EUROMOT

FAQ
CYBER RESILIENCE ACT

JUNE 2024

Regulation (EU) 2024/**** of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements, amending Regulations (EU) 168/2013 and (EU) 2019/1020 and Directive 2020/1828/EC (Cyber Resilience Act).

DISCLAIMER

This document reflects the view of EUROMOT, with regards to the legal provisions of the Regulation (EU) 2024/**** of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements, amending Regulations (EU) 168/2013 and (EU) 2019/1020 and Directive 2020/1828/EC (Cyber Resilience Act) and it must not be considered or intended as a legally binding text for any reason whatsoever.

This FAQ must be intended as a living document; its content could be modified or updated by EUROMOT, based on updates of the legislation, and according to its understanding on the matter.

EUROMOT accepts no responsibility for the recommendations, advice, statements and conclusions expressed or implied in this FAQ and give no warranty, representation or assurance with respect to the accuracy or validity of the same. Only the text of the Regulation is authentic in law.

Accordingly, in case of discrepancies between the content and interpretation of this FAQ and the text of the legislation (2024/****)[1], the legislation must be applied.

CONTACT

EUROMOT aisbl
The European Association of Internal Combustion
Engine and Alternative Powertrain Manufacturers
Rue Joseph Stevens 7
1000 Brussels
Belgium
Email: secretariat@euromot.eu
Web: www.euromot.eu

TABLE OF CONTENT

1 INTRODUCTION

The impact of cyber-attacks through digital products has increased dramatically in recent years. The 'cyber resilience act' (CRA) therefore aims to impose cybersecurity obligations on all products with digital elements whose intended and foreseeable use includes direct or indirect data connection to a device or network. The proposal introduces cybersecurity by design and by default principles and imposes a duty of care for the lifecycle of products.

The CRA aims to harmonise cybersecurity rules for the placing on the market of products with digital elements. The CRA has two main objectives for digital products (i.e. hardware and software), and its aim is to create the conditions for the development of secure digital products, by ensuring that hardware and software products are placed on the market with fewer vulnerabilities. It also aims to oblige manufacturers to take security seriously throughout products' lifecycles, and to encourage users to take cybersecurity into account when selecting and using products.

As the first ever EU-wide legislation of its kind, the proposed EU cyber-resilience act seeks to bolster the cybersecurity of products with digital elements (digital products) in the European Union and to address existing regulatory cybersecurity gaps. Devices with digital elements that fail to meet the requirements of the CRA would be banned from the EU market. As the CRA would also target digital products from non-EU vendors when marketed in the EU, it might have a potential impact on the cybersecurity standards for such products beyond EU borders.

The purpose of this frequently asked questions document (hereinafter 'FAQ') is to contribute to a clear understanding of the Regulation (EU) 2024/****[1]. It is intended to provide answers to key questions that are likely to be asked by engine manufacturers.

Delegated Regulation (EU) 2024/***[1] applies to the engine manufacturer. Throughout this FAQ "manufacturer" means engine manufacturer.

ABOUT EUROMOT

EUROMOT, the European Association of Internal Combustion Engine and Alternative Powertrain Manufacturers, represents the key manufacturers of internal combustion engines and alternative powertrains installed in industrial non-road mobile machinery, marine and stationary applications that are operating in Europe and worldwide.

Founded in 1991, we provide an unparalleled heritage and hub of expertise for businesses, authorities, regulators, and public stakeholders worldwide. In partnership with major sector associations and institutions, it is our mission to drive smart regulation and sustainable innovation.

2 TIMELINE, APPLICATION AND SCOPE

2.1 What is the timeline for the implementation of the Cyber Resilience Act (CRA)? And when is the application date for manufacturers, i.e. the end of the transition period?

Industry and governments will have three years (36 months) to adapt to the new requirements, which will start applying in late 2027 (Article 71). The standards for Annex I.1 of the CRA are expected to be finalised by mid-2025 and the standards for Annex I.2 are expected for mid-2026.

Article 14 on reporting obligations applies 21 months after the entry into force of this Regulation and Chapter IV (Articles 35 to 51) shall apply from 18 months after entry into force of the Regulation.

