ISAGCA Webinar Series

# European Union Legislative Landscape: CRA, RED and their relation to ISA/IEC 62443 Webinar


## Eaton Industries GmbH

## Markus Wünsche - Oct 2024


ISA GLOBAL CYBERSECURITY ALLIANCE

EATON
Powering Business Worldwide

## Markus Wünsche

Engineering Manager - Processes Methods Tools,
Functional Safety and Cybersecurity

markuswuensche@eaton.com

Eaton Industries GmbH


Eaton is a power management company made up of over 92,000 employees, doing business in more than 175 countries.

Eaton also has a highly mature secure development lifecycle for products and applications which is also certified regarding world leading industrial cybersecurity standards.

As Engineering Manager for Processes Methods Tools, Functional Safety and Cybersecurity Markus Wünsche is leading a cross functional team. In that function he has the responsibility for the development process landscape and Continuous Improvement program of the engineering as also for the management systems regarding Cybersecurity and Functional Safety, covering the complete development lifecycle.

Markus is a certified specialist for IEC 62443, which is one of the world leading standards for cybersecurity in automation business. By his engagement in regulation and standardization on international level he contributes actively to shape the future of several cybersecurity-oriented standards and drives the integration of industry related aspects and requirements.

# Agenda

| | |
|---|---|
| European Legislation | Legal Acts and Consent Procedure |
| | Harmonized Standards |
| | From the Standardization Request to the citation in the Official Journal of the European Union |
| Paths to the Declaration of Conformity | Conformity – Radio Equipment Directive (RED) |
| | Conformity – Cyber Resilience Act (CRA) |
| Delegated Regulation supplementing Radio Equipment Directive (RED) | Overview |
| | Standardization Request |
| | RED and ISA/IEC 62443 |
| Cyber Resilience Act | Overview |
| | Reporting Obligations for Manufacturers |
| | Product Classes of Cyber Resilience Act |
| | CRA and ISA/IEC 62443 |
| Question/Answers | |

# Legal Acts and Consent procedure

## Legal acts of the European Union

- Regulation
  - A binding legislative act applied in its entirely across the EU
- Directive
  - A legislative act setting out a goal to EU countries. The individual countries must devise their own laws to reach this goal

# Legal Acts and Consent procedure

## National Consent procedure

- The national parliaments must be informed at the same time as the EU Parliament regarding the draft legislation
- If necessary, national parliaments can take a position against the law
- Is the draft legislation declined by at least a third of the national parliaments, a new review must take place

# Harmonized standards

## Harmonized Standards are a specific category of European standards

### Purpose

- Harmonized Standards are created in consent of different interested parties and containing solutions to fulfill legal requirements related to legislation of the European Union

