Manufacturers' Obligations and Standardization Efforts

Aligning with CEN-CENELEC JTC 13 WG 9 Initiatives

Cyprus – Building a Cybersecure Future – Nicosia, May 5th 2025

cen CENELEC

Gabriel Faifman - Director, Product Security Standardization & Governance – Schneider Electric

Life Is On Schneider Electric

Gabriel Faifman

Director, Product Security Standardization & Governance

- Director, Product Security Standardization & Governance – Schneider Electric
- MS Electronic Engineer since 1994 | Specialized in Industrial Automation
- CSS1 Infosec Professional | Advanced Trained at INL
- 30+ years in Cybersecurity & Automation Leadership
- Active IEC Member since 2011 | Co-Convenor, IEC TC 65 WG 10
- Chair, Product Security TSG – Connectivity Standards Alliance (CSA)
- Former roles at Wurldtech (GE Digital), Coca-Cola, Deloitte, Accenture
- Bridging standards (IEC, ISO, ETSI) & certifications (ISASecure, IECEE)Promoting cybersecurity principles across IT, OT, IoT & IIoT

Agenda – May 5th 2025

Cyprus – Building a Cybersecure Future

- Overview of the Cyber Resilience Act (CRA)
- Manufacturer Obligations under CRA
- Standardisation Efforts – European Standardisation Organisations ESOs
- Essential Cybersecurity Requirements
- IEC 62443-4-1 Overview
- Mapping CRA to IEC 62443-4-1 Requirements
- Implementation Guidance for Industry
- Q&A

Manufacturers' Obligations

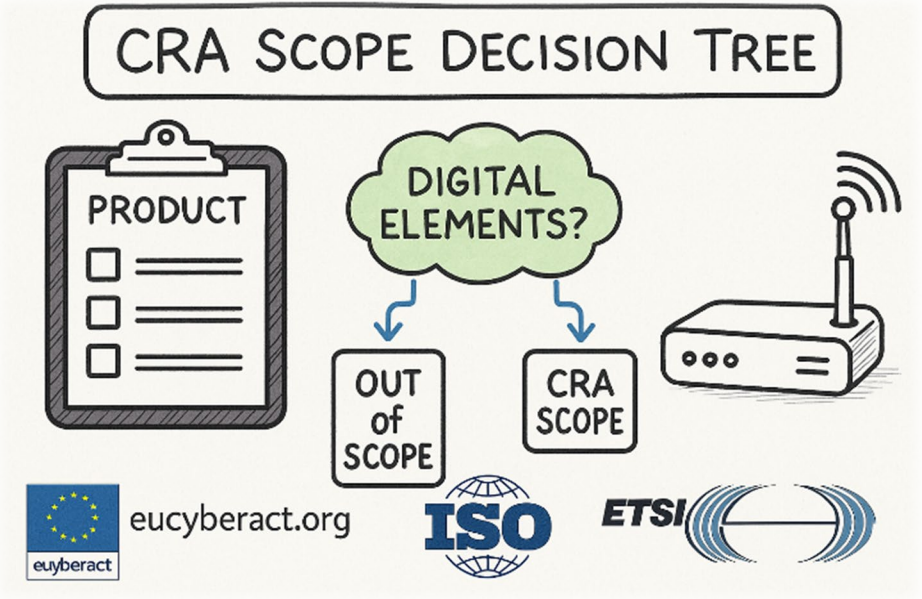
For hardware and software products to be placed on the market

- Conduct ***cybersecurity risk assessments***
- Ensure ***secure design, development & production***
- Implement ***vulnerability handling processes***
- Provide ***security updates*** for its components for at least five years or the expected product lifespan
- Maintain ***technical documentation***
- Ensure ***CE marking*** & ***declaration of conformity***
- ***Standardisation efforts*** to facilitate conformity

What is the CRA

Enhancing cybersecurity across digital products in the EU

- ✓ Horizontal cybersecurity regulation (Regulation (EU) 2024/2847)
- ✓ Applies to all "***products with digital elements***" placed on the EU market (Including ***remote data process solutions***)
- ✓ Aims to reduce vulnerabilities and enforce lifecycle security



