European Union Legislative Landscape: CRA, RED & their Relation to ISA/IEC 62443 Webinar

UPDATE & CURRENT STATE

Eaton Industries GmbH
Markus Wünsche
September 2025

EATON
Powering Business Worldwide

ISA GLOBAL CYBERSECURITY ALLIANCE

Speaker Bio

Markus Wünsche

Engineering Manager of Processes Methods Tools,
Functional Safety and Cybersecurity -
EMEA Engineering, Electrical Sector

Eaton Industries GmbH

Powering Business Worldwide

Eaton is a power management company made up of over 92,000 employees, doing business in more than 160 countries.

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

As Engineering Manager of Processes Methods Tools, Functional Safety and Cybersecurity Markus Wünsche is leading cross functional teams. 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 in the EMEA Region, covering the complete development lifecycle.

Markus is also member of the Eaton Cybersecurity Steering committee, lead of the Secure development lifecycle and a certified specialist for IEC 62443, which is one of the world's leading standard series for cybersecurity related to Operational Technology (OT). 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 and Conformity Assessment
  - Legal Acts & Harmonized Standards
  - Conformity Assessment
- Delegated Regulation supplementing Radio Equipment Directive (RED)
  - RED & CEN-CENELEC EN 18031 Standard Series and Implementing Act
  - EN 18031 Standard Series Assessment Approach
- Cyber Resilience Act
  - Reporting Obligations for Manufacturers
  - Product Classes of Cyber Resilience Act and Draft Implementing Regulation
- Standardization Approach related to Cyber Resilience Act (CRA) – Activities and State
  - Horizontal Standards created by CEN-CENELEC JTC 13 WG9
  - Working Structure and Standardization Request
  - EN IEC 62443 based vertical Standards for Operational Technology (OT)
- Question/Answers

European Legislation and Conformity Assessment

Legal Acts and Harmonized Standards

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

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

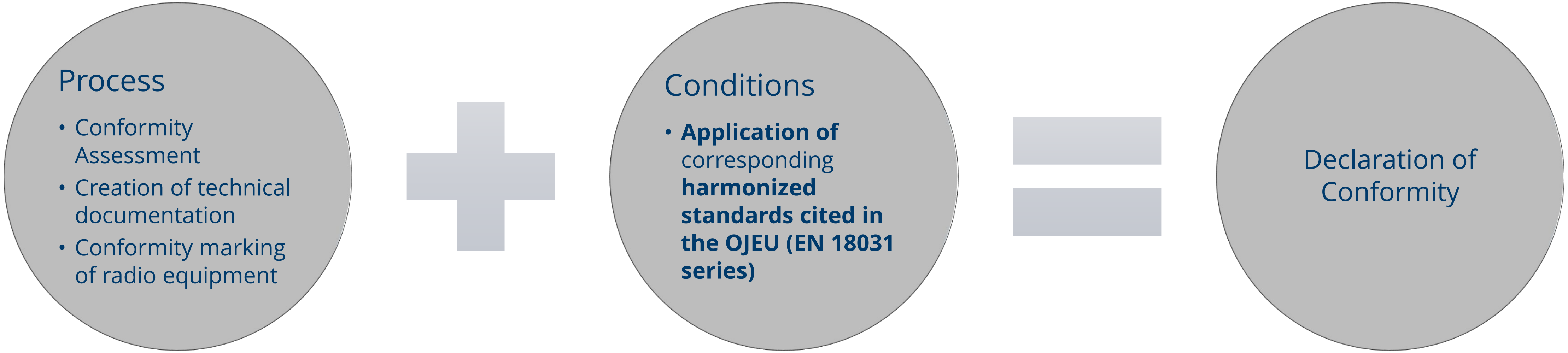
- If harmonized standards are applied which is voluntarily there can be achieved the Presumption of Conformity. This fact will increase the legal certainty in a law case (Reversed Burden of Proof)
- By application of harmonized standards Manufacturers can demonstrate that their products are satisfying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

EATON Powering Business Worldwide

RED - Internal Control Module A
Manufacturer Self Assessment



Process

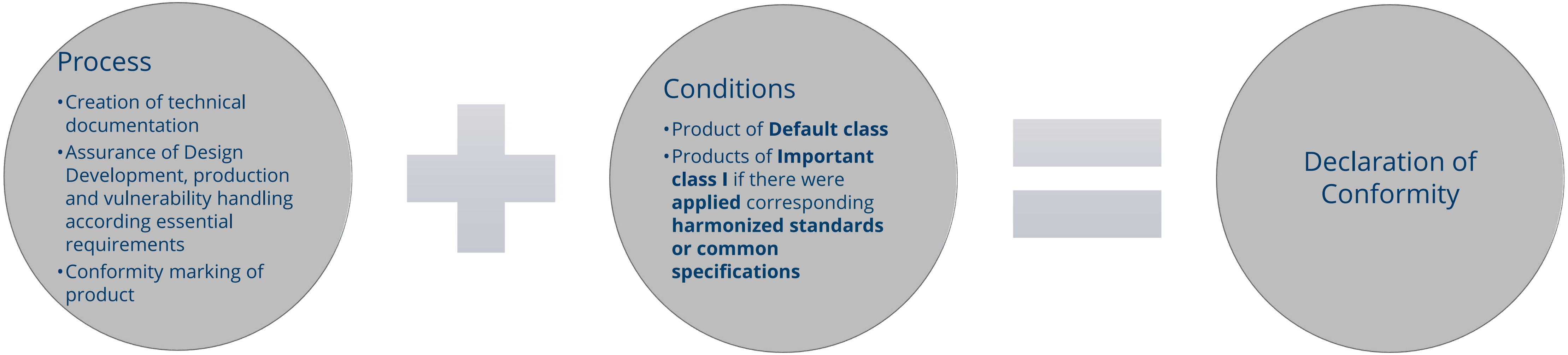
- Conformity Assessment
- Creation of technical documentation
- Conformity marking of radio equipment

