Taiwan Section

CRA Countdown:

Bridging the gap between ISA/IEC 62443 and CRA

Michael Yao, ISA Taiwan Section
15 April 2025

Disclaimer

This gap analysis and recommended enhancement reflect my own personal view, and do not represent any official position of ISA or the ISA Taiwan Section.

Agenda

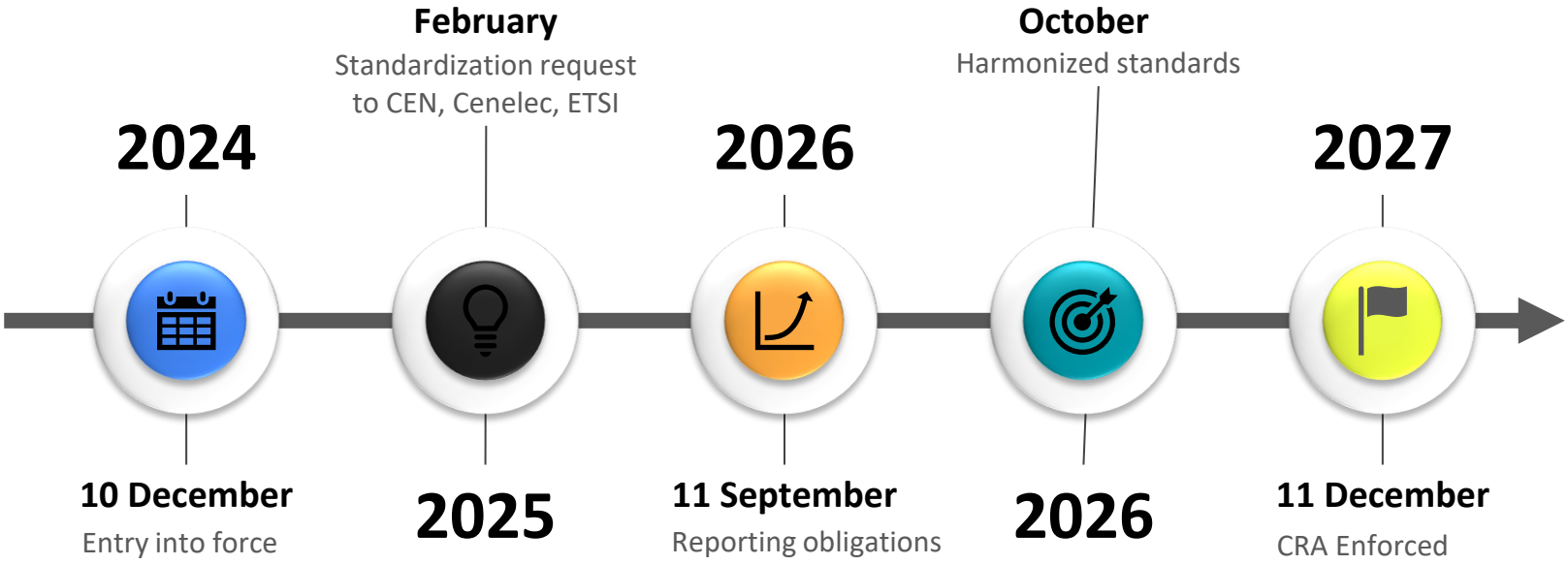
- **CRA Overview**
  - Main elements
  - Timeline
- **ISA/IEC 62443-4-1 & 62443-4-2 Recap**
- **Gap Analysis**
- **Key Takeaways**