Article 69.1 provides an additional 6 months for the transitional period when products have type-examination and approval decisions under a union legislation that contains cybersecurity requirements. Example of union legislation that contains cybersecurity requirements: RED DA 2022/30, MR 2023/1230. Module B is providing a type-examination and approval decisions. According to Article 69.1, "EU type-examination certificates and approval decisions issued regarding cybersecurity requirements for products with digital elements that are subject to other Union harmonisation legislation shall remain valid until ... [42 months from the date of entry into force of this Regulation], unless they expire before that date, or unless otherwise specified in such other Union harmonization legislation, in which case they shall remain valid as referred to in that Union legislation."

Reference: Art. 71 (Entry into force and application); Art.69.1 (Transitional provisions) of the CRA.

2.2 Will the CRA apply to products which are already being produced and for which a full redesign will be necessary to comply with the legislation?

The CRA applies as to when the product is placed on the market. As for 'making available', the concept of 'placing on the market' refers to each and individual product, not to a type of product, and whether it was manufactured as an individual unit or in series. When a manufacturer or an importer supplies a product to a distributor or an end user for the first time, the operation is always labelled in legal terms as 'as placing on the market'. Any subsequent operation, for instance, from a distributor to distributor or from a distributor to an end-user is defined as 'making available'. (Blue guide 2023 clause 2.3). Any machine delivered to a distributor or end user in Europe after the deadline date, estimated Sept 2027, must comply to the new regulation. This means that older design machines cannot be sold in EU after the deadline date if the machine does not comply with CRA. (interpretation from blue guide – 2023 clause 2.3).

Industry and governments will have three years to adapt to the new requirements, which will start applying around Sep 2027 tentatively (CRA - Article 71). As stated in Article 69 of CRA, "products with digital elements that have been placed on the market before ... [date of application of this Regulation], shall be subject to requirements of this Regulation only if, from that date, those products are subject to substantial modifications".

Reference: Art. 13 (Obligations of manufacturers); Art. 14 (Reporting obligations of manufacturers); Art. 19 (Obligations of Importers); Art.691 (Transitional provisions) of the CRA; Blue guide 2023 clause 2.3.

2.3 Are engines in scope of the product Class I or II found in Annex III of the CRA outlining critical products with digital elements?

Engines are not in scope of the products in Class I or II of Annex III, unless manufacturers put the product on the market as one of the components listed in class I or II of Annex III. Therefore, engines only have to fulfil the essential requirements of the CRA.

If manufacturers integrate components into their devices which are part of Class I or II of Annex III, then manufacturers need to make sure that their suppliers have complied with Class I or II requirements.

If manufacturers buy components from outside the EU which are part of Class I or II, then manufacturers can request that suppliers provide a Declaration of Conformity (DoC) and CE marking for the component. However, as there is no legal obligation for suppliers, manufacturers should ensure that this is part of their contractual agreement with suppliers. If there is no DoC and/or CE making for the imported component, then manufacturers need to keep in mind that they will be held responsible for the component.

Reference: EUROMOT meeting with the European Commission from 5. September 2023; Annex III (IMPORTANT PRODUCTS WITH DIGITAL ELEMENTS), Class I & II; Art. 14 (Reporting obligations for manufacturers); Art. 19 (Obligations for Importers); Art. 22 (Other cases in which obligations of manufacturers apply) of the CRA.

2.4 If the engine does not have an Engine Control Model (ECM) on it (e.g. mechanically governed) will this fall under the scope of the CRA if the final product has a digital element in it?

To be part of the scope of the CRA, a product has to have both a digital element in it and "a direct or indirect logical or physical data connection to a device or network" (Article 2). This Regulation applies to products with digital elements made available on the market, whose intended purpose or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network. Therefore, if an engine has a "direct or indirect logical or physical data connection to a device or network" but does not have a digital element in it, then it does not fall under the scope of the CRA. Manufacturers need to verify whether the final product has a digital element in it or not. However, if the final product does have a digital element in it, then the end-product has to meet the essential requirements of the CRA.