Conditions

- **Application of** corresponding **harmonized standards cited in the OJEU (EN 18031 series)**

Declaration of Conformity

CRA - Internal Control (Module A)
Manufacturer Self Assessment



Process

- Creation of technical documentation
- Assurance of Design Development, production and vulnerability handling according essential requirements
- Conformity marking of product

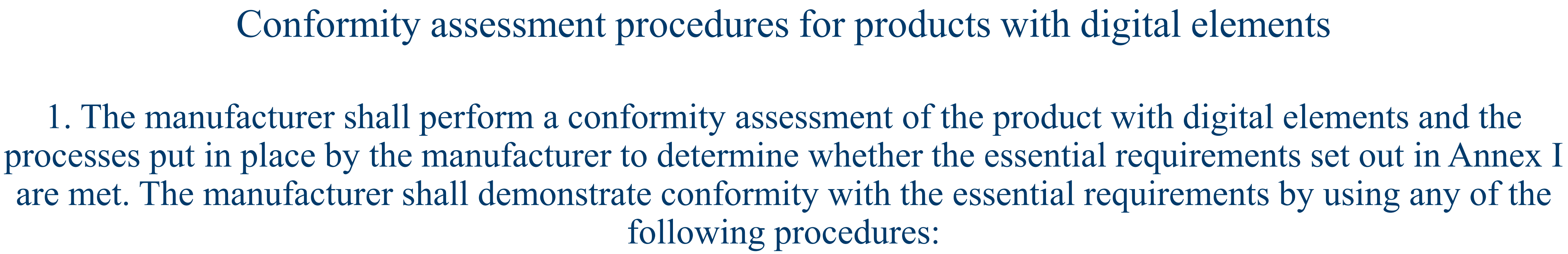
Conditions

- Product of **Default class**
- Products of **Important class I** if there were **applied** corresponding **harmonized standards or common specifications**

Declaration of Conformity

Powering Business Worldwide

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**

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

- Since **August 2025** DA **is 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 finished the work
- **Voting was successful**
- **Citation of CEN-CENELEC EN 18031 series in OJEU took place 30th of Jan 2025**

Important to note:

- Standards were sited 30th of January 2025 with minor restrictions **– so if not covered by this restrictions a manufacturers self assessment following this standards is possible now,** including the presumption of conformity

Harmonized EN 18031 Standard series and Implementing decision

EN 18031 series

Citation in Official Journal of the European Union

- Publication in OJEU took place on 30th of January 2025

EN 18031 Common security requirements for radio equipment

- Part 1: Internet connected radio equipment
- Part 2: radio equipment processing data, namely Internet connected radio equipment
- Part 3: Internet connected radio equipment processing virtual money or monetary value

Next Steps

- Corrigenda on EN 18031- series to fix some issues
- Proposed changes were reviewed by WG8 on the 22nd of May, currently the update documents are being edited

Implementing decision

Restrictions

Clauses 6.2.5.1 and 6.2.5.2 of harmonized standards EN 18031-1:2024, EN 18031-2:2024 and EN 18031-3:2024

- **If it is possible not to set or use any password**

Clauses 6.1.3, 6.1.4, 6.1.5 and 6.1.6 of harmonized standard EN 18031-2:2024

- **Not all implementation categories are compatible with parental or guardian control, in such a case is still an involvement of NB necessary**

Clause 6.3.2.4 of harmonized standard EN 18031-3:2024

- **If the product processes financial assets involvement of NB is required**

- **Link to Implementing decision**
  - Implementing decision - 2025/138 - EN - EUR-Lex

EATON
Powering Business Worldwide

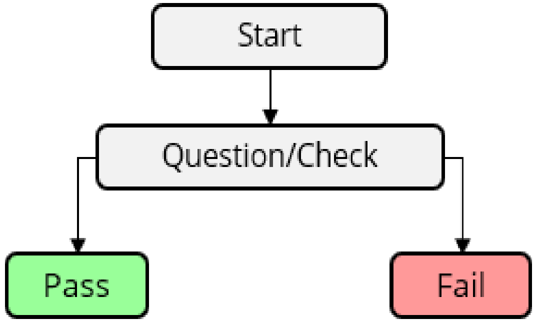
EN 18031 Series based Assessment approach

- 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
- Detailed Assessment criteria were described for each requirement to enable reproducible assessment results

Assessment and the CE Technical documentation

Assets have to be listed and described

- Per asset the decision tree must be passed
- Depending on the product the asset list could be long, leading to many loops in the decision tree

