VDA German Association of the Automotive Industry

Position

Cyber Resilience Act

Content

Executive Summary 3

1 Current Situation 4

2 Challenge 4

3 Regulation of Automotive Systems and Components 4
3.1 Applicability of Regulation (EU) 2019/2144 for Suppliers 5
3.2 Risk of double-regulation for Tachograph 6
3.3 Applicable Cyber Security Regulation for Vehicle Category O 8

4 Free and Open Source Software 8

5 Intermediate Period of RE-D DA enforcement before repealing by CRA 10

6 Hybrid product GSR/CRA scope /original product/ spare part/ independent AM 11

7 Allow pentesting that this is not in conflict IP rights 12

Berlin, September 2023

Executive Summary

With the European Council's endorsement of the General Approach on July 13, 2023, and the ITRE Committee's report adoption on July 19, 2023, the co-legislators have now articulated their positions regarding the EU Commission's proposal for the Cyber Resilience Act. German automotive industry is aligned with the European Union's ambition to comprehensively enhance Europe's cyber resilience by imposing cybersecurity requirements on all products containing digital components. As we approach the interinstitutional negotiations, German automotive industry urges policymakers to uphold the principles of proportionality and practicality in these requirements. Instead of introducing overarching bureaucratic demands, the co-legislators should aim for risk-based solutions that significantly boost Europe's cyber resilience. Such an approach would not only assist vital entities in implementing the requirements outlined in the NIS 2-Directive but also allow manufacturers of digital products to focus on developing and producing cyber-resilient products rather than burdening them with administrative tasks.

The Cyber Resilience Act should establish a straightforward, cohesive, and efficient legal framework for the comprehensive regulation of cybersecurity across all covered products upon entering the market. This framework should be crafted in a manner that prevents existing, product-specific regulations from taking precedence, adhering to the "lex specialis" principle. This encompasses both current and forthcoming legislation, such as the regulation of automotive systems and components, RED Delegated Regulation and hybrid products. Streamlining the existing legal framework is essential to enable proper implementation by all stakeholders and bolster cyber resilience.

1 Current Situation

With the UN Regulation No. 155, the German and International automotive industry, has a well-defined Regulation to ensure Cybersecurity for Road Vehicles. With the international industry standard ISO/SAE 21434 Road vehicles - Cybersecurity Engineering, the automotive industry also established organizational measures and the state of the art for Cybersecurity in the engineering of road vehicles in a distributed development. Accompanied with the ISO PAS 5112 Road vehicles - Guidelines for auditing cybersecurity engineering, the automotive industry also established the baseline for ISO/SAE 21434 conformity audits along the whole supply-chain. Based on this, the automotive industry has already gained a good maturity with regards to the Cybersecurity of vehicles and its systems and components.

2 Challenge

With several new horizontal regulations in the last years, the regulatory landscape of Cybersecurity has increased tremendously. Besides the meanwhile established industry-related regulation, especially the Regulation (EU) 2019/2144, the horizontal regulations of the CRA, RE-D DA, NIS 2.0 have been published or are currently under draft. Additionally, based on the NLF approach, several hENs are under negotiation. With the approach of the Cyber Resilience Act to also push for hEN, further standardization activities will most probably start soon.

This increasingly complex situation makes it hard for the automotive industry to ensure compliance by understanding the different scope statements, interrelationships and interdependencies between the regulations and hENs in the right way. Additionally, a general lack of cybersecurity experts in the European job market is compounding this situation.

Therefore, the Automotive industry strongly recommends limiting the complexity of Cybersecurity-related regulation approaches effecting automotive vehicles, systems and components to the minimum.

This position will highlight points where the current regulation needs more clarity and should be streamlined to ensure harmonized regulations for the entire automotive industry.

3 Regulation of Automotive Systems and Components

The automotive industry appreciates the Cyber Resilience Act’s recognition of the Regulation (EU) 2019/2144 as an an established regulation for protection of vehicles of the categories M and N against cyberattacks and the exclusion of respective vehicles from its scope. Vehicles are much more complex than smaller products with digital elements directly sold to an end-customer. The vehicle manufacturers face strong cybersecurity requirements from the UN Regulation No. 155 with its European Implementation in Regulation (EU) 2019/2144 and the international standard ISO/SAE 21434. However, the automotive industry has a deep and complex supply-chain, but by today component providers are not directly subject to the requirements under Regulation (EU) 2019/2144. It is therefore essential that the cybersecurity requirements for systems and components are set in such a way, that it is easier for automobile manufacturers to comply with Regulation (EU) 2019/2144.