CRA Main Elements

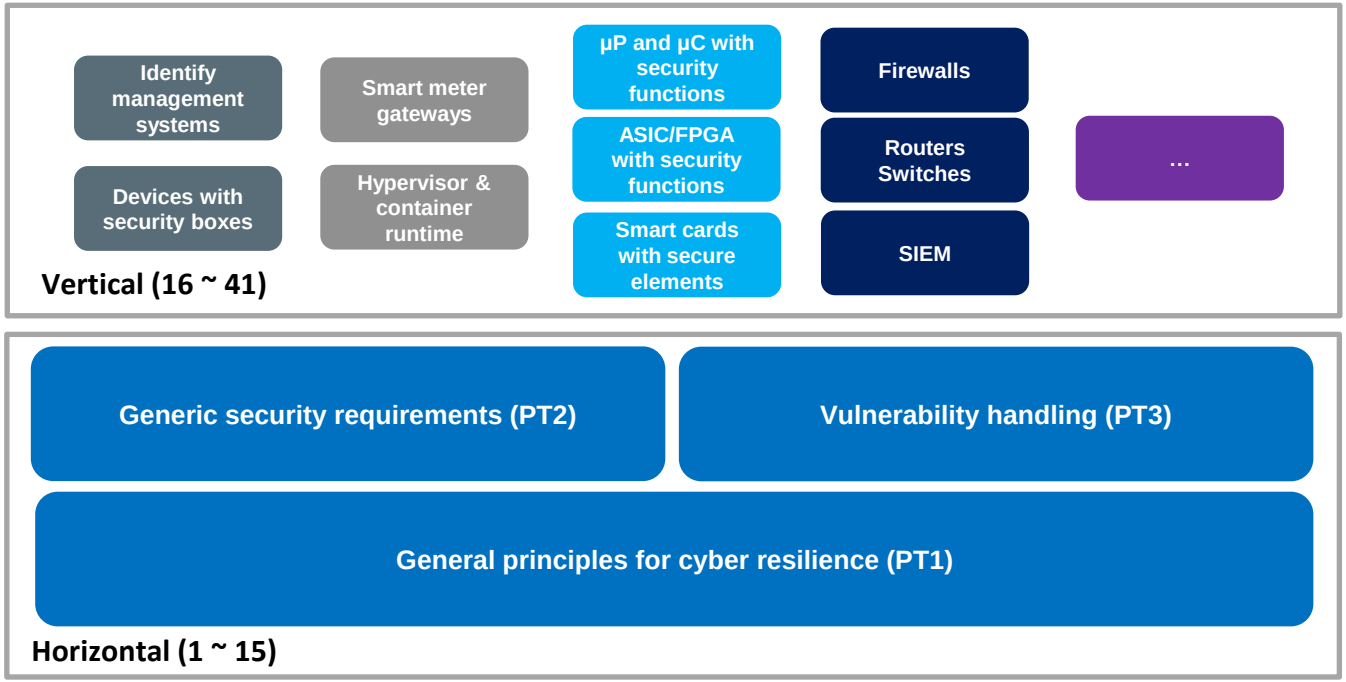
- **Cybersecurity rules** of placing products with digital elements on European markets
  - HW or SW products and their remote data processing solutions, including SW or HW components being placed on the market separately
- **Obligations** of manufacturers, importers and distributors
- Cybersecurity **essential requirements** across the product lifecycle on product itself and manufacturers' processes and policies respectively
  - Annex I Part 1: Requirements related to properties of products with digital elements
  - Annex I Part 2: Vulnerability handling requirements for manufacturers
- **Conformity assessment** for different product categories
  - **Harmonized standards** jointly developed by ESOs (CEN, CENELEC and ETSI)
- **Market surveillance and enforcement**

Ref: CEN/Cenelec webinar, "Standards supporting the Cyber Resilience Act", 2025-03-10

