervention is gathered.
- NLF: **Cybersecurity Resilience Act (CRA)**: the European Commission identified that RED and Machinery Regulation might not suffice and that gaps remain. Therefore they have launched a new proposal on 15 September, introducing mandatory horizontal cybersecurity requirements for hardware and software products with digital elements. The aim is to ensure that such products are less vulnerable, and that manufacturers are responsible for the cybersecurity of a product throughout its life cycle. The majority of products falls under the default category, under which a **self-assessment is sufficient**. That include off-road machinery. Also **tractors and agricultural implements are in scope**. **The requirements are similar as UNECE Regulation 155**.
- Concerning the EU type approval for agricultural vehicles **167/2013**: there are no cybersecurity requirements yet and also in the current revision to be resumed in autumn 2022, it is not in scope. Main reason is that within the Working group of agricultural tractors (WGAT), that is chaired by the European Commission and which is attended by Member States representatives and industry stakeholders, the topic has not been discussed yet.

Standards related to cybersecurity:

- **ISO/SAE 21434:2021** Road vehicles — Cybersecurity engineering developed under **ISO/TC 22/SC 32** Electrical and electronic components and general system aspects / CEMA experts were not involved in the development
- **ISO/DIS 24089** Road vehicles — Software update engineering developed under **ISO/TC 22/SC 32** Electrical and electronic components and general system aspects / CEMA experts are not involved in the development
- **ISO 26262** part x Road vehicles – Functional safety developed under **ISO/TC 22/SC 32** Electrical and electronic components and general system aspects / CEMA experts are not involved in the development
- **ISO 25119-x** Tractors and machinery for agriculture and forestry — Safety-related parts of control systems
- **ISO/IEC 27005:2018** Information technology — Security techniques — Information security risk management developed under ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection
- **ISO 31000:2018** Risk management — Guidelines developed under ISO/TC 262 Risk management
- ETSI EN 303 645 'Cyber Security for Consumer Internet of Things: Baseline Requirements',
- Standards are expected within the collaboration CEN-CENELEC-ETSI: on the Radio Equipment Directive / Cyber Resilience Act.

Legislation and standards in relation to software updates

- In the new **Machinery Regulation** in relation to the 'Safety and reliability of control systems', there must be a tracing log of the versions of safety software uploaded after the machinery product has been placed on the market or put into service. This must be enabled for five years after such upload, exclusively to demonstrate the conformity of the machinery product with the EHSR.
- Beyond the requirements that the OEM needs to take all necessary precautions and actions to ensure that conformity is not compromised, including when updating software, the Machinery Regulation does not have any particular requirements on software updates or software update management systems.
- Regulation **167/20213** also contains requirements on repair and maintenance information. The implementation is strongly dependent on the development of generic diagnostic tools for independent operators to use OBD and make software updates. Access to OBD is possible for any new types after 07/2021. It is expected to take another 8-10 years before the entire new fleet is ready for repair and maintenance including software updates by independent operators.

Assessment of the different legislations for agricultural machinery and vehicles

Where in the past safety requirements was always in main focus (Figure 1), with connected, cooperative, automated machinery/products, additional requirements are necessary, going beyond the single machine/product performance, also on the link with other products and the network. In response to these threats, many new legal initiatives have been launched in relation to different sectors. For the biggest group, being the technological machinery industry, it concerns many new pieces of New Legislative Framework (NLF) legislation (Figure 2).