CEN CENELEC Standardisation Efforts:PT#1 / #2 /#3

Work in progress for Horizontals

Project Team #1

High Level process **activities** to address the Total Product Life Cycle

Process activities such as security monitoring, risk assessment, verification, validation and release

Project Team #3

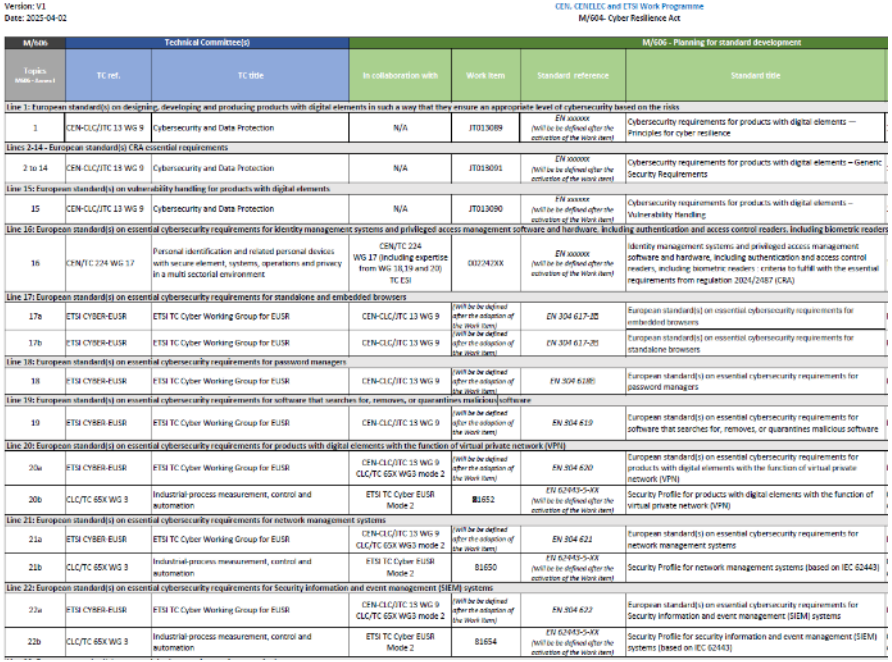
More detailed process **activities** with assessment criteria to address the vulnerability management requirements

Project Team #2

Mapping of the essential product requirements to the appropriate risk-based security controls

CEN, CENELEC and ETSI work programme

- ✓ [Lines: 20b, 21b, 22b, 25b, 27b, 36b]: Security for industrial automation and control systems - **Part 4-1**: Secure product development lifecycle requirements
- ✓ [Lines: 20b, 21b, 22b, 25b, 27b, 36b]: Security for industrial automation and control systems - **Part 4-2**: Technical security requirements for IACS components
- ✓ [Lines: 20b, 21b, 22b, 25b, 27b, 36b]: Security for industrial automation and control systems - **Part 3-3**: Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels



Version: V1
Date: 2025-04-02

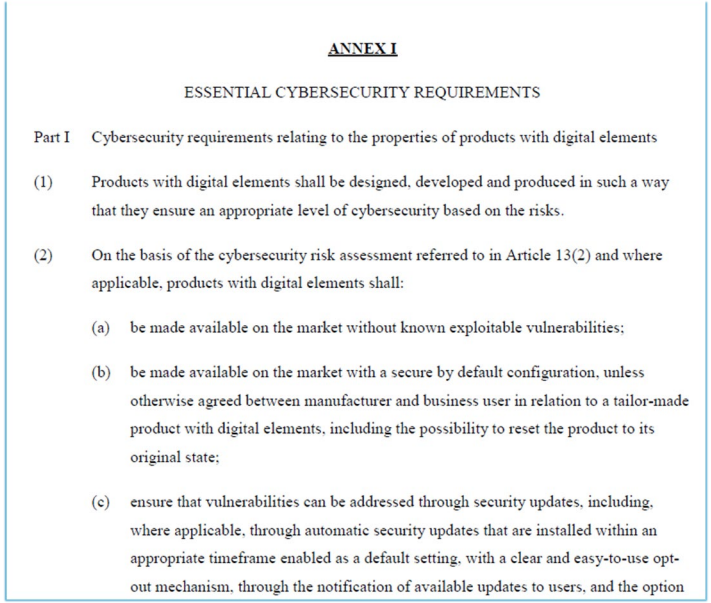
CEN, CENELEC and ETSI Work Programme
M/604- Cyber Resilience Act