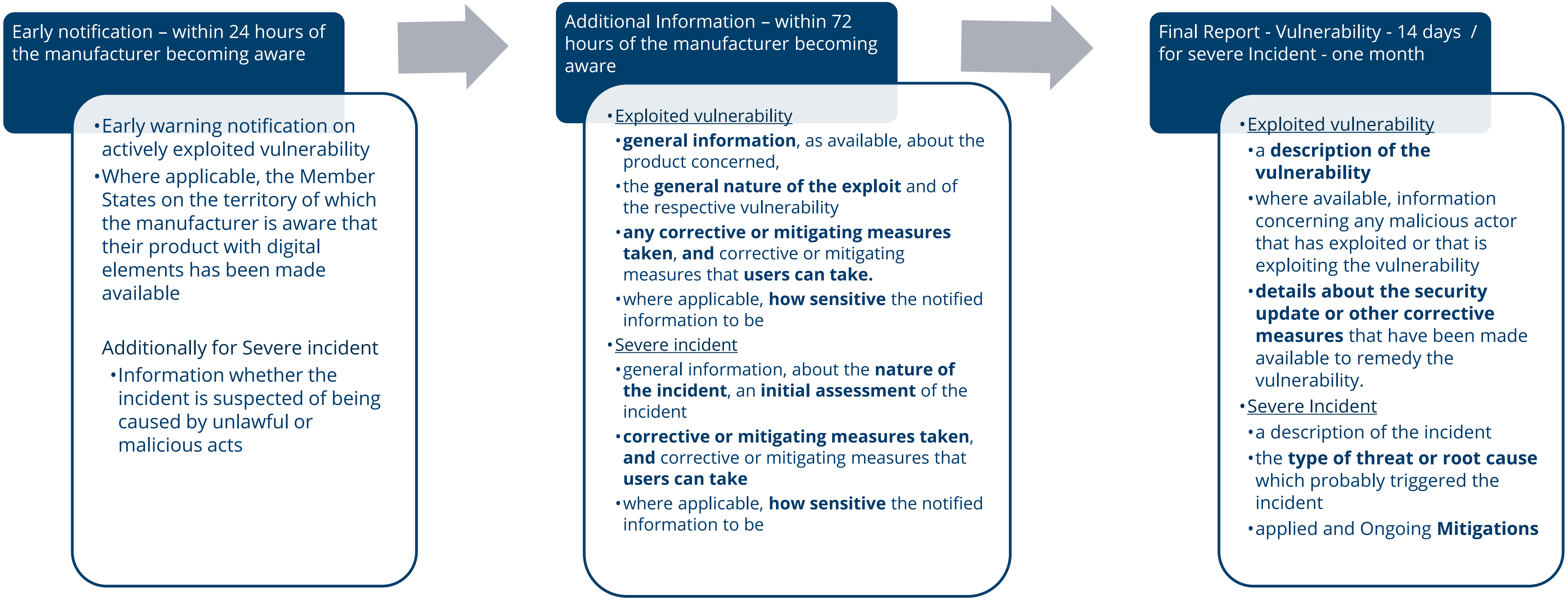


Cyber Resilience Act (CRA)

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 – within 24 hours of the manufacturer becoming aware

- 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 – within 72 hours of the manufacturer becoming aware

- 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 / for severe 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**

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 (EU) 2024/2847

- 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 or longer if the reasonable expected time in use is higher than five years
- 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 applicable from September of 2026**
  - **Product related Applicability** (end of transition period) **December 2027**

CRA Product classes

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**

Important Class II

Involvement of notified body necessary 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

Draft Implementing Regulation related to Product classes - Ares(2025)2037850

Definitions

A product's core functionality refers to its fundamental features and capabilities that fulfil the primary purpose for which the product with digital elements has been made available on the market and without which the product would not be able to meet its intended purpose or reasonably foreseeable use.

the **integration of a product with digital elements** which has the core functionality of a product category set out in Annex III and Annex IV to Regulation (EU) 2024/2847 does not in itself render the product in which it is integrated subject to the conformity assessment procedures applicable to those product categories

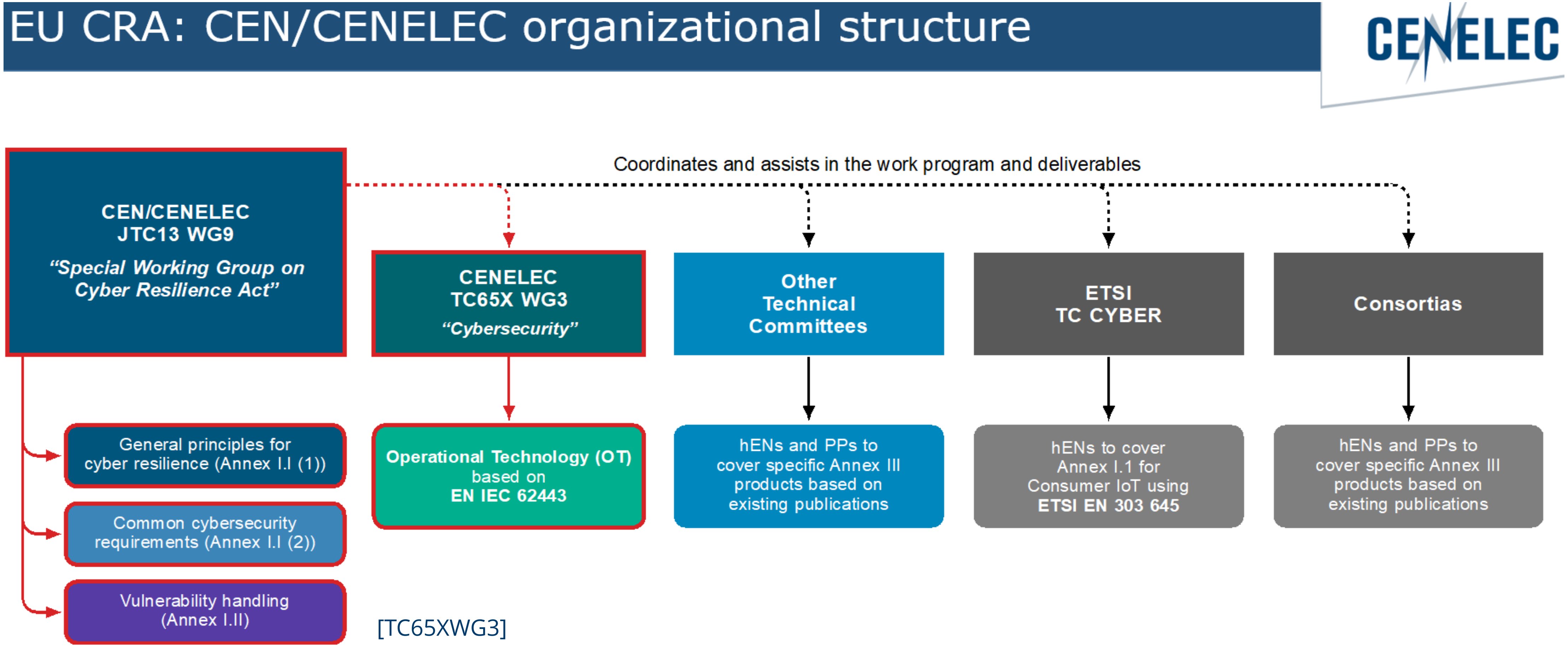
he fact that a product with digital elements performs functions other than or additional to those detailed in the technical descriptions set out in the Annexes does not in itself mean that the product with digital elements does not have the core functionality of a product category set out in the Annexes