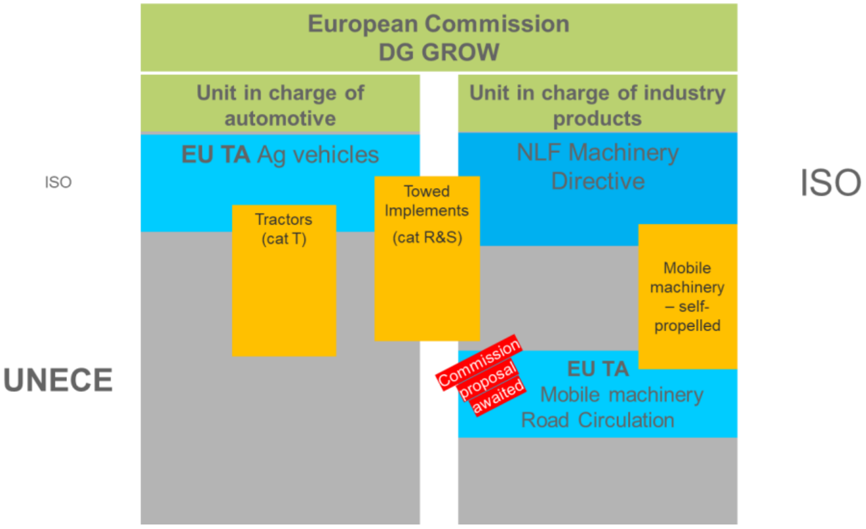
European Commission
DG GROW
Unit in charge of automotive
Unit in charge of industry products
ISO
EU TA Ag vehicles
NLF Machinery Directive
ISO
Towed Implements (cat R&S)
Tractors (cat T)
Mobile machinery – self-propelled
UNECE
Commission proposal awaited
EU TA Mobile machinery Road Circulation

Figure 1: past situation with focus on safety and health

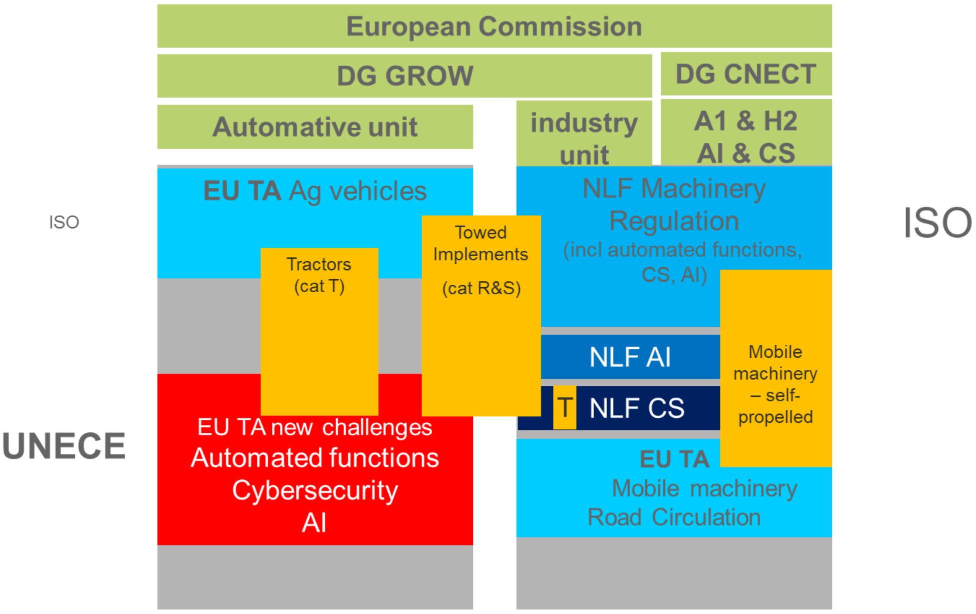

Figure 2: present-future situation taking into account connected, cooperative automated agriculture

The main benefit of using NLF legislation is that it solves the interdependencies by allowing compliance with all relevant NLF legislation following the compliance rules of only one legislation. As a result many machinery will comply with all safety AND security requirements using one Technical file, one CE label and one Declaration of Conformity under the Machinery Regulation.

Another benefit, in particular for small volume industries and SMEs is the self-certification conformity compliance which allows for a lean approach without specific templates and without many administrative and costly requirements in relation to testing by third parties and overall compliance. For all machinery, including agricultural towed machinery and self propelled mobile machinery, this ensures a good working of the internal market and in particular for the many newcomers like start-ups on agricultural robotics.

NLF legislation stands in great contrast with EU type approval, which was initially designed for the automotive sectors but also offered to tractors, being the only EU legal tool available, as a way to speed up the industrialisation and therefore food production in the EU after WW II (green revolution). It remains a rigid legal construction with requirements to be checked by a third party with preformulated templates of tests and reports, and with little regard for ‘self-declaration’, meaning that the OEM declares compliance with a signed statement.