3.1 Applicability of Regulation (EU) 2019/2144 for Suppliers

The Regulation (EU) 2019/2144 is ensuring a high level of cybersecurity for such vehicles overall. As part of the vehicle type-approval the vehicle manufacturer has also to demonstrate how the supply-chain was managed and how the supplier components are part of the overall cybersecurity architecture of the vehicle. The consideration of the potential threats and mitigations, listed in the Annex 5 of the UN Regulation No. 155 provides the requirements to ensure a high level of cybersecurity for systems and components of a vehicle type.

In combination with the industry standard ISO/SAE 21434, the automotive industry also defined a high state of the art for the design, development and production of automotive systems and components in a distributed environment. However, even though the vehicle manufacturers are subject to strict cybersecurity requirements and the automotive industry has a deep and complex supply-chain, by today, system and component providers are not directly subject to the cybersecurity requirements under Regulation (EU) 2019/2144. Developing, producing and maintaining components according to ISO 21434 is legally not mandatory, but suppliers are committed to prove their compliance to ISO/SAE 21434 towards the manufacturers through certification according to this standard to support the cybersecurity activities of the manufacturers.

The Commission recognizes this in the Impact Assessment Report and states that such products and systems should be subject to the Cyber Resilience Act. The commission highlights that “Therefore, it will be easier for vehicle manufacturers to manage their dependencies, as the components would carry the CE marking probing compliance with cyber-security requirements.“

As a preferred solution, the automotive industry considers it preferable to cover all members of the value chain in a single regulation. Therefore, those suppliers of systems and components that can demonstrate that they have implemented and comply with Regulation (EU) 2019/2144 and thus have a certified cybersecurity management system (CSMS) in place in accordance with the applicable UN Regulation No. 155 on technical specifications and cybersecurity measures and processes for their systems and components are not subject to the Cyber Resilience Act.

Therefore, this solution, together with the clarification from the Impact Assessment of the Commission shall be amended for the Cyber Resilience Act.

To make this clear, we are proposing the following amendments:

ITRE Proposal, General Approach (EC)

Amendment to Recitals (13)
Regulation (EU) 2019/2144 of the European Parliament and of the Council establishes requirements for the type-approval of vehicles, and of their systems and components, introducing certain cybersecurity requirements, including on the operation of a certified cybersecurity management system, on software updates, covering organisations policies and processes for cyber risks related to the entire lifecycle of vehicles, equipment and services in compliance with the applicable United Nations regulations on technical specifications and cybersecurity, and providing for specific conformity assessment procedures. In the area of aviation, the principal objective of Regulation (EU) 2018/1139 of the European Parliament and of the Council is to establish and maintain a high uniform level of civil aviation safety in the Union. It creates a framework for essential requirements for airworthiness for aeronautical products, parts, equipment, including software that take into account obligations to protect against information security threats. Products with digital elements to which Regulation (EU) 2019/2144 applies and those products certified in accordance with Regulation (EU) 2018/1139 are therefore not subject to the essential requirements and conformity assessment procedures set out in this Regulation. The certification process under Regulation (EU) 2018/1139 ensures the level of assurance aimed for by this Regulation.

Systems and components provided by suppliers who can prove that they have implemented and follow the Regulation (EU) 2019/2144 and therefore implemented a certified cybersecurity management system (CSMS) in compliance with the applicable UN Regulation No.155 on technical specifications and cybersecurity measures and processes for their systems and components in accordance to ISO/SAE 21434 are not subject of this Regulation. Otherwise, systems, components and separate technical units designed and constructed to vehicles that are regulated by Regulation (EU) 2019/2144 and the manufacturer does not have a certified CSMS would be subject to the requirements of this Regulation.

Therefore, it will be easier for vehicle manufacturers to manage their dependencies, as the components would carry the CE marking probing compliance with cyber-security requirements.