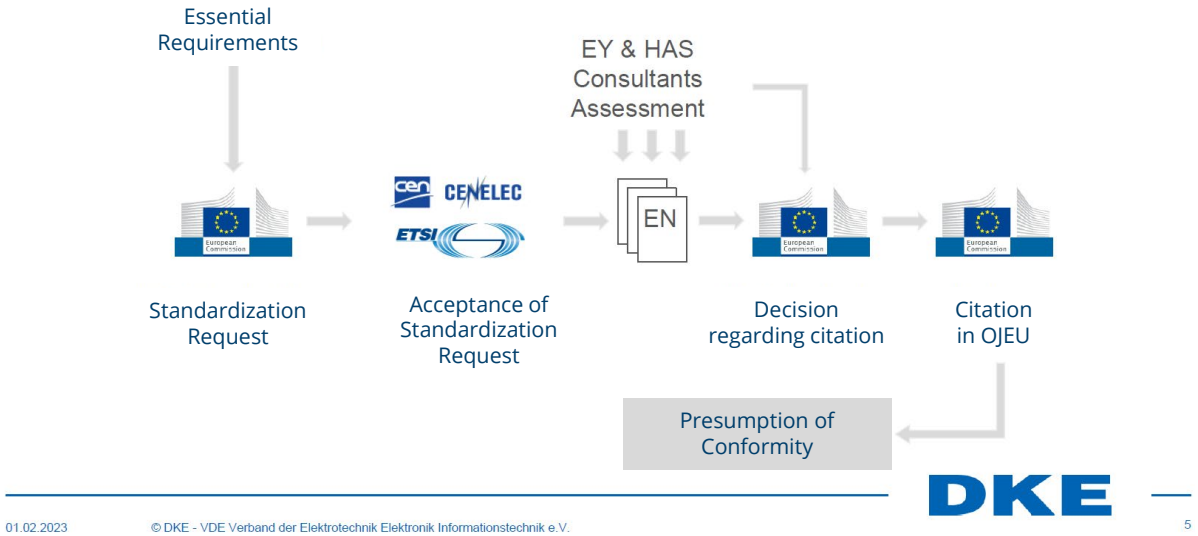
### Application and externality effect

- If harmonized standards are applied which is voluntarily there can be achieved the Presumption of Conformity. This fact will increase the legal certainty in a law case.
- By application of harmonized standards Manufacturers can demonstrate that their products are satisfying the legal requirements of the European Union

### Conditions

- A Standardization Request raised by the European Commission to one or multiple of the official European Standardization Organizations (ESO)
- Citation in the Official Journal of the European Union (OJEU)

# From the Standardization Request to the citation in the Official Journal of the European Union




[Derived from PeMa]

**Request**
- It is raised a standardization request from the European commission to the European Standardization Organizations (ESOs)

**Negotiation**
- The standardization request is negotiated between the ESOs and the European Commission by a Standardization Request Ad-hoc Group (SRAHG), which is organized by the ESOs

**Creation**
- After Acceptance of the standardization request, the corresponding standard(s) are worked out in an agreed timeframe. It is also possible to decline a standardization request. If the standardization request is declined completely the ESOs cannot influence the drafting process or the content anymore

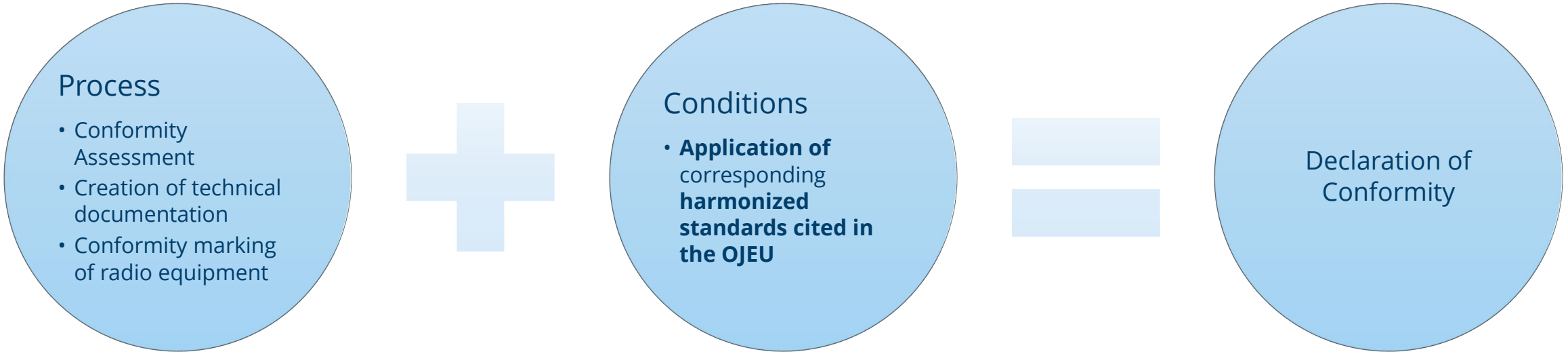
**Assessment**
- It takes place an assessment if the created standard(s) are satisfying the in the standardization request stipulated requirements of the European Commission.

**Citation**
- If the Assessment was successfully the created Standards get cited in the Official Journal of the European Union.