Link to the Draft Implementing Regulation

- Technical description of important and critical products with digital elements

Standardization related to Cyber Resilience Act (CRA) – Activities and State

CRA related Working Structure



EU CRA: CEN/CENELEC organizational structure

CENELEC

Coordinates and assists in the work program and deliverables

CEN/CENELEC JTC13 WG9 *"Special Working Group on Cyber Resilience Act"*

- General principles for cyber resilience (Annex I.I (1))
- Common cybersecurity requirements (Annex I.I (2))
- Vulnerability handling (Annex I.II)

CENELEC TC65X WG3 *"Cybersecurity"*

- **Operational Technology (OT)** based on **EN IEC 62443**

Other Technical Committees

- hENs and PPs to cover specific Annex III products based on existing publications

ETSI TC CYBER

- hENs to cover Annex I.1 for Consumer IoT using **ETSI EN 303 645**

Consortias

- hENs and PPs to cover specific Annex III products based on existing publications

[TC65XWG3]

CENELEC JTC 13 WG 9
Horizontal Standards and Project Teams

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 -
   1. **Common security requirements**
   2. **Threats and Security Objectives**
3. Cybersecurity requirements for products with digital elements – **Security vulnerability handling**

Project Team 1 - General principles for cyber resilience

- Process activities for security risk management during the product life cycle.
- Horizontal standard therefore not explicit concerning methods
- Activities description based as security objective, with inputs, outputs and constraints, content vise **there are many parallels to 62443-4-1**
- Review State:
  - Internal WG 9 review was done,
  - 1st HAS Review took place, receiving 194 comments
- **ENQ (1st voting for national bodies) + HAS Assessment expected – Nov 2025**
- Date of publication targeted for Oct 2026

CENELEC JTC 13 WG 9
Horizontal Standards and Project Team 2

Cybersecurity requirements for products with digital elements – Common security requirements

- Covering the essential product requirements and library of security controls
- Provides a library of security controls and objectives + assessment criteria as also a mapping to essential requirements
- **Currently based on EN 18031:2024 series**, with some additional security controls.
- **Draft 1st HAS Assessment targeted Jan 2026**
- Discussions how much text of RED related EN 18031 series could be re-used concerning the transition of RED and CRA

Cybersecurity requirements for products with digital elements – Threats and Security Objectives

- PT2 works on a draft TR concerning common threats related to the essential product requirements and the security objectives.
- NWIP in circulation with a progressed draft to be available for the contributors drafting standards
- **State**
  - NWIP Approval pending
  - 2nd Working Draft targeted 26th of Sep 2025
  - Vote submission 19th of Dec 2025
  - Date of availability targeted 5th of Jun 2026
  - Ballot closes 16th of July

PT currently on hold to focus on PT 3 Standards

CENELEC JTC 13 WG 9
Horizontal Standards and Project Team 3

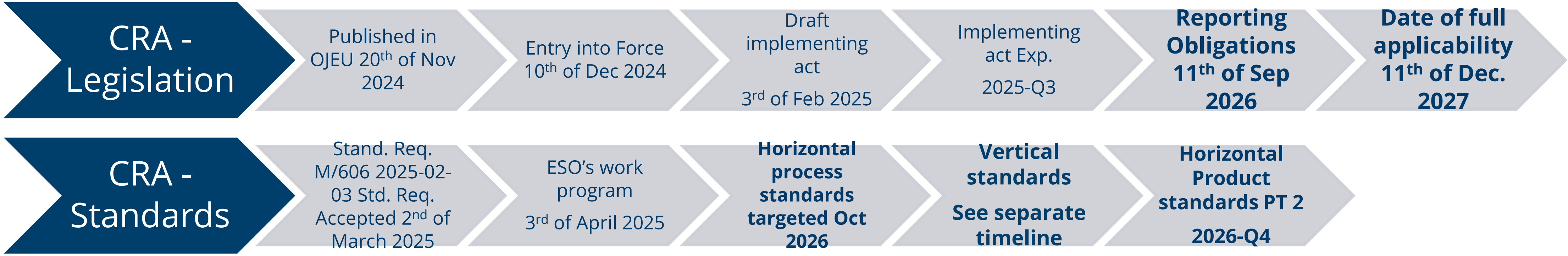
Cybersecurity requirements for products with digital elements - Security vulnerability handling

- Covering process activities for vulnerability handling.
- Intended as horizontal standard which verticals could normatively reference without or with less adaptions
- The **only horizontal standard** of the three intended to be cited **providing the presumption of conformity for** Annex I, part II **– Essential requirements for Vulnerability Handling**
- Strong normative dependency on the Standards
  - **EN ISO/IEC 30111** Information technology - Security techniques - Vulnerability handling processes
  - **DIN EN ISO 29147** Information technology - Security techniques - Vulnerability disclosure
- 1st internal circulation took place
- **Enquiry + HAS Assessment targeted 1st of Nov 2025**
- Date of Availability targeted Oct 2026