3.2 Risk of double-regulation for Tachograph

Besides the systems and components mentioned in Recital 13 of this Regulation there are systems that are regulated by other regulations that are partly also giving requirements on the Cybersecurity of these systems. This is especially true for tachographs. By not excluding them from the scope of the Cyber Resilience Act, those products would be regulated by two different regulations.

The tachographs are regulated by Regulation (EU) 165/2014. The implementation of the requirements of EU 165/2014 and the technical definition of the recording equipment (tachograph) are defined in EU 2016/799 (Annex I C). Components which are type approved according to Annex I C are fully compliant with Common Criteria specifications, as defined in Appendix 10 of Annex I C.

The type approval of the vehicle is defined by EU 2018/858 and is implemented according to EU 2020/683. The Implementing Regulation EU 2020/683 refers to tachograph in Annex I point 4.9. There is no distinct requirement in this Annex I point 4.9. that a vehicle type approval can only be achieved with a type approved tachograph. This understanding is shared by various authorities. The Regulation EU 2018/858 is amended by Regulation EU 2019/2144 in regard to protection of vehicle against cyberattacks, by referring to the UN Regulation No 155.

According to the scope of UN Regulation No 155 point 1.4. this regulation excludes '… national or regional legislation governing the development and installation/system integration of replacement parts and components, physical and digital, with regards to cybersecurity'. With the EU wide Regulation EU 165/2014, UN Regulation No 155 is not applicable for tachograph / recording equipment.

ITRE Proposal, General Approach (EC)

Amendment to Recitals (13)
Regulation (EU) 2019/2144 of the European Parliament and of the Council establishes requirements for the type-approval of vehicles, and of their systems and components, introducing certain cybersecurity requirements, including on the operation of a certified cybersecurity management system, on software updates, covering organisations policies and processes for cyber risks related to the entire lifecycle of vehicles, equipment and services in compliance with the applicable United Nations regulations on technical specifications and cybersecurity, and providing for specific conformity assessment procedures. Additionally, the Regulation (EU) 165/2014 establishes requirements on tachographs in road transportation.

In the area of aviation, the principal objective of Regulation (EU) 2018/1139 of the European Parliament and of the Council is to establish and maintain a high uniform level of civil aviation safety in the Union. It creates a framework for essential requirements for airworthiness for aeronautical products, parts, equipment, including software that take into account obligations to protect against information security threats.

Products with digital elements to which Regulations (EU) 2019/2144 and (EU) 165/2014 applies are therefore not subject to the essential requirements and conformity assessment procedures set out in this Regulation. Products certified in accordance with Regulation (EU) 2018/1139 are therefore not subject to the essential requirements and conformity assessment procedures set out in this Regulation. The certification process under Regulation (EU) 2018/1139 ensures the level of assurance aimed for by this Regulation.

Amendment to Article 2 – Scope, 2.
This Regulation does not apply to products with digital elements to which the following Union acts apply:
(a) Regulation (EU) 2017/745;
(b) Regulation (EU) 2017/746;
(c) Regulation (EU) 2019/2144;
(d) Regulation (EU) 165/2014;

3.3 Applicable Cyber Security Regulation for Vehicle Category O

Even though the UN Regulation No. 155 and the Regulation (EU) 2019/2144 both have the vehicle category O mentioned in the scope, Regulation (EU) 2019/2144 does not bring the vehicle category O into the scope of this Regulation clearly. The Annex II of this Regulation lacks a reference regarding category O to make a “D4 Protection of vehicle against cyber-attacks” applicable to this vehicle category.

Consequently, the vehicle category O is not regulated by Regulation (EU) 2019/2144 in terms of Cyber Security and could therefore possibly fall within the scope of the Cyber Resilience Act.

To overcome this unclear situation, the Regulation (EU) 2019/2144 should also apply "D4 Protection of the vehicle against cyberattacks" to vehicle category O.

The related transition period has to be defined in a way to enable the European Trailer Industry to establish a Cyber Security Management System (CSMS) according to the UN Regulation No. 155.

Therefore, transition periods should be given that require a date for refusal to grant EU type-approval not earlier than 7 January 2026. The date for the prohibition of the registration of vehicles, as well as the placing on the market and entry into service of components and separate technical units should be not before 7 January 2029.