Timeline

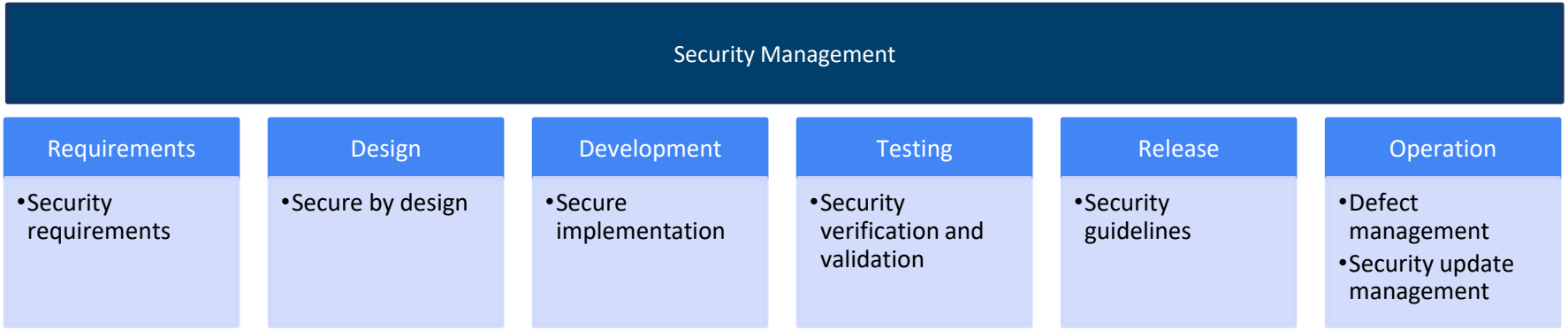


Harmonized Standards



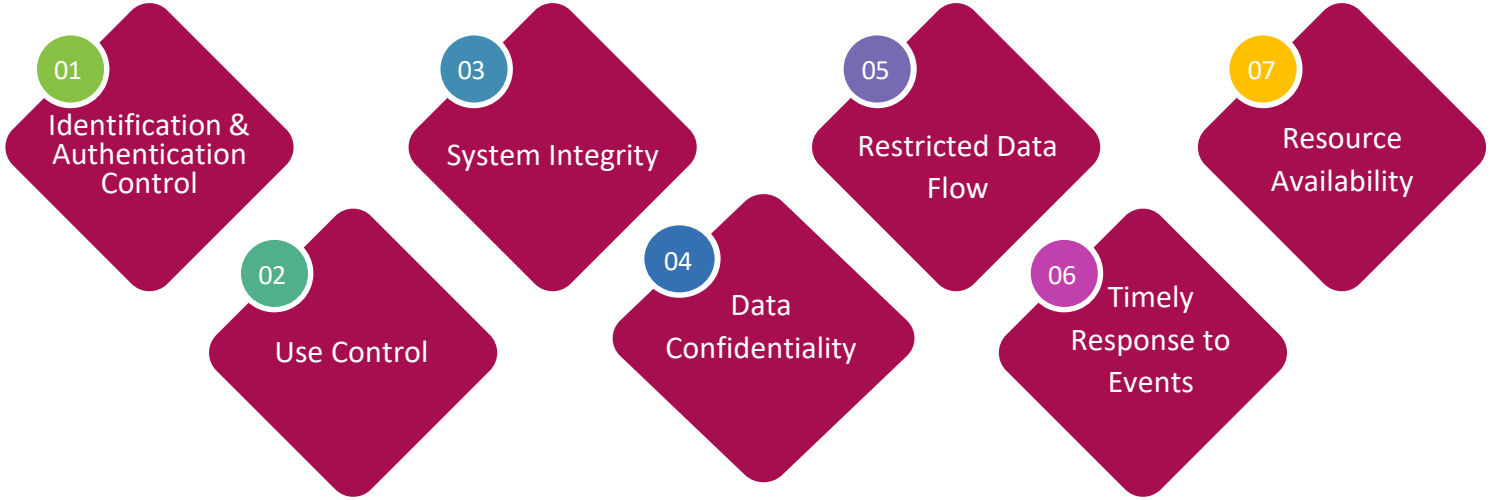
ISA/IEC 62443-4-1:

Secure Product Development Lifecycle



ISA/IEC 62443-4-2:

Technical Security Requirements for IACS Components



Essential Requirements vs ISA/IEC 62443

CRA Annex I Part 1	Description	Applicable ISA/IEC 62443 Requirements
1	Cybersecurity risk-based product development principles	**62443-4-2 SL1** CCSC 4: Software development process (62443-4-1)
2(a)	Without known exploitable vulnerabilities	**62443-4-2 SL1** CCSC 4: Software development process (62443-4-1)
2(b)	Delivered with secure by default configuration	**Refer to secure-by-default tactics in a joint initiative by CISA*** - Eliminate default password - Mandate MFA for privileged users - Secure logging (62443-4-2 CR 2.8) - Software authorization profile (62443-4-2 CR2.1) - Track and reduce “hardening guide” size - Consider user experience consequences of security settings

*Source: https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf, “Shifting the balance of cybersecurity risk: Principles and approaches for secure by design software”, October 25, 2023

Essential Requirements vs ISA/IEC 62443

CRA Annex I Part I	Description	Applicable ISA/IEC 62443 Requirements
2(c)	Vulnerabilities can be addressed through security update, and where applicable, through automatic security update	**1. 62443-4-2 SL1** System integrity (EDR 3.10, HDR 3.10, NDR 3.10) **2. Design notification mechanisms for users to decide whether and when to perform automatic update**
2(d)	Protect from unauthorized access and report unauthorized access	**62443-4-2 SL2** Identification and authentication (CR 1.1, CR 1.2) Use control (CR 2.8, CR 2.10)
2(e)	Protect the confidentiality of data	**62443-4-2 SL1** Data confidentiality (CR 4.1, CR 4.3)
2(f)	Protect the integrity of data against unauthorized manipulation and report on corruption	**1. 62443-4-2 SL2** System integrity (CR 3.1, CR 3.4, CR 3.5, EDR 3.10 RE1, HDR 3.10 RE1, NDR 3.10 RE1, EDR 3.11, HDR 3.11, NDR 3.11) **2. Enhance logs to record data corruption details**