M/606	Technical Committee(s)		M/606 - Planning for standard development			
Topics M606 – Annex I	TC ref.	TC title	In collaboration with	Work item	Standard reference	Standard title
Line 1: European standard(s) on designing, developing and producing products with digital elements in such a way that they ensure an appropriate level of cybersecurity based on the risks						
1	CEN-CLC/JTC 13 WG 9	Cybersecurity and Data Protection	N/A	JT013089	*EN xxxxxx (will be defined after the adoption of the Work item)*	Cybersecurity requirements for products with digital elements – Principles for cyber resilience
Lines 2-14 - European standard(s) CRA essential requirements						
2 to 14	CEN-CLC/JTC 13 WG 9	Cybersecurity and Data Protection	N/A	JT013091	*EN xxxxxx (will be defined after the adoption of the Work item)*	Cybersecurity requirements for products with digital elements – Generic Security Requirements
Line 15: European standard(s) on vulnerability handling for products with digital elements						
15	CEN-CLC/JTC 13 WG 9	Cybersecurity and Data Protection	N/A	JT013090	*EN xxxxxx (will be defined after the adoption of the Work item)*	Cybersecurity requirements for products with digital elements – Vulnerability Handling
Line 16: European standard(s) on essential cybersecurity requirements for identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers						
16	CEN/TC 224 WG 17	Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment	CEN/TC 224 WG 17 (including expertise from WG 18,19 and 20) TC ESI	00224720	*EN xxxxxx (will be defined after the adoption of the Work item)*	Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers : criteria to fulfill with the essential requirements from regulation 2024/2987 (CRA)
Line 17: European standard(s) on essential cybersecurity requirements for standalone and embedded browsers						
17a	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	CEN-CLC/JTC 13 WG 9	*(will be be defined after the adoption of the Work item)*	*EN 304 617-20*	European standard(s) on essential cybersecurity requirements for embedded browsers
17b	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	CEN-CLC/JTC 13 WG 9	*(will be be defined after the adoption of the Work item)*	*EN 304 617-30*	European standard(s) on essential cybersecurity requirements for standalone browsers
Line 18: European standard(s) on essential cybersecurity requirements for password managers						
18	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	CEN-CLC/JTC 13 WG 9	*(will be be defined after the adoption of the Work item)*	*EN 304 618*	European standard(s) on essential cybersecurity requirements for password managers
Line 19: European standard(s) on essential cybersecurity requirements for software that searches for, removes, or quarantines malicious software						
19	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	CEN-CLC/JTC 13 WG 9	*(will be be defined after the adoption of the Work item)*	*EN 304 619*	European standard(s) on essential cybersecurity requirements for software that searches for, removes, or quarantines malicious software
Line 20: European standard(s) on essential cybersecurity requirements for products with digital elements with the function of virtual private network (VPN)						
20a	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	CEN-CLC/JTC 13 WG 9 CLC/TC 65X WG3 mode 2	*(will be be defined after the adoption of the Work item)*	*EN 304 620*	European standard(s) on essential cybersecurity requirements for products with digital elements with the function of virtual private network (VPN)
20b	CLC/TC 65X WG 3	Industrial process measurement, control and automation	ETSI TC Cyber EUSR Mode 2	81652	*ETSI 62443-5-XX (will be be defined after the adoption of the Work item)*	Security Profile for products with digital elements with the function of virtual private network (VPN)
Line 21: European standard(s) on essential cybersecurity requirements for network management systems						
21a	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	CEN-CLC/JTC 13 WG 9 CLC/TC 65X WG3 mode 2	*(will be be defined after the adoption of the Work item)*	*EN 304 621*	European standard(s) on essential cybersecurity requirements for network management systems
21b	CLC/TC 65X WG 3	Industrial process measurement, control and automation	ETSI TC Cyber EUSR Mode 2	81650	*ETSI 62443-5-XX (will be be defined after the adoption of the Work item)*	Security Profile for network management systems (based on IEC 62443)
Line 22: European standard(s) on essential cybersecurity requirements for Security Information and event management (SIEM) systems						
22a	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	CEN-CLC/JTC 13 WG 9 CLC/TC 65X WG3 mode 2	*(will be be defined after the adoption of the Work item)*	*EN 304 622*	European standard(s) on essential cybersecurity requirements for Security Information and event management (SIEM) systems
22b	CLC/TC 65X WG 3	Industrial process measurement, control and automation	ETSI TC Cyber EUSR Mode 2	81654	*ETSI 62443-5-XX (will be be defined after the adoption of the Work item)*	Security Profile for security Information and event management (SIEM) systems (based on IEC 62443)