# Paths to the Declaration of Conformity

# Conformity – Radio Equipment Directive (RED)

# RED - Internal Control (Module A)



# RED - EU-type examination by notified body (Module B) and type based on internal production control (Module C)

**Module B**

- Creation of technical documentation
- **EU-type examination by a notified body**, this examination includes the **technical design** of the radio equipment
- EU-type examination certificate issued by notified body

+

**Module C**

- **Manufacturer assures** so that the production and its monitoring ensure **conformity of the radio equipment** with the approved type described in the EU-type examination certificate **meeting applicable requirements** of RED
- Conformity marking of radio equipment

=

Declaration of Conformity

# RED - Full Quality Assurance (Module H)

Process

- Creation of technical documentation
- **Assessment** of Quality Management Systems **via a notified body**
- Conformity marking of radio equipment

+

Conditions

- The **manufacturer shall operate an approved quality system** for design, manufacture, final radio equipment inspection and testing of the radio equipment concerned
- **Surveillance under** the **responsibility of** the **notified body**

=

Declaration of Conformity

# Conformity – Cyber Resilience Act (CRA)

# CRA - Conformity assessment procedures for products with digital elements

Conformity assessment procedures for products with digital elements

1. The manufacturer shall perform a conformity assessment of the product with digital elements and the processes put in place by the manufacturer to determine whether the essential requirements set out in Annex I are met. The manufacturer shall demonstrate conformity with the essential requirements by using any of the following procedures:

a) the **internal control procedure** (based on **module A**)
b) the **EU-type examination** procedure (based on **module B**) **followed by** conformity to **EU-type based on internal production control** (based on **module C**)
c) conformity assessment based on **full quality assurance** (based on **module H**) or
d) where available and applicable, a **European cybersecurity certification scheme**

# Conformity assessment procedures for products with digital elements – Procedures and Conditions

| Conformity Assessment procedures | Conditions |
|---|---|
| a) the **internal control procedure** (based on **module A**) | • Applicable for products of **the default class**<br>• Applicable for products of **important class I if** there were **applied** corresponding **harmonized standards or common specifications** |
| b) the **EU-type examination** procedure (based on **module B**) **followed by** conformity to **EU-type based on internal production control** (based on **module C**)<br><br>**Involvement of notified body necessary** | • Applicable for products of the **default class**<br>• Applicable for products of **important class I if** there were **not applied** corresponding **harmonized standards**, **common specifications** or **European cybersecurity certification scheme**<br>• Applicable for products of **important class II** |
| c) conformity assessment based on **full quality assurance** (based on **module H**)<br><br>**Involvement of notified body necessary** | • Applicable for products of the **default class**<br>• Applicable for products of **important class I if** there were **not applied** corresponding **harmonized standards**, **common specifications** or **European cybersecurity certification scheme**<br>• Applicable for products of **important class II** |
| d) where available and applicable, a **European cybersecurity certification scheme** | • Applicable for products of **the default class**<br>• Applicable for products of **important class I**<br>• Applicable for products of **important class II** |

# Conformity assessment procedures for products with digital elements – Critical Products

For the compliance with the Cyber Resilience Act critical products must follow specific rules

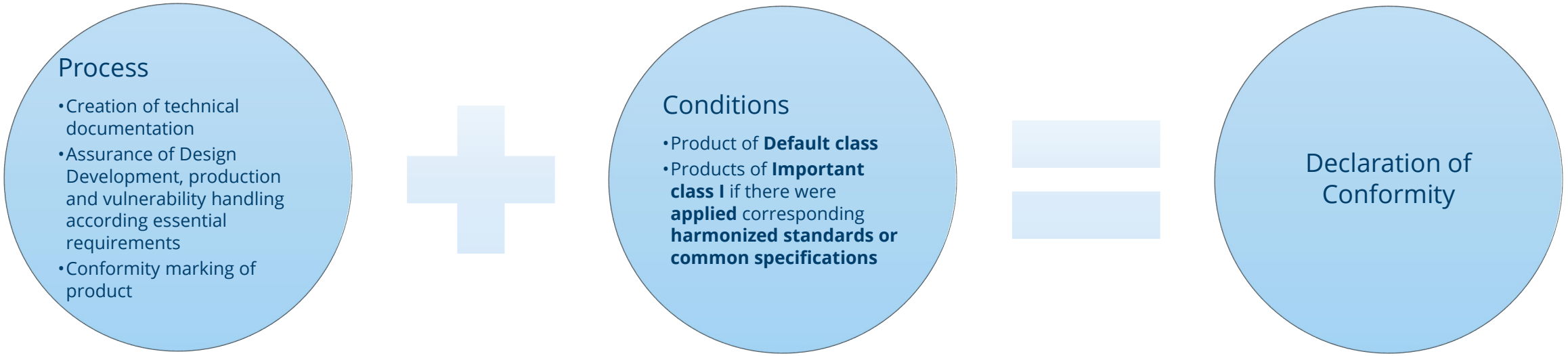
**Depending on the legal situation** it is necessary to **leverage European Cybersecurity Certification Schemes** to achieve compliance **or the rules for Important class II products** are applying