Like for vehicle categories M and N, it shall be avoided that vehicle category O becomes regulated by CRA in a first step and by Regulation (EU) 2019/2144 in a later step.

Therefore, we are proposing to clearly exclude vehicle category O from CRA if vehicle category O is regulated by Regulation (EU) 2019/2144 in the future as proposed above.

4 Free and Open Source Software

Cybersecurity obligations, like other compliance obligations, must remain with the companies that place FOSS on the market and use it commercially (downstream), not with the developers who make FOSS available for free in the form of source code (upstream), regardless of whether the developer is employed by a commercial company or not.

The German automotive industry already uses free and open source software (FOSS) today and plans to use it in cooperation with organizations such as the Eclipse Foundation, COVESA, or the EU SDV Initiative, in order to further drive standardization in the automotive industry and make the European automotive sector future-ready. The automotive industry uses FOSS, i.e. software that is freely available and which anyone can modify and distribute. The deployment of FOSS has become key element in our industry owing to its numerous advantages such as cost-efficiency, flexibility, transparency and collaboration. To date it has always been well understood that the economic operator who uses open source in an automobile was responsible for ensuring its cybersecurity, functional safety, and compliance with the relevant standards. Our industry sees the cost of shifting that burden to FOSS developers and nonprofits as unnecessary, counter-productive, and counter to established industry best practices. As outlined below the current CRA approach will harm the competitiveness of the German automotive industry.

In the automotive sector FOSS enables OEMs and suppliers to utilize existing software solutions, adapt them to their specific requirements, and share improvements with the community. This collaborative approach fosters innovation, accelerates the development cycles and promotes standardization across the entire sector.

The efficient cooperation by means of FOSS is crucial to the competitiveness of the German and European automotive industries. A short paper by the Expert Group on the Transformation of the Automotive Industry emphasizes the advantages and was distributed in the German Federal Ministry for Economic Affairs and Climate Action on June 14, 2023.

The European Commission plans to introduce the EU Cyber Resilience Act (CRA) in order to improve the general requirements and standards applicable to the cybersecurity of software and other digital products. The German Association of the Automotive Industry (VDA) supports this objective but perceives a danger that the FOSS community could be harmed permanently and that this could negatively impact the European economy. The FOSS community consists of a large number of developers, non-profit foundations and enterprises which cooperate on a voluntary basis. Together they develop FOSS code, which is made publicly available free of charge, and helps generate innovation in the European automotive industry.

If individual developers, projects and FOSS organizations are held responsible for fulfilling the obligations envisaged in the CRA, there is a risk that FOSS development and access to FOSS for the European market will be restricted.

Instead, more FOSS products might be marketed in countries with either low-level cybersecurity requirements or none at all. This means that Europe would close itself to the successful collaboration between the FOSS community and the industry, which contributes to the development of secure FOSS products. On the other hand, clarifying that CRA compliance is the responsibility of the companies commercializing open source code could lead to proven procedures from the collaborations between the FOSS community and the industry is transferred to the FOSS community and thus to the establishment of high security standards for major FOSS projects worldwide.

We therefore propose a necessary differentiation between the collaborative development of FOSS (upstream) and its commercial use (downstream).

Amendment to Recitals (13)
We therefore propose a necessary differentiation between the collaborative development of FOSS (upstream) and its commercial use (downstream).

- The CRA should accordingly not be applied to the collaborative development of FOSS, irrespective of the business activities of the stakeholders (upstream).
- The regulation should apply only when FOSS is used in products and services (downstream).
- The cybersecurity obligations should apply to the companies that bring FOSS to market and use it commercially, and not to the developers who make the FOSS source code available free of charge.

As a result, for FOSS that is developed in foundations like the Eclipse Foundation, the Linux Foundation and COVESA, the obligations apply to the companies that use them commercially – not to the foundations where the components were developed collaboratively.

5 Intermediate Period of RE-D DA enforcement before repealing by CRA

The incumbent COM (2022)/454 CRA draft proposals speak of the intention to repeal the 2022/30 RE-D DA once the COM (2022)/454 CRA is enforced suggesting a similar scope of applicability between COM (2022)/454 CRA (Article 55 (3a) ITRE final compromise) and 2022/30 RE-D DA in the intention to prevent double regulation.