Reference: Art. 2 (Scope) of the CRA.

2.5 Are Internal networks, hardware and software components of the engine under the scope of the risk assessment for the CRA?

Based on Article 2, “direct or indirect logical or physical data connection to a device or network”, all hardware / software components and networks of a product fall under the scope of the CRA and therefore, all essential requirements would apply.

Reference: Art.3 (Definitions) of the CRA.

2.6 Is a replacement engine (as spare part or remanufacturing part) in scope of the CRA?

This regulation does not apply to spare parts made available in the market to replace identical component in products with digital elements and that are manufactured according to the same specifications as the components that they are intended to replace. (Article 2.6)

If going to be a brand new or a custom-made part for a new machine, then it will fall under the CRA when placed on the market. A replacement engine is to replace a component or engine on an existing machine which is already placed on the market is out of scope of the CRA. Re-certification of legacy engines is not needed (Recital 29).

Art. 2.6: “This Regulation does not apply to spare parts that are made available on the market to replace identical components in products with digital elements and that are manufactured according to the same specifications as the components that they are intended to replace”.

Recital 29: “In order to ensure that products with digital elements made available on the market can be repaired effectively and their durability extended, an exemption should be provided for spare parts. That exemption should cover both spare parts that have the purpose of repairing legacy products made available before the date of application of this Regulation and spare parts that have already undergone a conformity assessment procedure pursuant to this Regulation”.

Reference: Art. 2.6 (Scope) and Recital 29 of the CRA.

2.7 When manufacturers conduct a field modification upgrade of machinery (i.e. upgrade kit for engine, controller) does it fall under the scope of the CRA and its obligations?

According to the Blue guide definition of Substantial Modification: “A product, which has been subject to important changes or overhaul after it has been put into service must be considered as a new product if: i) its original performance, purpose or type is modified, without this being foreseen in the initial risk assessment; ii) the nature of the hazard has changed or the level of risk has increased in relation to the relevant Union harmonisation legislation; and iii) the product is made available (or put into service if the applicable legislation also covers putting into service within its scope).

This has to be assessed on a case-by-case basis and, in particular, in view of the objective of the legislation and the type of products covered by the legislation in question.

Where a modified product is considered as a new product, it must comply with the provisions of the applicable legislation when it is made available or put into service. This has to be verified by applying the appropriate conformity assessment procedure laid down by the legislation in question.”

Examples of substantial modifications under the CRA are changing the architecture of the product and/or its connection to interfaces, etc.

Reference: Blue guide Article 3 (31) 'substantial modification' means a change to the product with digital elements following its placing on the market, which affects the compliance of the product with digital elements with the essential requirements set out in Section 1 of Annex I or results in a modification to the intended purpose for which the product with digital elements has been assessed. Art. 69.2 (Substantial modification); Art. 2.1 (Scope); Art. 21 (Cases in which obligations of manufacturers apply to importers and distributors); Art. 22 (Other cases in which obligations of manufacturers apply) of the CRA.

2.8 What if somebody other than the original manufacturer makes a substantial modification to the product?

According to the Blue guide definition "The person who carries out important changes to the product carries the responsibility for verifying whether or not it should be considered as a new product in relation to the relevant Union harmonisation legislation. If the product is to be considered as new, this person becomes the manufacturer with the corresponding obligations."

Reference: Blue guide.

2.9 Consider a scenario in which a machine in the field (made available on the market before 2027) requires a substantial modification to one of its components (e.g., the engine) to solve a problem (e.g., a functional safety issue). Does the entire machine fall within the scope of the CRA or just the engine?

Based on preamble 41, if the product has undergone substantial modification a new conformity assessment would be required and if a third party was involved they need to be notified. If it is a product refurbishment it might not be classed as substantial modification (especially where the risk remains unaffected). If an upgrade of the product does not lead to the change of functionalities of the previous product and the level of risk is unaffected then it is not considered a substantial modification (according to preamble 42).