Cybersecurity requirements for products with digital elements – Vocabulary

- Intended to ensure consistent use of terms and definitions for all horizontal deliverables of JTC13/WG9 for the CRA.
- PT1 related ENQ will include Terms and Definitions
- Schedule of the Vocabulary document will be aligned with PT3.
- **Enquiry + HAS Assessment targeted 1st of Nov 2025**
- **Publication might be in March 2026**

Cyber Resilience Act timeline of legislation vs timeline of deliverables created/coordinated by WG 9



CRA - Legislation

Published in OJEU 20th of Nov 2024

Entry into Force 10th of Dec 2024

Draft implementing act

3rd of Feb 2025

Implementing act Exp.

2025-Q3

Reporting Obligations 11th of Sep 2026

Date of full applicability 11th of Dec. 2027

CRA - Standards

Stand. Req. M/606 2025-02-03 Std. Req. Accepted 2nd of March 2025

ESO's work program

3rd of April 2025

Horizontal process standards targeted Oct 2026

Vertical standards

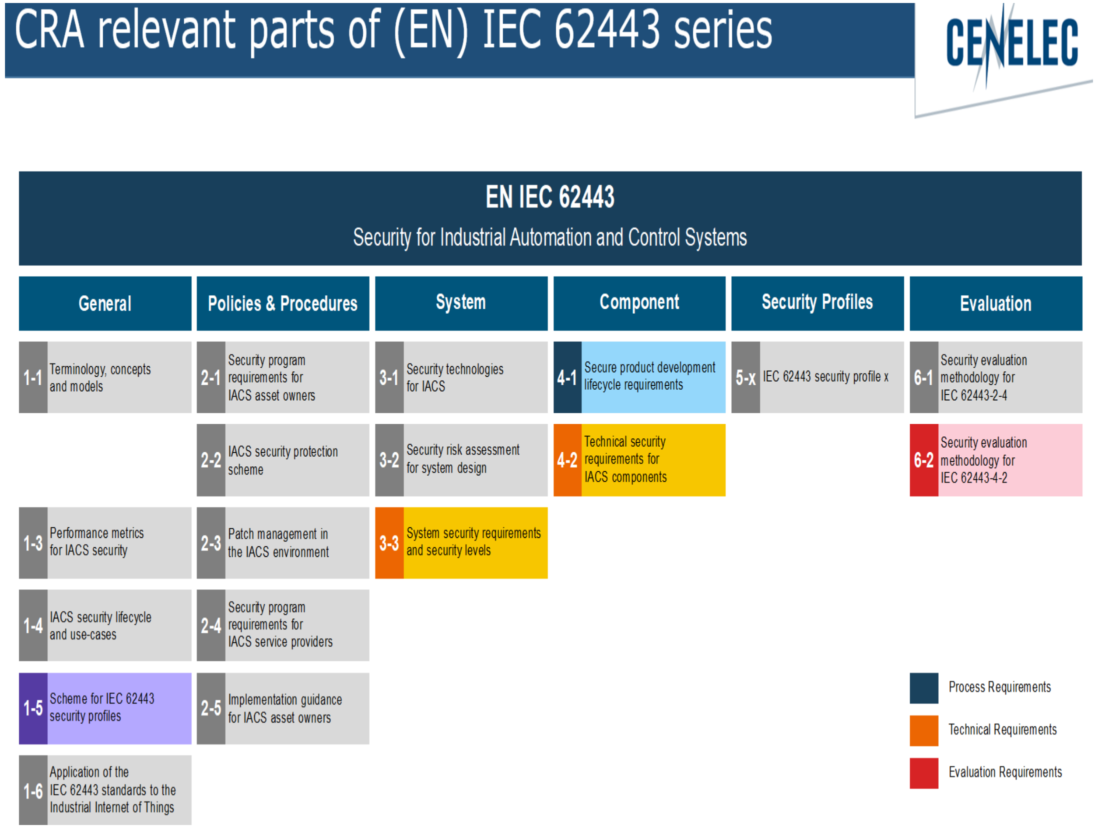
See separate timeline

Horizontal Product standards PT 2

2026-Q4

Timelines related to standards are not perfectly fixed and can vary

For CRA relevant parts of 62443 Series



CRA relevant parts of (EN) IEC 62443 series

CENELEC

EN IEC 62443

Security for Industrial Automation and Control Systems

General	Policies & Procedures	System	Component	Security Profiles	Evaluation
1-1 Terminology, concepts and models	2-1 Security program requirements for IACS asset owners	3-1 Security technologies for IACS	4-1 Secure product development lifecycle requirements	5-x IEC 62443 security profile x	6-1 Security evaluation methodology for IEC 62443-2-4
	2-2 IACS security protection scheme	3-2 Security risk assessment for system design	4-2 Technical security requirements for IACS components		6-2 Security evaluation methodology for IEC 62443-4-2
1-3 Performance metrics for IACS security	2-3 Patch management in the IACS environment	3-3 System security requirements and security levels			
1-4 IACS security lifecycle and use-cases	2-4 Security program requirements for IACS service providers				
1-5 Scheme for IEC 62443 security profiles	2-5 Implementation guidance for IACS asset owners				
1-6 Application of the IEC 62443 standards to the Industrial Internet of Things					

🟦 Process Requirements

🟧 Technical Requirements

🟥 Evaluation Requirements

[TC65XWG3]