***Critical products with digital elements listed in Annex IIIa shall demonstrate conformity with the essential requirements set out in Annex I by using one of the following procedures:***

***(a) a European cybersecurity certification scheme or,***

***(b) where the conditions are not met, any of the procedures referred to in paragraph 3 of this Article.***

# CRA - Internal Control (Module A)



# CRA - EU-type examination by notified body (Module B) and Type based on internal production control (Module C)

The **notified body** shall carry out **periodic audits** to ensure that the vulnerability handling processes are implemented adequately

**Module B**

- Creation of technical documentation
- EU-type **examination by a notified body**, this examination includes the **design and development** of the product as also the **vulnerability handling** processes
- EU-type examination certificate issued by notified body

+

**Module C**

- **Manufacturer assures** so that the production and its monitoring ensure **conformity of the manufactured products** with the approved type described in the EU-type examination certificate meeting **essential requirements** as also the **vulnerability handling** processes
- Conformity marking of product

=

Declaration of Conformity

# CRA - Full Quality Assurance (Module H)

Process

- Creation of technical documentation
- Assessment of Quality Management System via a notified body
- Conformity marking of the product

+

Conditions

- The manufacturer shall operate an **approved quality system for design, development and product inspection and testing** of the products concerned **and for handling vulnerabilities**, **maintain** its effectiveness **for the time** the **products** concerned **are expected to be in use**
- **Surveillance under** the **responsibility of** the **notified body**

=

Declaration of Conformity

# Delegated Regulation supplementing Radio Equipment Directive (RED)

# Delegated Act (DA) for Radio Equipment Directive (RED) - Overview

## Delegated Act (DA) on RED Article 3 (d, e, f)

### Overview

- Introduction of Cybersecurity in RED via DA

### Current State

- Beginning from **August 2025** the DA **will be applicable** for products which are placed on the European market after this point of time

### Impacted devices and aspects

Radio equipment which is capable to communicate over the Internet (also indirectly) and/or handles privacy or financial related data

3 Main aspects

- RED - Article 3 (d) Radio equipment does not harm the network
- RED - Article 3 (e) Radio equipment protects personal data and privacy
- RED - Article 3 (f) Radio equipment protects from fraud (focus monetary value)

## Situation regarding Standards

### Overview

- Request for harmonized standards to show compliance to DA for RED was raised via European Commission (EC)

### Current state

- CEN/CENELEC JTC 13 WG 8 "Special Working Group for RED related harmonized standards
- **Voting was successful**
- **HAS Assessment negative** – no citation in the Official Journal of the European Union (OJEU)

### Important to note:

- **As long the standards are not cited in the OJEU a self responsible Assessment (Module A) is not possible**

# Standardization Request Requirements

**Standardization Request:**

**Harmonised standards in support of the essential requirement set out in Article 3(3), point (d/e/f), of Directive 2014/53/EU for the categories and classes specified by Delegated Regulation (EU) 2022/30 shall contain technical specifications that ensure at least that those radio equipment, where applicable:**