There are clauses for manufacturers/distributors who carry out substantial modifications would need to ensure that meet the requirements in Article 13 and Article 14 (based on Article 22, clause 2). Similarly, if a product is placed on the market before CRA and undergoes substantial modification it shall be subjected to CRA requirements (based on clause 2 of article 69).

Reference: Recitals 41 & 42 of the CRA, as well as Art. 3.30 (Definitions), Art. 22.1 & 22.2 (Other cases in which obligations of manufacturers apply) & Art. 69.2 (Transitional provisions).

3 CONFORMITY AND COMPLIANCE

3.1 How shall manufacturers demonstrate conformity with the CRA?

Conformity is based on self-assessment and consists of fulfilling the essential requirements of the CRA for products that need to satisfy only essential requirements in Annex I. In the self-assessment, companies need to demonstrate compliance with the essential requirements and outline the tests they do to ensure conformity, as well as provide a self-declaration.

However, there's currently a gap as the relevant cybersecurity standards are not finalised and therefore, cannot assist manufacturers with the conformity assessment. Once the standards are harmonised, then manufacturers should use these standards to demonstrate they are meeting the essential requirements of the CRA, therefore giving a presumption of conformity.

Conformity is not linked to Class 1 & Class 2 requirements found in Annex III as engines don't fall under the critical product category.

Reference: Chapter III (Conformity of the product with digital elements) of the CRA.

3.2 Is a harmonised standard available to assess the conformity to the CRA?

No harmonised standards are available for the time being. The EC's standards request is still being prepared. Currently, the European Commission (EC) is mapping the different standards, it is still unclear if the standards will be harmonised or not.

Reference: European Commission Standardisation Request.

3.3 Can the conformity be demonstrated by complying with ISO 21434/ ISO 62443?

Most of the essential requirements in Annex I of the CRA can be met with ISO/IEC 62443 but compliance to IEC 62443 does not mean compliance to CRA. Standards are being developed that refer to IEC 62443. ISO 21434 is to support the UNECE activities and is not harmonised at European level. ISO 21434 is a superset of the CRA, it includes a lot more process requirements and it is focused on on-road cybersecurity engineering. ISO SC19/WG 8 voted to pursue separate off-road standard (including 21434 parts that are applicable to cover CRA requirements). See answer to Question 3.2.

Reference: EUROMOT call with the EC from 5th September 2023. See Question 3.2 of this FAQ.

3.4 Is self-declaration by the manufacturer for the compliance to the essential requirements (annex I.1) allowed under the CRA?

For non-critical products, manufacturers would have to declare under their own responsibility that the devices with digital elements comply with all the security requirements defined in the draft CRA (self-assessment). Third party assessment is mandatory for Class II or higher products. declaration is required for IMPORTANT PRODUCTS WITH DIGITAL ELEMENTS (annex III) & CRITICAL PRODUCTS WITH DIGITAL ELEMENTS (Annex IIIa)

Reference: Annex I.1 of the CRA; Polona Car & Stefano De Luca(2023)[5]; European Parliament Briefing EU Legislation in Progress – EU cyber-resilience act. Members' Research Service PE 739.259. Available at : EU cyber-resilience act (europa.eu); Cyber Risk GmbH (2023)[6]; the European Cyber Resilience Act (CRA)[1].

3.5 How long must the vulnerability handling requirements (annex I.2) be fulfilled after placement on the market of a product with digital elements under the CRA?

For products with a lifespan longer than five years, then the supporting period shall be at least 5 years. If the lifespan of the product is shorter than 5 years, then the reporting needs to be conducted throughout the lifetime of the product. The lifespan of a product refers to time the product is expected to be in use. The manufacturer shall determine the support period (based on reasonable user expectations, nature of product, intended purpose, relevant union law). Chapter II, Article 13 (8) "Without prejudice to the second subparagraph of this paragraph, the support period shall be at least five years. When the product with digital elements is expected to be in use for less than five years, the support period shall correspond to the expected use time."

Art. 13.8: "Manufacturers shall ensure, when placing a product with digital elements on the market, and for the support period, that vulnerabilities of that product, including its components, are handled effectively and in accordance with the essential requirements set out in Annex I, Part II.