CRA Annex I – Essential Requirements

Horizontal requirements – very wide variety

- Secure by design & default
- Protection of confidentiality, integrity, availability
- Reduce attack surface
- Vulnerability management
- Data minimisation
- Logging and monitoring
- Incident mitigation
- Secure update mechanisms



ANNEX I

ESSENTIAL CYBERSECURITY REQUIREMENTS

Part I Cybersecurity requirements relating to the properties of products with digital elements

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.

(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:

(a) be made available on the market without known exploitable vulnerabilities;

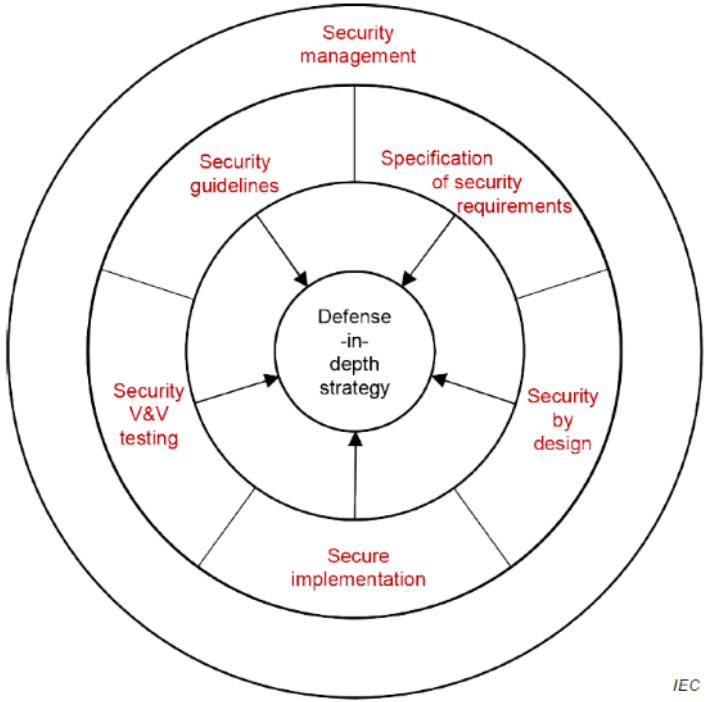
(b) be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;

(c) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option

IEC 62443-4-1 at a Glance

Security lifecycle requirements for OT Components & Systems

- 8 Practice Areas:
  - SM: Security Management
  - SR: Security Requirements Definition
  - SD: Secure Design
  - SI: Secure Implementation
  - SVV: Security Verification & Validation
  - DM: Defect Management
  - SUM: Security Update Management
  - SG: Security Guidelines



IEC

CRA–IEC 62443-4-1 Mapping Matrix

(Part 1)

CRA Requirement	62443-4-1 Practice ID
Risk-based design	SR-1 to SR-4
No known vulnerabilities	SVV1 to SVV-3, SUM 1-2
Secure defaults	SR-3, SD-1, SD-4
Vulnerability handling	SUM-1 to SUM-4
Access control	SR-4, SD-2, SI-1

CRA–IEC 62443-4-1 Mapping Matrix

(Part 2)

CRA Requirement	62443-4-1 Practice ID
Confidentiality	SD-4, SD-5, SD-7
Integrity	SD-2, SD-5, SI-2
Data minimisation	SR-1, SD-1, SD-7
Availability	SR-2, SI-1
Logging	SI-1, SI-2
Secure wipe	SUM-3, SD-7

