EU Cyber Resilience Act

Product Security Requirements for Digital Elements

OT Security Learning Series

Document 145 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

The Cyber Resilience Act (CRA) is an EU regulation establishing mandatory cybersecurity requirements for products with digital elements. Unlike NIS2, which regulates operators of essential services, the CRA targets manufacturers, importers, and distributors of hardware and software products. For OT environments, this means PLCs, RTUs, industrial sensors, and control system software must meet security requirements before being placed on the EU market.

The CRA addresses a fundamental gap in EU cybersecurity regulation: while NIS2 requires operators to secure their systems, the products they purchase often lack basic security features. The CRA shifts responsibility to manufacturers to build security into products from design through end-of-life.

For OT asset owners, the CRA will improve the baseline security of industrial products. For OT vendors and integrators, it creates new compliance obligations that affect product development, documentation, and support.

2 Scope and Applicability

2.1 Products with Digital Elements

The CRA applies to products with digital elements—any software or hardware product and its remote data processing solutions:

- **Hardware with Software** – PLCs, RTUs, industrial PCs, network equipment, sensors
- **Standalone Software** – SCADA software, HMI applications, engineering tools
- **Remote Data Processing** – Cloud components essential to product function

Figure 1: OT products covered by the CRA

2.2 Exclusions

The CRA does not apply to:

- Products already regulated by sector-specific EU legislation (medical devices, vehicles, aviation)
- Open-source software developed non-commercially
- Cloud services (covered by NIS2 instead)
- Products exclusively for national security or military use

2.3 Product Categories

Category	Description	OT Examples
Default	Standard products	Basic sensors, simple HMIs
Important Class I	Higher risk products	Firewalls, IDS, network management
Important Class II	Critical products	Operating systems, hypervisors
Critical	Highest risk	Industrial automation systems, smart meters

Table 1: CRA product risk categories

Warning

Industrial automation and control systems (IACS) are explicitly listed as “critical” products in Annex III of the CRA. This means stricter conformity assessment procedures apply to most OT products.

3 Essential Requirements

3.1 Security by Design

Manufacturers must ensure products meet essential cybersecurity requirements:

Requirement	Description
Risk Assessment	Cybersecurity risks identified and addressed in design
Secure by Default	Delivered in secure configuration; no default passwords
Access Control	Authentication and authorization mechanisms
Data Protection	Confidentiality and integrity of stored/transmitted data
Minimized Attack Surface	Only necessary functions enabled
Incident Mitigation	Security features to limit impact of incidents

Table 2: CRA essential security requirements

3.2 Vulnerability Handling

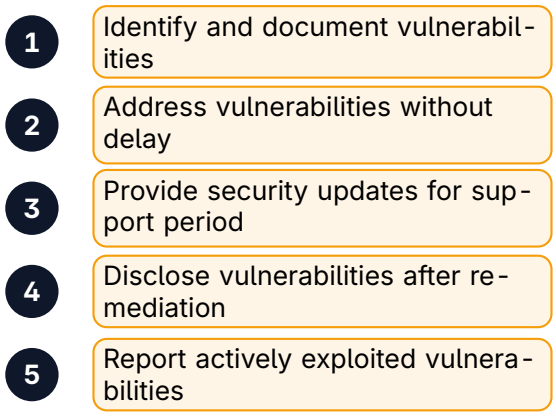

Figure 2: CRA vulnerability handling requirements

3.3 Support Period

Manufacturers must provide security updates for the entire support period:

- **Minimum 5 Years** – Or expected product lifetime, whichever is shorter
- **Free Security Updates** – At no additional cost to users
- **Separate from Features** – Security updates must be installable independently
- **Clear Communication** – End-of-support date must be stated at purchase

Tip

For OT products with 15–25 year lifecycles, the support period requirement creates significant obligations. Manufacturers must plan long-term support strategies or clearly communicate shorter support windows to buyers.