For agricultural vehicles a limited nr of requirements are currently allowed under ‘self-declaration’ being RMI and structural integrity.
There are however large differences between the automotive vehicles and agricultural vehicles, where the former has many direct reference to UNECE regulations. The latter has not one single direct reference to a UNECE regulation but many dated references to ISO standards. The use of UNECE regulations is limited to components and in some cases installation requirements, often in separate regulations that are made fit for purpose. Examples are glazing components (adapted installation requirements are described within 167/2013 delegated act 2015/208), tyres (R106), lighting and signalling installation (R86), mechanical couplings (R147).
With the new NLF legislation, the Cyber-Resilience Act, there is an important piece of legislation, with similar requirements as UNECE R155, that can deliver on cybersecurity for agricultural machinery and vehicles, including the possibility for self-certification.

Assessment of standards in relation to agricultural vehicles and machinery: for many industries and certainty the technological industry which includes agricultural vehicles and machinery, dedicated standards on cybersecurity and software update management systems are missing. The automotive industry is one of the few that have their own standards with ISO 21434 and ISO 24089. And latter is only due for publication end of 2022. It indicates how new the topic is and in particular in relation to the description of harmonised requirements.

The lack of regulatory requirements (the CRA is just out) and suitable standards for the overall machinery industry, including the agricultural machinery/vehicles industry, shows how advanced the automotive sector is on the matter. The expertise and knowledge gained should certainly be used as source to develop requirements for the industrial sectors. However, each sector with its ecosystem, its particularities, its capabilities and its related safety and health hazards, need lead time to develop requirements, based upon proper assessment, adapted to these particularities and also its legacy. It cannot be forced to take over standards and compliance requirements from other sectors in a straightforward way. Such developments and the gain in knowledge and experience should be done within the own experts group. In particular on developing a suitable standard, the experts within ISO TC23 SC19 should be engaged. The resulting standards should be applicable to all agricultural machinery and vehicles to be referenced in NLF and EU type approval legislation, and to be used as basis within UNECE regulations.
To follow-up and assess the standardisation activities and gain knowledge, industry is proposing to setup a GRVA subgroup only dedicated to agricultural vehicles. This would allow to work with less time pressure and not disturbing the ongoing automotive work.

CEMA/AEF identified challenges for developing CS/SU requirements suitable for the agricultural machinery sector

The Agricultural industry Electronics Foundation (AEF – see https://www.aef-online.org/home.html), within its Project team ‘security’ has assessed the challenges and in particular in relation to the hard-and software changes necessary.

Roadmap with timing in relation to CyberSecurity features:
The assessment revealed that the automotive cybersecurity regulations and standards require about 3 dozen new cybersecurity features to be created and implemented. These features fall into 3 categories which require different amounts of time and effort to realize (see Figure 3).

Some of these security features involve process **updates to the existing development processes** that can be implemented in a shorter period of time, for example in **2 years**. These process updates include support such as Threat Analysis Risk Assessment (TARA), Penetration testing, and Incident Response Plans (IRP).

Some of these security features involve **software updates to the machine software**. When implemented across dozens of machine platforms and merged with platform update schedules, these software updates require a medium period of time to schedule, implement, and validate. This timing is typically **4-5 years**. These software based security features include signing application software, disabling ECU development interfaces, supporting machine certificates, creating IT infrastructures tools such as Public Key Infrastructure (PKI), updating Service Tools, and updating Manufacturing plant infrastructure.

However, the majority of the new security features require **machine electronics hardware updates and machine network architecture updates**. The effort to realize these hardware and architecture changes is much higher and the timing to execute the updates across dozens of machine platforms is much longer taking **8-10 years**, following the vehicle type change-over timeline. These hardware and architecture updates include electronics hardware redesign with security microprocessors (HSM), secure communications network updates, diagnostics authentication updates, manufacturing security updates, and advanced monitoring and reporting updates. The earlier and thus rushed implementation of cybersecurity rules would lead to a higher potential risk of being error-prone. The turnover of HW / SW architecture and platforms needs to be verified and validated within 2-3 planting and harvesting loops. That means 2-3 years for verification and validation. Our business is unfortunately depending on yearly cycles of agricultural production.

In particular due to the large number of interdependencies, there is a need for a full change-over per type, rather than quick introduction of limited, restricted security updates over all types. As a result it would take around 8-10 years to make the entire new fleet (all new vehicles placed on the market) to comply with the requirements.