| | | |
|---|---|---|
| D | 1. | include elements to monitor and control network traffic, including the transmission of outgoing data; |
| D | 2. | is designed to mitigate the effects of ongoing denial of service attacks; |
| DEF | 3. | implement appropriate authentication and access control mechanisms; |
| DEF | 4. | are provided, on a risk basis, with up-to-date software and hardware at the moment of placing on the market that do not contain publicly known exploitable vulnerabilities as regards harm to the <d><e><f>; |
| DEF | 5. | are provided with automated and secure mechanisms for updating software or firmware that allow, when necessary, the mitigation of vulnerabilities that if exploited may lead to <d><e><f>; |
| DEF | 6. | protect the exposed attack surfaces and minimise the impact of successful attacks. |
| EF | 7. | protect stored, transmitted or otherwise processed <e> <f> against accidental or unauthorised storage, processing, access, disclosure, unauthorised destruction, loss or alteration or lack of availability of <e> <f>; |
| E | 8. | include functionalities to inform the user of changes that may affect data protection and privacy; |
| EF | 9. | log the internal activity that can have an impact on <e> <f>; |
| E | 10. | allow users to easily delete their stored personal data, enabling the disposal or replacement of equipment without the risk of exposing personal information; |

<d> = network or its functioning or misuse of network resources, <e> = personal & location data protection and privacy, <f> = financial or monetary data

[Kokx1]

- Monitoring and control of network traffic
- Mitigation of DoS Attacks
- Authentication and Access control
- Software Updates and no known and exploitable vulnerabilities
- Secure and automated Software Updates
- Reducing the Attack Surface and Minimization of Influence of successful attacks
- Protection of stored, transmitted or processed data against accidently or unauthorized storage, processing, access, disclosure, destruction, loss, alteration or unavailability
- User notification related to changes which could impact privacy
- Logging of internal activities
- Easy deletion of stored personal data by the user

# RED and ISA/IEC 62443 Requirements

- RED DA related essential requirements were necessary to be directly addressed in new standards requested by the standardization request
- Requirements in the CEN-CENELEC EN 18031 series were derived mainly from ISA/IEC 62443-4-2 and ETSI EN 303 645

- Security levels are addressed implicitly on base of different standards
- **CEN-CENELEC EN 18031-1** - Internet connected radio equipment
- **CEN-CENELEC EN 18031-2** - radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment
- **CEN-CENELEC EN 18031-3** -Internet connected radio equipment processing virtual money or monetary value

Aspects which were not considered explicitly already in ISA/IEC 62443-4-2

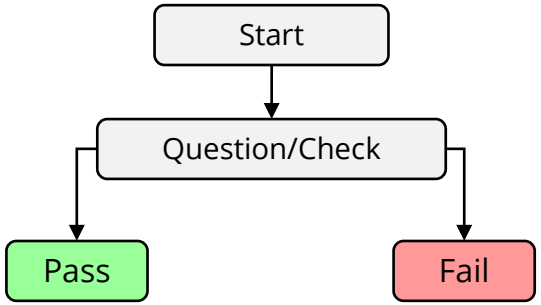
- Automated Updates
- Up-to-date software and hardware with no publicly known exploitable vulnerabilities
- Applicability and Appropriateness of user notification mechanisms
- *The equipment shall provide user notification mechanism(s) for informing the user of the equipment about changes affecting the protection or privacy of personal information, except for changes where: — other methods of informing the user exist, which do not involve the equipment.*

- A simple mapping between 18031 series and ISA/IEC 62443-4-2 is published as Annex in the published standards
- As these are informal Annexes those can only serve as a guideline

# RED and ISA/IEC 62443 Assessment Criteria

- As the CEN-CENELEC EN 18031 series was requested to serve as harmonized standards, additional requirements related to the content and drafting process applying
- Requirements must have a clear relation to the Essential requirements and the standardization request and have to cover them completely
- Detailed Assessment criteria are necessary for each requirement to enable reproducible assessment results

- ISA/IEC 62443-4-2 do not cover assessment criteria therefore it was necessary to draft them from scratch for the new standard series
- They were separated into the following sections for each requirement
  - Conceptual Assessment
  - Functional Completeness Assessment
  - Functional sufficiency Assessment
  - To improve tangibility decision trees were introduced which are reflecting the assessment process



# Cyber Resilience Act (CRA)

# Cyber Resilience Act (CRA) Overview

## Scope

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**.