4 Obligations by Role

4.1 Manufacturers

Obligation	Details
Conformity Assessment	Demonstrate compliance through appropriate procedure
Technical Documentation	Maintain detailed security documentation
CE Marking	Affix CE marking when requirements met
EU Declaration	Issue declaration of conformity
Vulnerability Management	Establish and operate handling processes
Incident Reporting	Report exploited vulnerabilities within 24 hours
Cooperation	Assist market surveillance authorities

Table 3: Manufacturer obligations under the CRA

4.2 Importers and Distributors

- **Importers** – Verify manufacturer compliance, ensure documentation available, report non-compliance
- **Distributors** – Verify CE marking and documentation, report non-compliance, do not supply non-compliant products

4.3 Open Source Considerations

- Non-commercial open source development is excluded
- Commercial use of open source triggers CRA obligations
- "Open Source Software Stewards" (foundations) have lighter obligations
- Manufacturers using open source components remain responsible for compliance

5 Conformity Assessment

5.1 Assessment Procedures

Category	Procedure	Description
Default Products	Self-assessment	Internal control by manufacturer
Important Class I	Self or Third-party	Standards-based or notified body
Important Class II	Third-party required	EU-type examination
Critical Products	Third-party required	EU-type examination + certification

Table 4: Conformity assessment procedures by category

5.2 Harmonized Standards

Compliance with harmonized standards provides presumption of conformity:

- **IEC 62443 Series** – Expected to be referenced for industrial products
- **ISO/IEC 27001** – For organizational security management
- **Common Criteria** – For product security evaluation

Key Point

Organizations already implementing IEC 62443 for OT products will have a significant head start on CRA compliance. The CRA's essential requirements align closely with IEC 62443's security levels and secure development lifecycle.

6 Incident and Vulnerability Reporting

6.1 Reporting Requirements

Critical

The CRA introduces mandatory vulnerability and incident reporting to ENISA. Actively exploited vulnerabilities must be reported within 24 hours—a significant operational requirement for manufacturers.

Event	Timeline	Content
Exploited vulnerability	24 hours (early warning)	Basic information, impact
Exploited vulnerability	72 hours (notification)	Detailed technical info
Exploited vulnerability	14 days (final report)	Root cause, remediation
Severe incident	24 hours	Impact on product security

Table 5: CRA reporting timelines

7 Relationship with Other Regulations

Figure 3: CRA relationship with other EU regulations

- **NIS2** – CRA covers products; NIS2 covers their operators. Together they create end-to-end security requirements.
- **GDPR** – CRA data protection requirements align with GDPR for products processing personal data.
- **Machinery Regulation** – CRA applies alongside machinery safety requirements.

- **Radio Equipment Directive** – CRA supersedes RED cybersecurity provisions.

8 Timeline and Enforcement

8.1 Implementation Timeline

Date	Milestone
December 2024	CRA entered into force
September 2026	Reporting obligations apply
December 2027	Full application of all requirements

Table 6: CRA implementation timeline

8.2 Penalties

- **Essential Requirements** – Up to EUR 15 million or 2.5% of global turnover
- **Other Obligations** – Up to EUR 10 million or 2% of global turnover
- **False Information** – Up to EUR 5 million or 1% of global turnover
- **Product Recall** – Authorities can order withdrawal from market

9 Impact on OT

9.1 For Asset Owners

- Products will have better baseline security
- Security documentation will be available for procurement decisions
- Support periods and end-of-life dates will be clearly stated
- Vulnerability information will be more readily available

9.2 For Vendors and Integrators

- Secure development lifecycle becomes mandatory
- Vulnerability management processes required
- Long-term support commitments needed
- Third-party certification may be required
- Documentation requirements increase significantly

10 Summary

Key Takeaways

- **Product Focus:** The CRA regulates products with digital elements, complementing NIS2's focus on operators
- **OT Coverage:** Industrial automation systems are classified as "critical" products with stricter requirements
- **Security by Design:** Products must be designed securely, delivered in secure default configuration, with no default passwords
- **Vulnerability Handling:** Manufacturers must manage vulnerabilities and report exploited ones within 24 hours
- **Support Period:** Security updates required for minimum 5 years or product lifetime
- **Full Application:** December 2027; organizations should begin preparation now

11 Further Reading

Official Sources

- **EU Cyber Resilience Act** – Official regulation text
  https://eur-lex.europa.eu/eli/reg/2024/2847
- **European Commission CRA Page** – Overview and guidance
  https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

Standards

- **IEC 62443** – Industrial automation security (expected harmonized standard)
  https://webstore.iec.ch/publication/7029

Resources

- **ENISA** – EU Agency for Cybersecurity
  https://www.enisa.europa.eu/

Part of the OT Security Learning Series