Manufacturers shall determine the support period so that it reflects the length of time during which the product is expected to be in use, taking into account, in particular, reasonable user expectations, the nature of the product, including its intended purpose, as well as relevant Union law determining the lifetime of products with digital elements. When determining the support period, manufacturers may also take into account the support periods of products with digital elements offering a similar functionality placed on the market by other manufacturers, the availability of the operating environment, the support periods of integrated components that provide core functions and are sourced from third parties as well as relevant guidance provided by the dedicated administrative cooperation group (ADCO) established pursuant to Article 52(15) and the Commission. The matters to be taken into account in order to determine the length of the support period shall be considered in a manner that ensures proportionality.

Without prejudice to the second subparagraph, the support period shall be at least five years. Where the product with digital elements is expected to be in use for less than five years, the support period shall correspond to the expected use time.

Taking into account ADCO recommendations as referred to in Article 52(16), the Commission may adopt delegated acts in accordance with Article 61 to supplement this Regulation by specifying the minimum support period for specific product categories where the market surveillance data suggests inadequate support periods.

Manufacturers shall include the information that was taken into account to determine the support period of a product with digital elements in the technical documentation as set out in Annex VII.

Manufacturers shall have appropriate policies and procedures, including coordinated vulnerability disclosure policies, referred to in Annex I, Part II, point (5), to process and remediate potential vulnerabilities in the product with digital elements reported from internal or external sources."

Reference: Art. 13.8 (Obligations of manufacturers) of the CRA

4 LINK WITH OTHER EUROPEAN REGULATIONS AND REQUIREMENTS

CYBER SECURITY ACT

4.1 How different are the CRA and the Cybersecurity Act (CSA) from a product, scope and requirement perspective?

The EU Cybersecurity Act[3] (Regulation (EU) 2019/881) introduces an EU-wide cybersecurity certification framework for ICT products, services and processes. The EU Cybersecurity Act (CSA) is commonly used across the EU and is used for Cyber Certification Schemes by Certification Assessment Bodies. The CSA allows for mutual recognition of European Certificates across the European Union (EU). It creates a common language for certification. Under the CSA, manufacturers can use third parties for third party certification, which at EU level adds some level of credibility. Under the CRA, when seeking certification, manufacturers can use the CSA for voluntary third-party certification.

According to Article 27 (9) "The Commission is empowered to adopt delegated acts in accordance with Article 61 of this Regulation to supplement this Regulation by specifying the European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 that can be used to demonstrate conformity of products with digital elements with the essential requirements or parts thereof as set out in Annex I to this Regulation. Furthermore, the issuance of a European cybersecurity certificate issued under such schemes, at least at assurance level 'substantial', eliminates the obligation of a manufacturer to carry out a third-party conformity assessment for the corresponding requirements, as set out in Article 32(2), points (a) and (b), and Article 32(3), points (a) and (b), of this Regulation."

Reference: [4]Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) and Recital 45; Art. 27.9 (Presumption of conformity).

4.2 Can a manufacturer use a Cybersecurity scheme under the CSA to get presumption of conformity to the CRA?

Yes, the manufacturer can get presumption of conformity to the CRA using CS scheme.

According to recital 82 "including when preparing the Union rolling work programme in line with Regulation (EU) 2019/881. Where there is a need for a new scheme covering products with digital elements, including in order to facilitate the compliance with this Regulation, the Commission may request ENISA to prepare candidate schemes in accordance with Article 48 of Regulation (EU) 2019/881."

Second, the EC needs to adopt a Delegated Act in accordance to Art 27.9 " The Commission is empowered to adopt delegated acts in accordance with Article 61 of this Regulation to supplement this Regulation by specifying the European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 that can be used to demonstrate conformity of products with digital elements with the essential requirements or parts thereof as set out in Annex I to this Regulation. Furthermore, the issuance of a European cybersecurity certificate issued under such schemes, at least at assurance level 'substantial', eliminates the obligation of a manufacturer to carry out a third-party conformity assessment for the corresponding requirements, as set out in Article 32(2), points (a) and (b), and Article 32(3), points (a) and (b), of this Regulation."