- EN IEC **62443-4-2** “Technical security requirements for IACS components”
- EN IEC **62443-3-3** “System security requirements and security levels”
- EN IEC **62443-4-1** “Secure product development lifecycle requirements”

- IEC TS **62443-6-2** “Security evaluation methodology for IEC 62443-4-2” (Draft)
  - Procedure for evaluating IEC 62443-4-2 requirements that have been implemented in a product following an IEC 62443-4-1 compliant secure product development lifecycle

- EN IEC TS **62443-1-5** “Scheme for IEC 62443 security profiles”
  - Procedure for specifying “security profiles”

EATON
Powering Business Worldwide

ISA

OT related important products in Standardization Request and Concept of Profiles

CRA Standardization Request (Annex I)

Important Class I Products:

- #20: products with digital elements with the function of virtual private network (VPN)
- #21: network management systems
- #22: Security information and event management (SIEM) systems
- #25: physical and virtual network interfaces
- #27: routers, modems intended for the connection to the internet, and switches

Important Class II Products

- #36: firewalls, intrusion detection and/or prevention systems, including specifically those intended for industrial use

Concept of Profiles (62443-1-5)

An IEC 62443 security profile is a defined subset of IEC 62443 requirements contextually mapped

- a **specific application domain** (e.g., discrete manufacturing, process industry);
- an **area of activity** (e.g., integration, patch management);
- the **intended operational environment and the security context** of a product (component, system) or automation solution within that environment; or
- **particular type(s) of product(s).**

[TC65XWG3]

CRA and 62443 series 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

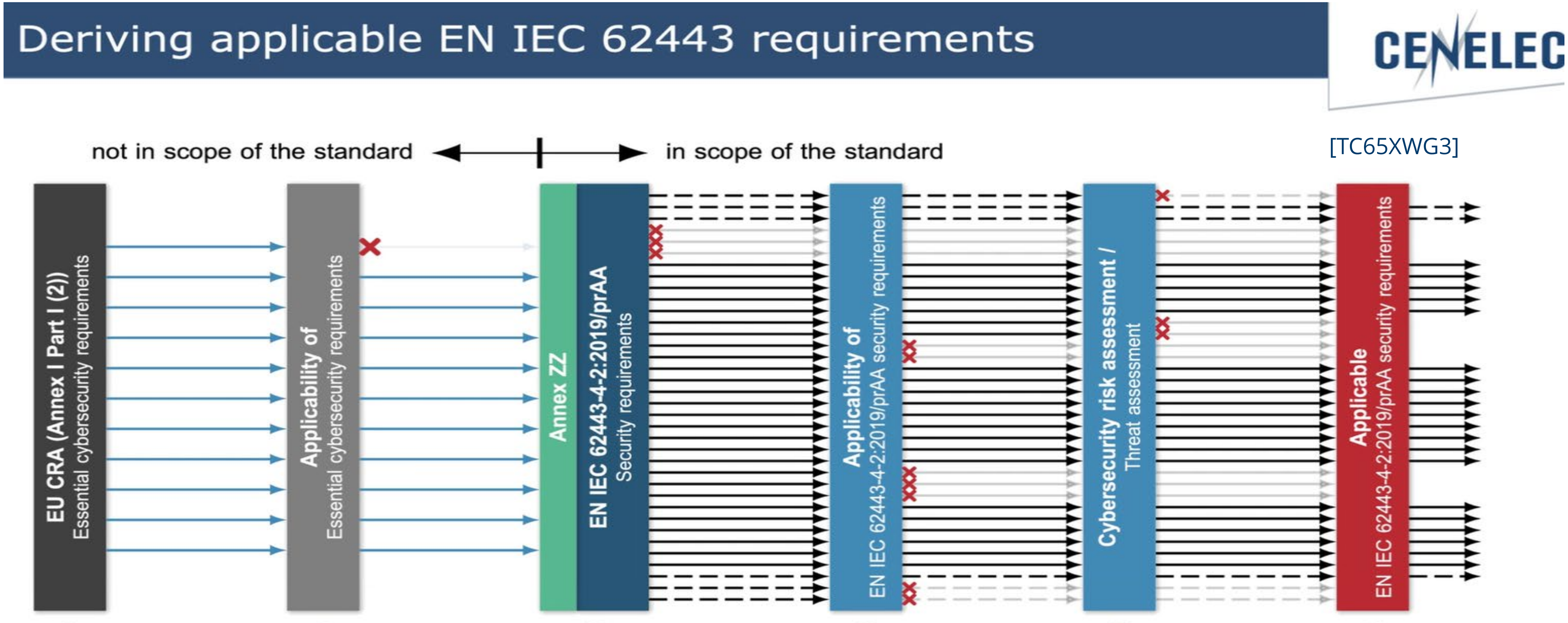
- Unique identification of the product
- documentation the conditions of reasonably foreseeable misuse.
- Internet address to retrieve EU declaration of conformity
- end-date of the support period…

CEN-CENELEC JTC 13 WG9

Overview of Activities

- Creation of Common modifications based on EN IEC 62443-4-1:2018 and EN IEC 62443-4-2:2019
- EN IEC 62443-4-1:2019/A11:2026
  - Close identified gaps
  - Determination of documentation related artifacts concerning CE Technical documentation
  - Align with PT 1 related activities – General principles of Cyber Resilience
- EN IEC 62443-4-2:2019/A11:2026
  - Creation of new requirements to close gaps currently uncovered
  - Adaption of existing requirements and rationales to meet essential requirements of CRA
  - Adding of Applicability and acceptance criteria for all CRs and RE
  - Determination of documentation related artifacts