COM (2022)/454 CRA excludes products with digital elements regulated by the 2019/2144 GSR from its scope while the 2022/30 RE-D DA excludes "...radio equipment, products or components..." to which 2019/2144 (GSR) would apply from its scope (CONTEXT OF THE DELEGATED ACT).

According to the VDA interpretation, when falling in scope of 2019/2144 the Delegated Regulation 2022/30 (RE-D DA) does not have to be followed once the CRA is enforced.

If the commission concurs with this VDA interpretation, the implementation of 2022/30 RE-D DA for internet connected radio equipment which is regulated by 2019/2144 GSR should be suspended immediately in order to avoid unnecessary effort and double regulation caused by an intermediate period of RE-D DA enforcement, until the CRA enters into force and repeals RE-D DA 2022/30.

The unnecessary effort caused by the transition period mentioned above between RE-D DA 2022/30 and COM (2022)/454 CRA can be characterized as below:

As the exact entry into force (EIF) of the COM (2022)/454 CRA is not finally confirmed (current estimate 05/2024) and the 2022/30 RE-D DA is already in force the industry is in a vacuum where one regulation is bound to expire and whilst its expiry its applicability is still impaired by unavailability of harmonized standards (hEN) - potentially forcing manufacturers into resource intensive involvement of notified bodies for conformity assessments.

This problem would also prevail in case of pro-active observance of the CRA (in lieu of the RE-D DA) before its official application date ((Article 55 (3a) ITRE final compromise) as standardization efforts for the CRA have not officially started yet.As a potential remedy in this situation the CRA proposals list common specifications as a "...fall back solution..." (Recital (41) – ITRE final compromise) or surrogate to harmonized standards. This remedy option would also be accessible within the scope of the 2022/30 RE-D-DA but applying this instrument would unnecessarily waste resources of cyber security expertise which is already stretched thin.

Thus, suspending the 2022/30 RE-D-DA immediately and focusing all standardization efforts on the hEN for the COM 2022/454 CRA should be the goal.

Change Proposal (COM (2022)/454 CRA (Article 55 (3a) ITRE final compromise))
…
The commission shall repeal the Delegated Regulation 2022/30 (RED-DA) (and its implementation) towards Cyber Security of systems and components, including Radio Equipment Devices, which are subject to the requirements of this Regulation (COM 2022/454 CRA)
…

6 Hybrid product GSR/CRA scope /original product/ spare part/ independent AM

The automotive industry appreciates the intention of the regulators to promote sustainability by keeping products operational within their expected lifetime (COM (2022)/454 CRA Article 2, 4a, Recital 14a - ITRE final compromise).

In order to facilitate this the supply of parts for repair and maintenance is imperative. Unfortunately, the current COM (2022)/454 CRA proposals unnecessarily limit the definition of what exactly constitutes a ("spare part") and under which pre-requisites they may be excluded from the scope of the COM (2022)/454 CRA.

The following example is intended to demonstrate the lack of definition with regards to scoping and interplay of the 2019/2144 (GSR) and COM (2022)/454 CRA:

In practicality many systems and components (parts) which are predominantly integrated into automotive vehicles (vehicle categories M, N, O according to regulation 2018/858) are also integrated into non-automotive vehicles and thus could be characterized as "hybrid parts".

While according to VDA interpretation the first class of systems, component qualifying as products with digital elements is also falling in scope of the sectoral regulation 2019/2144 (GSR) and thus are excluded from the COM (2022)/454 CRA Article 2, 2c - ITRE final compromise) the latter class of systems and components would fall in scope of COM (2022)/454 CRA creating unclarity of precedence and burden of double regulation for the system / component manufacturer.

Another precedence question arises when COM (2022)/454 CRA (COM (2022)/454 CRA Article 2, 4b - ITRE final compromise) is considered stating the primacy of the sectoral rule in case of equal or higher degree of protection which suggests that a product (including systems/components) which is falling in scope of sectoral regulation 2019/2144 GSR is excluded from COM (2022)/454 CRA - the supporting argument being that a high degree of cybersecurity protection is offered by virtue of recognizing the equivalence of UNECE R155 (Cyber Security Management System) by 2019/2144 GSR.