There are key enabling technologies within agriculture, developed or under development within AEF. These are e.g. Tractor-implement management (TIM) that allows not only information- but also task messages to be transferred V2V, Wireless infield communication (WIC) and High Speed Interface (HSI; using ethernet type II). The AEF project team ‘security’ looks as an overarching group at all these technologies when developing the necessary security rules. These will deviate from the automotive sectors.

Further assessment must clarify whether the categories R&S need more stringent requirements on-road beyond what will be in place under the Machinery Regulation for in-field use. This includes the travel in-field but also use on field roads and on-farm use. Main question is to what extent any risks remain from transporting the electronic control systems on public roads, although these systems are shut down and not used. It is expected that the Cyber-Resilience Act will cover sufficiently the risks for R&S vehicless

Further assessment should also be done on the suitability of similar requirements including administrative reporting, testing, and audits, for all tractors. As indicated, T1 tractors of higher power classes are in main focus but for many T2-T3 tractors or low power T1 tractors, and certainly the specialised tractors T4.1, the stringency of certain requirements is questionable.

Overall the new Cyber-Resilience Act need to be assessed in relation to the regulatory implementation in the EU.

Roadmap in relation to Software Updates:
Overall the aim of the Software update Management System Regulation is clear and the process requirements logical:

- Processes for configuration control for **recording the hardware and software versions**
- Processes for **identifying** the software and hardware on a vehicle and **tracking** if that software changes
- Processes **for verifying** the software on a vehicle component is the correct one
- Processes for **identifying interdependencies** of systems with respect to software updates
- Processes for identifying target vehicles and **verifying their compatibility** with an update
- Processes to **assess if a software update will affect type approvals** or other legally defined parameters for a given target vehicle (including adding or removing functionality)
- Processes to assess to assess if an **update will affect the safety** or safe driving of a vehicle
- Processes to **inform vehicle owners of updates**
- Processes to **document all of the above**

- Processes to **ensure the cyber security of software updates before they are sent to a vehicle**

The SUMS regulation is an extension of the existing health and safety requirements, but in particular it ensures that software updates are not cause for increased risk of hazards or for the creation of new hazards.

In all three major parts, being SUM requirements, vehicle requirements and software identification requirements, the key concept is RxSWIN. This Regulation X Software Identification number represents information about the type approval relevant software of the Electronic Control System contributing to UN Regulation No. X type approval relevant characteristics of the vehicle. Although alternative systems are allowed, it is clear that there is a link with the many existing control systems on braking/steering/… but also the new ADAS and ADS functionalities that lead to specific RxSWIN like R157SWIN or R79SWIN… . As for agricultural vehicles, there are very few dedicated UNECE regulations and in particular in relation to control systems, to be linked with.

The SUMS requirements were in development parallel with ISO/DIS 24089, to be published end of 2022. As this standard is not out yet and with agricultural experts not involved in the ISO work within ISO/TC 22/SC 32, it is more difficult to make a thorough assessment at this point.

As of 2023 a dedicated AEF project team will start the assessment, similar to Cybersecurity, on the technical requirements within the ISO 24089 and the link with the SUMS, and will create a suitable, fit for purpose off-road standard, as the basis for further harmonised requirements on testing, reporting and possible audits.

Given the uncertainty on what requirements are exactly necessary and how it impacts the timeline, it would be better to start the discussions on CS, which is also a small part within SUMS, and only as of 2023 work-out the details within a roadmap for SUMS. If SUMS requirements comes first, removal of CS references must be considered.

CEMA proposal for timeline to define requirements and for the implementation

Cybersecurity

Work of AEF Project Team Cybersecurity

• Start of analysis of security regulations and standards	Mai 2022
• First outline of Cybersecurity Standard for Agricultural vehicles	Sept. 2022

CEMA and AEF

• Request for a New Work Item @ISO	29 Sept SC19 meeting
• Start of standardisation projects (NWI)	Quarter 1 2023
• Publication of ISO/CEN Standard	Quarter 1 2026
• Application within Type approval for a new type of vehicle	preference to leave it open
• Application within Type approval for any new vehicle placed on the market (all types)	2034-2036
• harmonised standard for compliance to all current relevant CS NLF legislation	the earliest 2028
• harmonised standard for compliance to the Cyber-Resilience Act	to be assessed

Software Update Management System:

The earliest 2023 a proper assessment can be done whether the timeline for CS should be followed or a more specific timeline is necessary. Depending on the assessment this timeline can be shorter or longer. However, a New Work Item will be launched on 29 September at the ISO TC23 SC19 plenary meeting.