The certificate can be used by manufacturer as outlined in Article 27.9.

Reference: [4]Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act); Recital 83 of the CRA; Art.27.9 (Presumption of conformity)

FUNCTIONAL SAFETY

4.3 What is the relationship between the CRA and functional safety?

The CRA and functional safety are fundamentally two different things which are connected. If a manufacturer is reliant on a control system to deliver its functional safety with a high level of reliability, there is some interplay with cybersecurity. The EC is currently working on implementing standards to promote consistency in particular on aspects related to cyber security, safety and reliability of the system.

According to Annex I Part II on Vulnerability handling requirements, "Manufacturers of the products with digital elements shall:

(2) in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates".

In the CRA, recital 53 outlines that "Manufacturers of products falling within the scope of Regulation (EU) 2023/1230 of the European Parliament and of the Council which are also products with digital elements within the meaning of this Regulation should comply with both the essential requirements set out in this Regulation and the essential health and safety requirements set out in Regulation (EU) 2023/1230. The essential requirements set out in this

Regulation and certain essential requirements of Regulation (EU) 2023/1230 might address similar cybersecurity risks. Therefore, the compliance with the essential requirements set out in this Regulation could facilitate the compliance with the essential requirements that also cover certain cybersecurity risks as set out in Regulation (EU) 2023/1230, and in particular those regarding the protection against corruption and safety and reliability of control systems set out in sections 1.1.9 and 1.2.1 of Annex III to that Regulation. Such synergies have to be demonstrated by the manufacturer, for instance by applying, where available, harmonised standards or other technical specifications covering relevant essential requirements following a risk assessment covering those cybersecurity risks. The manufacturer should also follow the applicable conformity assessment procedures set out in this Regulation and in Regulation (EU) 2023/1230. The Commission and the European Standardisation Organisations, in the preparatory work supporting the implementation of this Regulation and of Regulation (EU) 2023/1230 and the related standardisation processes, should promote consistency in how the cybersecurity risks are to be assessed and in how those risks are to be covered by harmonised standards with regard to the relevant essential requirements. In particular, the Commission and the European Standardisation Organisations should take into account this Regulation in the preparation and development of harmonised standards to facilitate the implementation of Regulation (EU) 2023/1230 as regards in particular the cybersecurity aspects related to the protection against corruption and safety and reliability of control systems set out in sections 1.1.9 and 1.2.1 of Annex III to that Regulation. The Commission should provide guidance to support manufacturers subject to this Regulation that are also subject to Regulation (EU) 2023/1230, in particular to facilitate the demonstration of compliance with relevant essential requirements set out in this Regulation and Regulation (EU) 2023/1230."

Reference: CRA Standardisation Request; Recital 53 of the CRA; Annex I part II (Vulnerability handling requirements) of the CRA

RADIO EQUIPMENT DELEGATED ACT

4.4 What is the link between the CRA & Radio Equipment Directive delegated act (RED DA)? Will the RED DA be repealed if the CRA is released?

The delegated act under the Radio Equipment Directive (RED DA) constitutes a significant step towards increasing the level of cybersecurity of wireless devices that are widely used by consumers. It will be completed with the future CRA, which would aim to cover more products, looking at their whole life cycle. The initiative was announced in the EU Cybersecurity Strategy presented in December 2020.

According to recital 30 "when the Commission repeals or amends Delegated Regulation (EU) 2022/30 with the consequence that it ceases to apply to certain products subject to this Regulation, the Commission and the European Standardisation Organisations should take into account the standardisation work carried out in the context of Commission Implementing Decision C(2022)5637 on a Standardisation Request for the RED Delegated Regulation 2022/30 in the preparation and development of harmonised standards to facilitate the implementation of this Regulation. During the transition period of this Regulation, the Commission should provide guidance to manufacturers subject to this Regulation that are also subject to Delegated Regulation (EU) 2022/30 to facilitate the demonstration of compliance with the two Regulations".