## Definitions

**(1)** **'product with digital elements'** means any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately;

**(2)** **'remote data processing'** means any data processing at a distance for which the software is designed and developed by the manufacturer or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions;

## Cyber Resilience Act
2022/0272 (COD) 20th of Dec 2023

- Cybersecurity related development processes enforced by law
- Cybersecurity risks must be documented
- Active Reporting of exploited vulnerabilities and incidents by manufacturers
- 5 years SW Updates enforced or until EoL of products if the lifetime is shorter
- User Manual and Hardening Documentation
- Essential Cybersecurity Requirements for design, development and production of products
- Essential Requirements for Vulnerability Handling Processes

**Important Class products** requires either **application of a harmonized standard, common specifications or a third-party assessment**

**Reporting Obligations** expected to be applicable **mid of 2026**
**Product related Applicability** (end of transition period) expected **Q4 of 2027**

# Reporting Obligations for Manufacturers

*Manufacturers must **notify** any*

- ***actively exploited vulnerability contained in the product** with digital elements **as also** any **severe incident having an impact on the security of the product** with digital elements*
- ***Communication simultaneously** to the CSIRT designated **as coordinator and to ENISA via a single reporting platform***

## Early notification - 24 hours

- Early warning notification on actively exploited vulnerability
- Where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available

Additionally for Severe incident

- Information whether the incident is suspected of being caused by unlawful or malicious acts

## Additional Information - 72 hours

- Exploited vulnerability
  - **general information**, as available, about the product concerned,
  - the **general nature of the exploit** and of the respective vulnerability
  - **any corrective or mitigating measures taken**, **and** corrective or mitigating measures that **users can take.**
  - where applicable, **how sensitive** the notified information to be
- Severe incident
  - general information, about the **nature of the incident**, an **initial assessment** of the incident
  - **corrective or mitigating measures taken**, **and** corrective or mitigating measures that **users can take**
  - where applicable, **how sensitive** the notified information to be

## Final Report - Vulnerability - 14 days / Incident - one month

- Exploited vulnerability
  - a **description of the vulnerability**
  - where available, information concerning any malicious actor that has exploited or that is exploiting the vulnerability
  - **details about the security update or other corrective measures** that have been made available to remedy the vulnerability.
- Severe Incident
  - a description of the incident
  - the **type of threat or root cause** which probably triggered the incident
  - applied and Ongoing **Mitigations**

# Product classes of Cyber Resilience Act

Default class

- Under the internal control conformity assessment (Module A) manufacturer ensures fulfillment of general obligations as also essential product requirements of CRA - other conformity assessment procedures (Slide 14) could be selected voluntarily

Important Class I

- Application of Harmonized Standards, common specifications or third-party assessment required, to create Declaration of Conformity of Impacted products

Important Class II

- Involvement of notified body necessary, to create Declaration of Conformity of Impacted products or if available Application of a European Cybersecurity Certification Scheme

Critical products - *Depending on the legal situation for the specific product*

- necessary to leverage European Cybersecurity Certification Schemes to achieve compliance or
- the rules for Important class II products are applying

Examples for product classes

- Important Class I
- Smart home products with security functionalities
- Physical and virtual network interfaces
- Important Class II
- Firewalls, intrusion detection and/or prevention systems
- Critical class
- Smartcards or similar devices including secure elements
- Hardware devices with security boxes

# CRA and ISA/IEC 62443 Requirements & Mapping

**CRA related requirements are separated into**

- Product requirements
- Vulnerability handling requirements
- Information and instruction to the user
- CE Marking related technical documentation

*Different Security levels need to be considered explicitly*

**Mapping Activity**

- Several Mapping activities were/are driven to determine the applicability of existing standards regarding the Cyber Resilience Act
- There are some aspects which needs to be added to ISA/IEC 62443
- For harmonized Standards assessment criteria needs to be added to the standards

# CRA and ISA/IEC 62443 Potential Gaps

**Product Requirements**

- possibility to reset the product to its original state
- Support of automatic updates
- Protection of personal data
- Minimization of data
- support for allowing the user to opt-out of monitoring functionalities
- Reporting of possible unauthorized access

**Vulnerability handling Requirements**

- no requirement to keep the security updates separate from functional updates
- ongoing testing during the product life cycle
- Support automatic updates in vulnerability handling