In addition to "hybrid parts" numerous "aftermarket" parts/components integrated into automotive vehicles but being seen as non-automotive and already subject to vigorous cybersecurity regulation (e.g. 165/2014 Tachograph) are unnecessarily brought into scope of COM (2022)/454 CRA with no gain with regards to cyber security.

In addition to the unclear scoping of COM (2022)/454 CRA the restriction of spare part usage to systems/component produced by the original manufacturer and being exclusively produced for usage as spare part defies industry practice supplying these parts our of current production or warehouse stock (COM (2022)/454 CRA Article 2, 4a, Recital 14a – ITRE final compromise).

The impact of the of the above unclarities and restriction threatens to weaken part supply-chain and sustainability.

Hence the automotive industry recommends to leave “aftermarket” parts/components in their established regulatory schemes and to assign “hybrid” parts to the scope of the sectoral regulation where they are predominantly used - in case of automotive usage 2019/2144 GSR.

Change Proposal (COM (2022)/454 CRA Article 2, Recital 14 - ITRE final compromise)
Recital (14a) shall be deleted entirely.
Article 2, 4a.
This Regulation does not apply to spare parts, or any other systems or component having established vertical regulation at entry into force of this regulation (COM (2022)/454 CRA) and being intended to complete, repair or maintain a product at higher integration level and that are supplied by the manufacturer of the original products with digital elements.

7 Allow pentesting that this is not in conflict IP rights

The “IT-Grundschutz-Compendium of the German Federal Office for Information Security stipulates that penetration tests should be carried out for applications and IT systems with an increased need for protection.[1] UNECE R 155 requires vehicle manufacturers to establish a cyber security management system (CSMS). According to the German Federal Motor Transport Authority (KBA), penetration tests are "one of the standard tools in the field of cyber security testing.”[2] At the same time, there are countless criminal laws in Germany alone that can be relevant to hacking - and thus also to penetration testing. These include §§ 202 a, 202 b, 202 c, 263 a, 303 a, 303 b German Criminal Code, §§ 23, 3, 4 German Trade Secret Act or §§ 106, 69 c German Copyright Act.

Even though recital 17 of directive 2013/40/EU contains exceptions to criminal liability in certain circumstances (which have not been neatly implemented in German law) and there is currently discussion as to whether decompiling software to search for security vulnerabilities is covered by Art. 6 (1) of Council Directive 91/250/EEC, the legal situation regarding penetration tests is still uncertain and the justification must be examined in each individual case. There is a risk of criminal law, especially for smaller companies without corresponding legal departments. The Chaos Computer Club has examined the effects of the so-called "hacker paragraphs".[3] Companies refrain from testing due to the risk of criminal law, which inevitably leads to a lowering of the security level.

Change Proposal
We therefore ask the EU legislator to create the legal framework for risk-free penetration testing by introducing provisions in the Cyber Resilience Act explicitly allowing penetration testing of products with digital elements by the lawful acquirer of the respective product.

Contact Persons

Dr. Marcus Bollig
Managing Director
marcus.bollig@vda.de

Martin Lorenz
Head of department technologies & eco-systems
martin.lorenz@vda.de

The German Association of the Automotive Industry (VDA) consolidates more than 650 manufacturers and suppliers under one roof. The members develop and produce cars and trucks, software, trailers, superstructures, buses, parts and accessories as well as new mobility offers.

We represent the interests of the automotive industry and stand for modern, future-oriented multimodal mobility on the way to climate neutrality. The VDA represents the interests of its members in politics, the media, and social groups. We work for electric mobility, climate-neutral drives, the implementation of climate targets, securing raw materials, digitization and networking as well as German engineering.

We are committed to a competitive business and innovation location. Our industry ensures prosperity in Germany: More than 780,000 people are directly employed in the German automotive industry. The VDA is the organizer of the largest international mobility platform IAA MOBILITY and of IAA TRANSPORTATION, the world's most important platform for the future of the commercial vehicle industry.

If you notice any errors, omissions or ambiguities in these recommendations, please contact VDA without delay so that these errors can be rectified.

Publisher	German Association of the Automotive Industry Behrenstraße 35, 10117 Berlin www.vda.de/en Registered representative R001243 EU Transparency No. 95574664768-90
Copyright	German Association of the Automotive Industry Reprinting and all other forms of duplication are only permitted with indication of the source.
Version	Version 1.0, September 2023