Applicability of 62443 Requirements



Deriving applicable EN IEC 62443 requirements

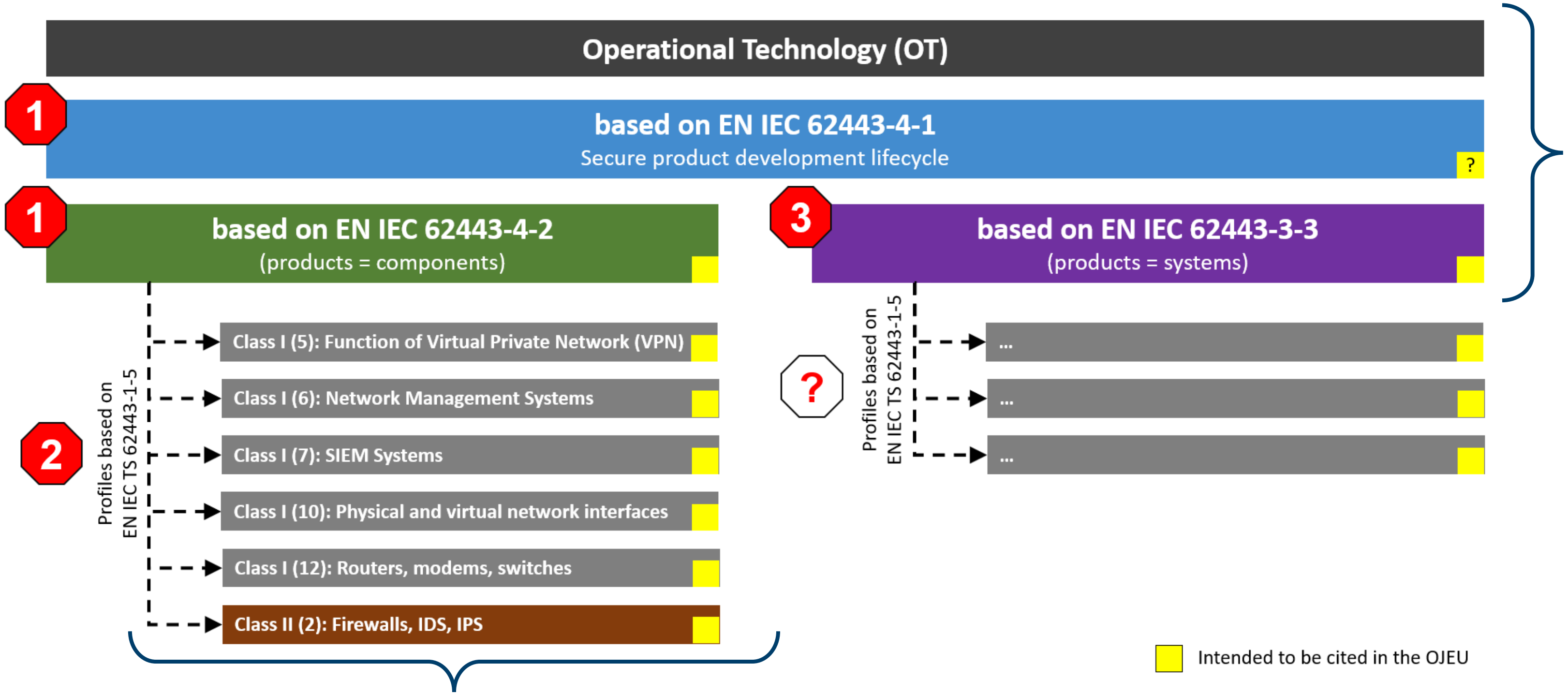
CENELEC
not in scope of the standard
in scope of the standard
EU CRA (Annex I Part I (2))
Essential cybersecurity requirements
Applicability of
Essential cybersecurity requirements
Annex ZZ
EN IEC 62443-4-2:2019/prAA
Security requirements
Applicability of
EN IEC 62443-4-2:2019/prAA security requirements
Cybersecurity risk assessment /
Threat assessment
Applicable
EN IEC 62443-4-2:2019/prAA security requirements

[TC65XWG3]

CRA 62443 based framework

EU CRA: EN IEC 62443 based standardization framework
Derived vertical product (category) standards ("profiles")

CENELEC



Operational Technology (OT)

1 **based on EN IEC 62443-4-1**
Secure product development lifecycle ?

1 **based on EN IEC 62443-4-2**
(products = components)

3 **based on EN IEC 62443-3-3**
(products = systems)

2 Profiles based on EN IEC TS 62443-1-5

- Class I (5): Function of Virtual Private Network (VPN)
- Class I (6): Network Management Systems
- Class I (7): SIEM Systems
- Class I (10): Physical and virtual network interfaces
- Class I (12): Routers, modems, switches
- Class II (2): Firewalls, IDS, IPS

? Profiles based on EN IEC TS 62443-1-5

- ...
- ...
- ...

🟨 Intended to be cited in the OJEU

Broad verticals
Ideally, we get 4-2 cited to provide presumption of conformity based on reference to 4-1 for default product category