**EU Technical Documentation**

- CRA related requirements for this aspect needs to be added

**Information and instructions to the user**

Needs to be extended as several potential gaps were determined – examples below

- Unique identification of the product
- documentation the conditions of reasonably foreseeable misuse.
- Internet address to retrieve EU declaration of conformity
- end-date of the support period…

# CRA and ISA/IEC 62443 Approach of Standard Drafting

## Content of CRA and Standardization Request

The proposal of CRA covers the following aspects

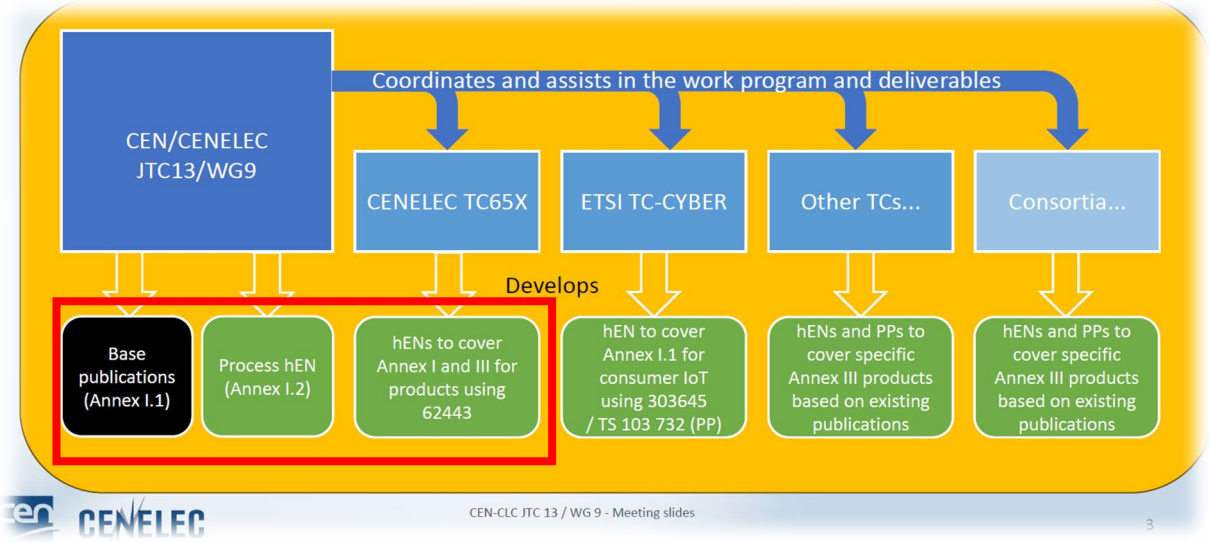
- Product Cybersecurity Requirements
- Vulnerability Handling Requirements
- Information and Instruction to the user
- CE Marking related Technical documentation

Standardization Request

- Under the scope of the EU Cyber Resilience Act Several standards needs to be drafted – The **Standardization requests is demanding 41 Standards** to be covered
- The Creation of these standards will be distributed in different TCs

## CEN/CENELEC JTC13 WG 9 Activities

- Acting as coordination group
- **CEN/CENELEC JTC 13 WG9** Drafting of **three base standards**
- **CENELEC TC65X WG 3** covering ISA/IEC **62443 related activities**
- Additional activities related to vertical standards will be driven by other TCs




[Kokx2]

# CRA and ISA/IEC 62443 Approach of Standard Drafting

## Scope of CEN/CENELEC JTC 13 WG 9

Drafting of three basic standards

1. Cybersecurity requirements for products with digital elements – **General principles for cyber resilience** (covering mainly the risk assessment approach)
2. Cybersecurity requirements for products with digital elements – **Common security requirements**
3. Cybersecurity requirements for products with digital elements – **Security vulnerability handling**

## Scope of CENELEC TC65X WG3

Operational Technology related standards – ISA/IEC 62443

- **Create harmonized standards** for ISA/IEC 62443 standards **to achieve Presumption of Conformity** for OT following ISA/IEC 62443 Series
- CENELEC TC65X WG 3 is **driving standardization projects to create harmonized standards (hEN) of ISA/IEC 62443-4-2** and **ISA/IEC 62443-3-3** which are defining System and Component Requirements