The RED requirements are mapped in IEC 62443-1-1, IEC 62443-4-2, IEC 62443-4-1 & EN 303 645. ETSI TS 103929 V1.1.1 standards are applicable for the RED. Following the finalisation of the legislative text of the CRA there will be more or alternative standards developed. Legal discussions are still ongoing as the Standardisation Request is still being finalised. The RED DA standardisation work is underway in the JTC 13 WG8 and will finish in June 2024. JTC 13 WG 9 is working on the CRA standards. Policymakers and industry need to ensure the work from both groups is aligned.

Reference: Recital 30 of the CRA; CRA Standardisation Request; EUROMOT meeting with the EC from 5 September 2023; [7]European Commission (2021) Questions and Answers: Strengthening cybersecurity of wireless devices and products. Available at: Q&A: Strengthening cybersecurity of wireless devices (europa.eu)

ANTI-TAMPERING

4.5 Does the CRA cover tampering topics? If we meet the CRA, does it help to implement anti tampering solutions?

The CRA doesn't specify any antitampering solutions. The CRA requires risk analysis on the integrity (Annex I.2.d "On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: (...) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;"). Through the risk analysis done by manufacturers under the CRA, antitampering shall be considered more thoroughly.

Reference: Annex I part I, 2.d (Essential Cybersecurity Requirements) of the CRA.

DATA ACT

4.6 As for the link between the CRA and the Data Act (Reg 2023/2854), how does any data which is produced relate to the CRA? Such as engine performance and location data used in remote monitoring.

Manufacturers need to ensure that data related to privacy is protected. It is down to manufacturers to determine what is privacy data and what is in scope of the data act. According to the Data Act[3], any information which is not confidential (for example personal, security, intellectual property, trade secrets data) shall be available to third party vendors (Article 4 of the Data Act).

Reference: CRA Annex I (All essential cybersecurity requirements) & [3]Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

MACHINERY REGULATION

4.7 If we meet the CRA, does it automatically qualify Cybersecurity aspects for the Machinery Regulation (MR)? Is there a link with the Machinery Regulation?

The two regulations are different, the MR focuses on the risk/harm due to malicious intent via cyberattack, whereas the CRA is not just safety related to components but everything, it covers a broader scope than MR. The MR will apply sooner than the CRA, therefore there will be a time where manufacturers will only have to comply to the MR.

There is no official synergy between the two regulations. There is no presumption of conformity possible between the two. However, work on the Standardisation Request is still ongoing. Synergies may take place at standards level. Although the MR will apply earlier than the CRA, the standards development work for the CRA is in advance to the standards work of the MR. When MR applies, there will be an absence of harmonised standards.

In the Annex you will find a comparison table prepared by EUROMOT members comparing the cybersecurity requirements from the Machinery Regulation[2] with the CRA requirements from the from the ITRE committee draft, dating 20 June 2023.

Reference: [2]Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC (Machinery Regulation or MR).

4.8 Do manufacturers need to provide two sets of Declaration of Conformity (DoC) documents to fulfil the CRA & MR?

The Blue guide (Article 4.4) states that if equipment is in scope of one or more regulations, in this case CRA & MR, then manufacturers only need one DoC "A single declaration of conformity is required whenever a product is covered by several pieces of Union harmonisation legislation requiring an EU Declaration of Conformity. The single declaration of conformity can be made up of a dossier containing all relevant individual declarations of conformity."

Reference: Blue guide Art. 4.4 (EU declaration of conformity); Art. 20 of the MR (Declaration of conformity).