EU Cyber Resilience Act

- Risk Management – Art 13 (functionality, connectivity, exposure, user type, market, tolerable risk)
- Process documentation (Art 53)
- Essential Requirements (Annex I)
- Due diligence – Art 13 (supplier trustworthiness)
- Vulnerability handling obligations (Art 13)
- Reporting obligations – Art 14
- Support throughout the product's lifecycle (Art 13)
- Instructions to users (Annex II, Annex VII)

Processes documented and updated

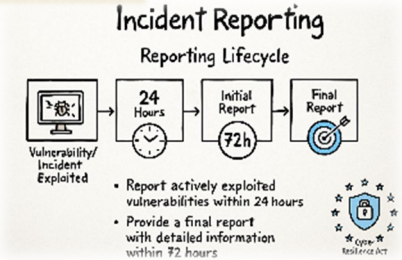
- Security Management
- Security Requirements
- Security Design Analysis
- Secure Implementation
- Verification & Validation
- Support period activities
- User information

IEC ISA EN 62443-4-1

- SM 1-13
- SR 1-5
- SD 1-4
- SI 1-2
- SVV 1-5
- DM 1-6
- SUM 1-5
- SG 1-7

Specific requirements for EU

Closing the gap with 62443-4-1



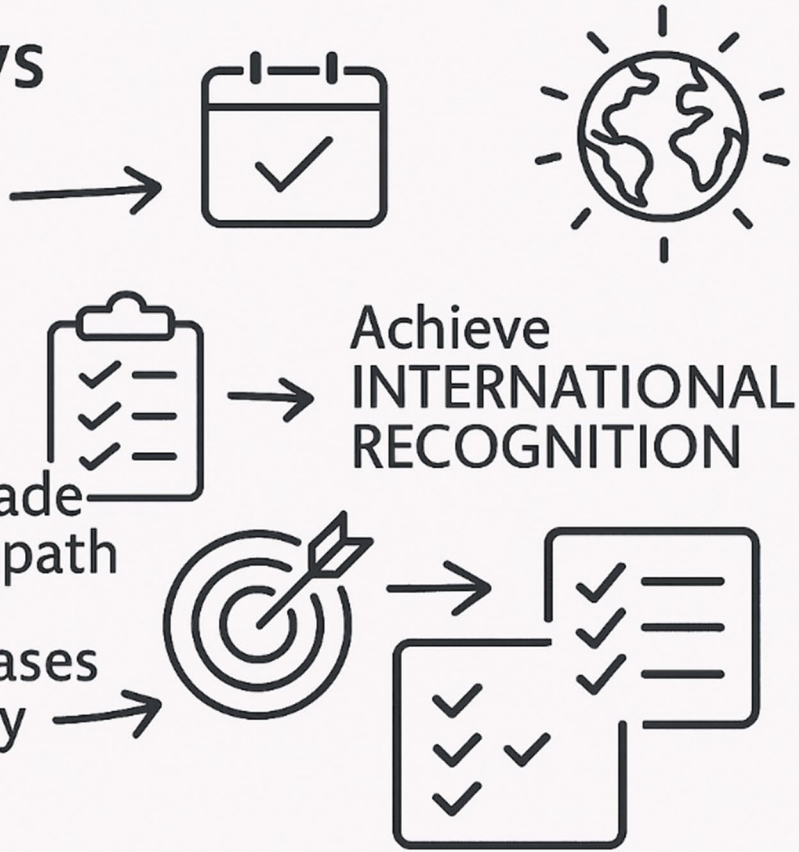
- ✓ ***SM-1*** – A general product development/ maintenance/ support process shall be documented and enforced including …***product description and requirements definition with requirements traceability***;
- ✓ ***SM-2*** – identify the organizational roles and personnel that are responsible for performing and completing them;
- ✓ ***SM-3*** – It is envisioned that a product supplier may apply this specification to selected products based on a number of factors, including the marketplace for which a product is intended and whether or not the product requires security to be built into the product and fully evaluated.
- ✓ ***SM-13*** – Continuous improvement, for the technical features and non-technical policies, processes and procedures.

Key takeaways

CRA introduces mandatory, lifecycle-wide security

IEC 62443-4-1 offers a ready-made implementation path

Early adoption eases future conformity assessments



Achieve INTERNATIONAL RECOGNITION

Manufacturers' obligations & Standardisation Efforts – CRA

Q&A?

Securing our digital world

Life Is On | Schneider Electric

se.com