ISA/IEC 62443 standards mainly relevant to cover Cyber Resilience Act

- **IEC 62443-3-3 – Project to create harmonized Standards ongoing**
- **IEC 62443-4-2 – Project to create harmonized Standards ongoing**
- **IEC 62443-4-1 –** there might be a new work item proposal (NP) raised as well
- **IEC 62443-1-5 –** specification of Security Profiles
- **IEC 62443-6-2 –** considered as input

# Summary

## RED

- Delegated Act of RED will be applicable 1st of Aug 2025
- Radio equipment is in scope
- Standards are available but not cited
- Currently Notified bodies needs to be involved in the conformity assessment

## CRA

- not in force now (expected end of Oct 2024)
- Applicability of Reporting Obligations 21 month after entry into force
- General Applicability 36 month after entry into force
- Products with digital elements are impacted
- Several Product classes with different conditions regarding the conformity assessment

## Standardization

- CEN/CENELEC JTC13 WG 8 still working on the citation for the CEN-CENELEC EN 18031 series to enable self assessment for RED related products
- General and horizontal standards regarding the CRA to be covered via CEN/CENELEC JTC13 WG9
- Harmonized verticals for industrial OT using ISA/IEC 62443 series to be covered by CENELEC TC65X WG3
- Vertical Standards for other sectors to be covered via other Technical Committees

# Questions/Answers

# Sources (Online)

- Consent Procedure: Consent procedure - EUR-Lex (europa.eu) (Download 7th October 2024)
- Arten von Rechtsvorschriften | Europäische Union (europa.eu) (Download 7th October 2024)
- Standardisation requests: https://single-market-economy.ec.europa.eu/single-market/european-standards/standardisation-requests_en (Download 7th October 2024)
- Europäische Normen: https://europa.eu/youreurope/business/product-requirements/standards/standards-in-europe/index_de.htm (Download 7th October 2024)
- Harmonisierte Normen – Europäischer Rechtsrahmen: https://www.dke.de/de/normen-standards/harmonisierte-normen (Download 7th October 2024)
- Richtlinie 2014/53/EU: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014L0053 (Download 7th October 2024)
- Delegierte Verordnung (EU) 2022/30: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R0030 (Download 7th October 2024)
- 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 – 2022/0272(COD): Texts adopted - Cyber Resilience Act - Tuesday, 12 March 2024 (europa.eu) (Download 7th October 2024)

# Sources (Presentations)


- [PeMa] Petermann, N. Marian, C. (2023). Online Schulung: Harmonized Standards (HAS) System (Slide 5). DKE
- [Kokx1] Kokx, B. (2023). Presentation: RED Delegated Act (2022/30) Standardization Request – First Working Draft (Slide 5-6). CEN/CENELEC JTC 13/WG 8
- [Kokx2] Kokx, B. (2023). Presentation: WG9 input for the CRA SRAHG (Slide 12). CEN/CLC JTC 13/WG 9

# Sources (Images)


- Périgois, G. (2020). Bild: Europäische Kommission. Unsplash (Abgerufen am 23.05.2023)
- Seibert, L. (2020). Bild: Bundestag Deutschland. Unsplash (Abgerufen am 23.05.2023)

# Be Part of the Movement to Prioritize OT Cybersecurity

## Change the Culture

Recognize cybersecurity as a fundamental workplace tenet alongside functionality, efficiency, and safety

**Learn more | www.isagca.org**

# ISA Cybersecurity Resources

## Free guidance, training, and more:

**ISA Global Cybersecurity Alliance - www.isagca.org**

A collaborative forum to advance OT cybersecurity and understanding of ISA/IEC 62443

**ISASecure www.isasecure.org**

The world's leading conformance certification program for ISA/IEC 62443

**ICS4ICS www.ics4ics.org**

Improve how cybersecurity incidents are managed with training, processes, and exercises

## Get involved:

- ISA/IEC 62443 standards available from ISA (free access with ISA professional membership!)
- Cybersecurity training and certificate program
- Help develop the standard – open to all at no charge – www.isa.org/ISA99