5 BIBLIOGRAPHY

1. European Parliament legislative resolution of 12 March 2024 on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (COM(2022)0454 – C9-0308/2022 – 2022/0272(COD)). Available at: Texts adopted - Cyber Resilience Act - Tuesday, 12 March 2024 (europa.eu)

2. Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC (Machinery Regulation or MR)

3. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)

4. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

5. Polona Car & Stefano De Luca (2023) European Parliament Briefing EU Legislation in Progress – EU cyber-resilience act. Members' Research Service PE 739.259. Available at: EU cyber-resilience act (europa.eu)

6. Cyber Risk GmbH (2023) The European Cyber Resilience Act (CRA). Available at: European Cyber Resilience Act (CRA) (european-cyber-resilience-act.com)

7. European Commission (2021) Questions and Answers: Strengthening cyber security of wireless devices and products**.** Available at: Q&A: Strengthening cybersecurity of wireless devices (europa.eu)

Annex: Comparison Matrix: Mapping of the MR vs. the CRA

MR 2023/1320		CRA ITRE (20 July)	
1.1.9 Protection against corruption	The machinery or related product shall be **designed and constructed** so that the connection to it of another device, via any feature of the connected device itself or via any remote device that communicates with the machinery or related product does not lead to a hazardous situation.	Article 2.1	This Regulation applies to products with digital elements whose intended, or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network.
		Article 10.1	When placing a product with digital elements on the market, manufacturers shall ensure that it has been **designed, developed and produced** in accordance with the essential requirements set out in Section 1 of Annex I.
		Article 10.2	For the purposes of complying with the obligation laid down in paragraph 1, manufacturers shall undertake an assessment of the cybersecurity risks associated with a product with digital elements and take the outcome of that assessment into account during the **planning, design, development, production**, delivery and maintenance phases of the product with digital elements with a view to minimising cybersecurity risks, **preventing security incidents** and minimising the impacts of such incidents, **including in relation to the health and safety of users**.
		Annex I.1.3.h	be designed, developed and produced to limit attack surfaces, **including external interfaces;**
	A **hardware component** transmitting signal or data, relevant for connection or access to software that is critical for the compliance of the machinery or related product with the relevant essential health and safety requirements shall be designed so that it is **adequately protected against** accidental or **intentional corruption**.	Annex I.1.3.b	ensure **protection from unauthorised access** by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;
	The machinery or related product shall collect evidence of a legitimate or illegitimate intervention in that hardware component, when relevant for connection or access to software that is critical for the compliance of the machinery or related product.	Annex I.1.3.j	provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions;
	Software and data that are critical for the compliance of the machinery or related product with the relevant essential health and safety requirements shall be identified as such and shall be **adequately protected against** accidental or **intentional corruption**.	Annex I.1.3.d	**protect the integrity of** stored, transmitted or otherwise processed **data**, personal or other, **commands**, **programs** and **configuration against any manipulation or modification not authorised** by the user, as well as report on corruptions;
	The machinery or related product shall **identify the software installed** on it that is necessary for it to operate safely and shall be able to **provide that information at all times in an easily accessible form**.	Annex I.2.1	**identify** and document vulnerabilities and **components contained in the product**, including by drawing up a **software bill of materials** in a **commonly used and machine-readable format** covering at the very least the top-level dependencies of the product;
	The machinery or related product shall collect evidence of a legitimate or illegitimate intervention in the software or a modification of the software installed on the machinery or related product or its configuration.	Annex I.1.3.j	provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions;

1.2.1 safety and reliability of control systems	1. they can withstand, **where appropriate to the circumstances and the risks**, the intended operating stresses and intended and unintended external influences, including **reasonably foreseeable malicious attempts** from third parties **leading to a hazardous situation**	Article 10.1	When placing a product with digital elements on the market, manufacturers shall ensure that it has been designed, developed and produced in accordance with the essential requirements set out in Section 1 of Annex I.
		Article 10.2	For the purposes of complying with the obligation laid down in paragraph 1, manufacturers shall undertake an **assessment of the cybersecurity risks** associated with a product with digital elements and take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements with a view to minimising cybersecurity risks, **preventing security incidents** and minimising the impacts of such incidents, **including in relation to the health and safety of users**.
		Annex I.1.1	Products with digital elements shall be designed, developed and produced in such a way that they enable **ensure an appropriate level of cybersecurity based on the risks**;

Contact Us

EUROMOT aisbl

The European Association of Internal Combustion Engine and Alternative Powertrain Manufacturers

Rue Joseph Stevens 7
1000 Brussels - Belgium

secretariat@euromot.eu

www.euromot.eu

EUROMOT