UNECE and European union dedicated groups

Up for discussion is the **setup of a GRVA subgroup** to discuss both CS and SUMS for agricultural vehicles. Depending on the internal UNECE rules for setup, this could be for Quarter 1 2023.

The topic is already placed on the agenda of the upcoming Working Group of Agricultural Tractors (**WGAT**) meeting of 12 October. It is expected that parallel discussions will happen in this group, including on the timeline for inclusion of requirements in the EU type approval legislation 167/2013 or complete exclusion as the Cyber-Resilience Act might become the main legislation for cybersecurity on agricultural machinery and vehicles.

CEMA summary on a dedicated roadmap for agricultural vehicles

It must be iterated that the agricultural vehicles and machinery industry is not refusing or obstructing any legal action in relation to cybersecurity and software updates. On the contrary we believe that legal support is necessary and this is reflected in the EU NLF legal activities with the Cyber-Resilience Act as main piece of legislation.

Rather does the off-road industry plea for an adapted approach with requirements, technical and administratively and a timeline that suits

- the technical development and system change over of agricultural vehicles;
- the ecosystem in which these vehicles and machines are operating, being fields with hardly any bystanders, having V2V communication within the fleet of the same owner or under contract with contractors.
- the low volumes per type;
- the many types with specific needs for the in-field functionalities;
- the small percentage of time spent on-road;
- the use of mainly rural roads, and limited use of multiple lane roads and prohibition to use high-speed motorways
- the low average on-road speed
- the limited or no use of smart functionalities on-road

The requirements must be such that they can be introduced, **fit for all agricultural vehicles and machinery**, and under different homologation systems. An extra reason is that in many non-EU countries this EU distinction between vehicles and machines in agriculture does not even exist.

Just like UNECE, industry strives toward a global solution to align requirements. Compared to the automotive sectors, our industry is smaller, with a lot of variants, customizations and low production volumes. Thus, any diverging requirements in different regions, could affect the industry negatively.

We also strive toward a similar approach among off-road sectors (more alignment) i.e. agriculture, construction, material handling, garden, municipal etc. We are looking upon ways to integrate and get on-board the respective associations and industries. It is expected that with robotics, a growing segment within agriculture, the historical thin line in Europe between tractors and mobile machinery will disappear and a harmonised approach will be formed for the entire non-road mobile machinery fleet. Therefore, having a collective discussion in-depth within the non-road industry associations would make a well-founded decision.

As a result, the first step is the **development of suitable technical requirements through standardisation** (under TC23/SC19) due to the existing network of global expertise. For our industry, achieving global alignment for all our product requirements, has always been done through international standardisation. It also allows the combining of different standardisation bodies to exchange expertise. Such approach was also used within the automotive with afterwards reference in the relevant legislation, It would make it suitable for vehicles like tractors that are subject to the type approval framework for all their safety and health requirements, as well as for a wide variety of agricultural machinery, that occasionally circulate on the road and that is only subject to EU or national 'vehicle type approval' for road circulation. The occupational safety of such machines is dealt with under other pieces of legislation, like the Machinery Directive (MD – future Machinery Regulation) in the EU, which lays down only the general safety principles, while technical requirements being specified in harmonised standards (ISO/CEN) which provides higher presumption of conformity. The occupational safety and security of machinery remain the main driver for new and more stringent requirements. Within the standardisation bodies the exchange with other off-road sectors can take place.

The approach proposed to develop first the technical requirements under ISO also allows to see what cybersecurity measures the new Machinery Regulation (in trilogue) will finally bring and allows an assessment of the new Cyber-Resilience Act.

A first assessment of the AEF has revealed the set of new cybersecurity features to be developed. The list identified can be the basis for the discussions in an **ISO New Work Item**.

In relation to SUMS, the outlined principles within the R156 are logical, but further assessment must reveal the stringency and thus detail required.

Industry proposes that the standardisation process is followed up within a dedicated **GRVA subgroup for agricultural vehicles**, in presence of suitable experts, that can also start working on UNECE requirements once a solid basic standardisation text is available.