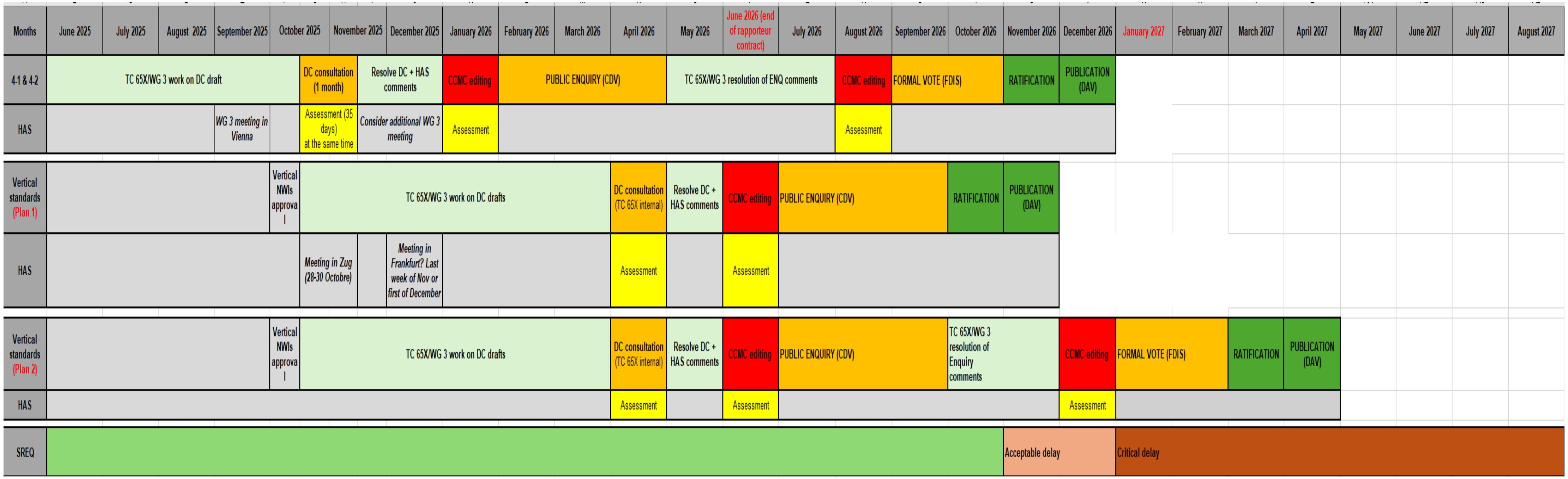
For 3-3 the situation is unclear

Verticals based on profiles
Part of Standardization request and Intended
to provide the **presumption of conformity for product requirements**

[TC65XWG3]

EATON
Powering Business Worldwide

Timeline for 62443 based deliverables



Months	June 2025	July 2025	August 2025	September 2025	October 2025	November 2025	December 2025	January 2026	February 2026	March 2026	April 2026	May 2026	June 2026 (end of rapporteur contract)	July 2026	August 2026	September 2026	October 2026	November 2026	December 2026	January 2027	February 2027	March 2027	April 2027	May 2027	June 2027	July 2027	August 2027
4-1 & 4-2	TC 65X/WG 3 work on DC draft				DC consultation (1 month)	Resolve DC + HAS comments		CCMC editing	PUBLIC ENQUIRY (CDV)			TC 65X/WG 3 resolution of ENQ comments			CCMC editing	FORMAL VOTE (FDIS)		RATIFICATION	PUBLICATION (DAV)								
HAS				*WG 3 meeting in Vienna*	Assessment (35 days) at the same time	*Consider additional WG 3 meeting*		Assessment							Assessment												
Vertical standards (Plan 1)					Vertical NWIs approval TC 65X/WG 3 work on DC drafts						DC consultation (TC 65X internal)	Resolve DC + HAS comments	CCMC editing	PUBLIC ENQUIRY (CDV)			RATIFICATION	PUBLICATION (DAV)									
HAS					*Meeting in Zug (28-30 Octobre)*		*Meeting in Frankfurt? Last week of Nov or first of December*				Assessment		Assessment														
Vertical standards (Plan 2)					Vertical NWIs approval TC 65X/WG 3 work on DC drafts						DC consultation (TC 65X internal)	Resolve DC + HAS comments	CCMC editing	PUBLIC ENQUIRY (CDV)			TC 65X/WG 3 resolution of Enquiry comments		CCMC editing	FORMAL VOTE (FDIS)		RATIFICATION	PUBLICATION (DAV)				
HAS											Assessment		Assessment						Assessment								
SREQ																		Acceptable delay		Critical delay							

- Draft of 4-1 / 4-2 related deliverables for HAS Assessment targeted for Q4 2025
- Verticals are dependent from horizontals which are delayed
- Additional work to create common modifications before every review step (DC, ENQ and FV)

[TC65XWG3]

I want to emphasize here again, the described regulations are laws and therefore it is crucial to understand the law as well as the standards. Therefore, legal and technical experts have to work united with national and European authorities to achieve the Goal.

Even if this upcoming laws are challenging there are also opportunities for the industry, and it should be considered that these regulations are intended to increase the Cyber Resilience for a society depending on technology.

Sources (Online)

- Arten von Rechtsvorschriften | Europäische Union (europa.eu) (Download 10th September 2025)
- Europäische Normen: https://europa.eu/youreurope/business/product-requirements/standards/standards-in-europe/index_de.htm (Download 10th of Sep 2025)
- Harmonisierte Normen – Europäischer Rechtsrahmen: https://www.dke.de/de/normen-standards/harmonisierte-normen (Download 10th of Sep 2025)
- Cyber Resilience Act:

Regulation - 2024/2847 - EN - EUR-Lex (Download 10th of Sep)

- Link to the Draft Implementing Regulation (Download 10th of Sep)

Technical description of important and critical products with digital elements

Sources (Presentations)

- [JTC13WG9] Kokx, B. (2025). Presentation: Horizontal cybersecurity for products with digital elements - CEN/CENELEC JTC 13/WG 9
- [TC65XWG3] Rossebo, J. & Wollenweber, K. (2025). Presentation: CLC/TC65X WG 3 “Cyber Security” Overview of CRA related activities CENELEC TC65X WG 3

Sources (Images)

- Périgois, G. (2020). Bild: Europäische Kommission. 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