Essential Requirements vs ISA/IEC 62443

CRA Annex I Part I	Description	Applicable ISA/IEC 62443 Requirements
2(g)	Process only data that are adequate, relevant and limited to what is necessary (data minimization)	**1. 62443-4-2 SL1** Use Control (CR 2.8) **2. Inform users what MINIMAL security related information will be logged**
2(h)	Protect the availability of essential and basic functions of the product	**62443-4-2 SL1** Resource availability (CR 7.1)
2(i)	Minimize the negative impact on the underlying services	**62443-4-2 SL2** Resource availability (CR 7.1 RE1)
2(j)	Limit attack surfaces	**1. 62443-4-2 SL1** CCSC 4: Software development process (62443-4-1) **2. Comply with 2(b) “Secure by default” requirement**

Essential Requirements vs ISA/IEC 62443

CRA Annex I Part I	Description	Applicable ISA/IEC 62443 Requirements
2(k)	Reduce the impact of an incident	**62443-4-2 SL1** CCSC 4: Software development process (62443-4-1)
2(l)	Record and monitor relevant internal activity with an opt-out mechanism	**1. 62443-4-2 SL1** Use Control (CR 2.8) **2. Allow users to control whether and when to enable or disable the recording and monitoring**
2(m)	Allow the permanent removal of data securely	**62443-4-2 SL2** Data confidentiality (CR 4.2)

Essential Requirements vs ISA/IEC 62443

CRA Annex I Part 2	Description	Applicable ISA/IEC 62443 Requirements
1	Identify and document vulnerabilities and components contained including to draw up a software bill of materials	**1. 62443-4-1** Security verification and validation (SVV-3, SVV-4) Defect management (DM-1 ~ DM-4) **2. Provide the SBOM in a well-accepted format, e.g. SPDX**
2	Address and remediate vulnerabilities with security updates promptly	**62443-4-1** Defect management (DM-2, DM-3, DM-4) Security update management (SUM-2 ~ SUM-6)
3	Regularly test and review the security of the product with digital elements	**62443-4-1** Security verification and validation (SVV-2 ~ SVV-4) Defect management (DM-4)
4	Disclose information about fixed vulnerabilities once a security update is available	**62443-4-1** Defect management (DM-5)

Essential Requirements vs ISA/IEC 62443

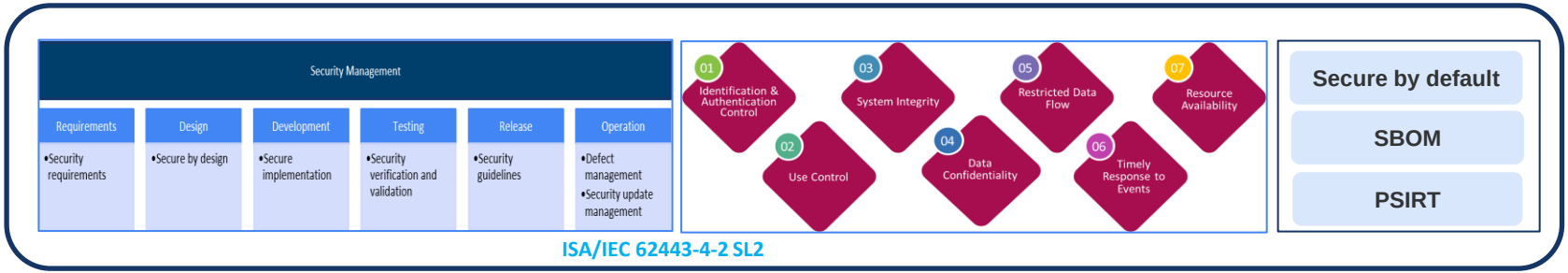
CRA Annex I Part 2	Description	Applicable ISA/IEC 62443 Requirements
5	Enforce a coordinated vulnerability disclosure policy	**1. 62443-4-1** Defect management (DM-1) **2. Refer to ETSI TR103 838** v1.1.1: "Cyber Security; Guide to Coordinated Vulnerability Disclosure“, 2022 -01
6	Facilitate the sharing of information about potential vulnerabilities and provide a contact address for reporting	**1. 62443-4-1** Defect management (DM-5) **2. Set up Product Security Incident Response Team (PSIRT) following industry best practices such as “PSIRT Services Framework**”**

**Ref: https://www.first.org, “Product Security Incident Response Team (PSIRT) Services Framework”, Version 1.1, Spring 2020

Essential Requirements vs ISA/IEC 62443

CRA Annex I Part 2	Description	Applicable ISA/IEC 62443 Requirements
7	Distribute updates securely	**62443-4-1** Security update management (SUM-4)
8	Distribute security patches free of charge along with the security advisories	**62443-4-1** Defect management (DM-5) Security update management (SUM-5)

Key Takeaways



Thank you

ISA Taiwan Section 企業贊助夥伴

PLATINUM Sponsor

| GOLD Sponsor

| SILVER Sponsor

ISA臺灣分會領英專頁