ODVA®

TECHNOLOGY OVERVIEW SERIES

CIP Security: A Valuable Tool for CRA Compliance

AT A GLANCE

The EU Cyber Resilience Act (CRA) introduces comprehensive cybersecurity regulations for digital products in the EU, requiring compliance by December 11, 2027. Covering a broad range of products and markets including Operations Technology (OT), the CRA mandates strict security standards, vulnerability management processes, and robust documentation practices.

CIP Security™, an EtherNet/IP™ network extension, helps meet key regulatory obligations by leveraging industry standards like TLS, OpenID Connect, and strong encryption protocols. Specifically, CIP Security enhances protection against unauthorized access, ensures secure data transmission, and supports integrity mechanisms, aiding manufacturers in meeting CRA's cybersecurity mandates.

Introduction

The Cyber Resilience Act (CRA) mandates cybersecurity requirements for all "products with digital elements." This includes any hardware or software that processes digital data and connects to other digital systems. The extensive scope of CRA covers IT, IoT, industrial control systems (OT), embedded devices, machinery, and more.

Starting December 11, 2027, any digital product sold in the EU must adhere to the cybersecurity standards set by CRA. Even earlier, on September 11, 2026, manufacturers must have a process in place to report vulnerabilities and security incidents for their digital products. To indicate compliance, manufacturers must apply the CE mark, a certification already recognized for ensuring safety in various products, such as bicycles, wrist watches, and vacuum cleaners. This standardized approach aligns cybersecurity regulations across the EU, integrating digital products into existing harmonization laws.

For most digital devices and software, companies can conduct their own assessments to confirm compliance. Most products incorporating Common Industrial Protocol (CIP™) technologies will fall into this lowest risk category, allowing manufacturers to apply the CE marking independently. However, products with higher security risks (defined as Important Class I or Important Class II within CRA) must meet specific harmonized standards, and the most critical category (defined as Critical within CRA) will require independent third-party evaluation before being approved for sale.

By December 11, 2027, every digital product made available in the EU must adhere to the CRA, regardless of when it was originally developed or launched. This includes both existing products on the market and products available after that date.

The content and conclusions of this document are based on the information available regarding the CRA at the time of publication of this document. Harmonized standards are expected to be developed to support CRA implementation. Once these standards are published, varying interpretations of how the CRA will be applied in practice may lead to revisions of some of the details outlined in this document.

CRA Requirements

The Cyber Resilience Act (CRA) establishes fundamental cybersecurity obligations for all regulated products and their manufacturers. These essential requirements, outlined in Annex I of the regulation, will be frequently referenced in discussions on compliance.

The CRA’s requirements are divided into two main categories:

1. **Product Cybersecurity Requirements** – These define the security standards and inherent protective features that digital products must possess. The regulation specifies 13 functional requirements, but since the CRA is a legal framework rather than a technical manual, some guidelines may appear broad or open to interpretation.

2. **Vulnerability Management Requirements** – Manufacturers must implement processes to identify, report, and mitigate security vulnerabilities. This includes a structured vulnerability handling process, a responsible disclosure policy, and a mechanism for distributing security advisories and updates. Additionally, companies must maintain a Software Bill of Materials (SBOM) to help identify potential risks within their supply chain.

Beyond these core security and vulnerability requirements, the CRA imposes additional obligations on manufacturers:

- **Technical Documentation** – While not publicly available, this documentation must contain all relevant details to demonstrate compliance, including system specifications, threat models, intended use documentation, architectural diagrams, and test reports verifying security assessments.
- **End-User Documentation** – This documentation must be publicly accessible and must provide users with clear instructions to securely install, configure, and maintain the product. It is expected to be derived from the technical documentation.
- **Secure Development Practices** – The CRA mandates that products be designed, developed, and produced with an appropriate level of cybersecurity. Compliance is typically demonstrated by following industry-recognized secure development frameworks such as IEC 62443-4-1 or NIST 800-218.

CRA Compliant CIP Products

Starting December 11, 2027, manufacturers of industrial Ethernet devices, including EtherNet/IP products, must comply with the CRA to continue selling in the European market. This means adhering to the requirements outlined in the previous section, including documentation, development practices, and cybersecurity measures.

Manufacturers and vendors bear full responsibility for ensuring that Technical Documentation, End-User Documentation, and Secure Development Practices are integrated into the secure product development lifecycle. These processes must be tailored to the specific product, department, manufacturer, the product's intended use, and the company's development framework.

Regarding Vulnerability Management Requirements, the primary responsibility lies with the product manufacturer. Each vendor must establish a structured process for vulnerability reporting, management, disclosure, and the distribution of security advisories and updates. For vulnerabilities related to CIP technologies, ODVA has developed a vulnerability management framework that aligns with CRA requirements, ensuring that any identified weaknesses are addressed and disclosed appropriately.

While most of the 13 cybersecurity requirements listed in Annex I, Parts 1, 2, apply directly to product design and fall outside the scope of CIP technologies, four specific requirements are influenced by CIP technologies. These are detailed below, along with an explanation of how CIP technologies contribute to compliance. In all cases, CIP Security, an EtherNet/IP network extension, leverages widely adopted security standards such as TLS and OpenID Connect, as well as proven encryption algorithms.

Key CRA Requirements Addressed by CIP Security

1. **Secure by Default (Annex I, Part 1, 2b)**
   Requirement: “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;”
   CIP Security Contribution: The CIP Security Pull Model is designed to function automatically by default. Devices implementing this model can independently locate a certificate authority and request provisioning certificates. Once deployed, all security configurations can be automatically retrieved from a server and applied to the device. Furthermore, devices must have non-TLS/DTLS ports disabled by default. End users may enable these non-secure EtherNet/IP ports later, based on their risk assessment, using the TCP/IP Interface Object. Port 44818/UDP, used for ListIdentity, can likely remain open by default, as it is solely intended for device identification purposes.

2. **Protection Against Unauthorized Access (Annex I, Part 1, 2d)**
   Requirement: “ensure protection from unauthorized access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorized access;”
   CIP Security Contribution: CIP Security offers multiple layers of protection against unauthorized access. The EtherNet/IP Confidentiality Profile supports authentication via both certificates and pre-shared keys, using mutual TLS. Additionally, for enhanced security, the CIP Security User Authentication Profile enables Role-Based Access Control and allows integration with external identity providers.

3. **Confidentiality of Transmitted Data (Annex I, Part 1, 2e)**
   Requirement: “protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state-of-the-art mechanisms, and by using other technical means;”
   CIP Security Contribution: CIP Security ensures secure data transmission using TLS and DTLS protocols, requiring AES encryption - a globally trusted standard. Users can configure cipher suites based on security needs, though all CIP Security-compliant devices must support confidentiality measures. While CIP Security secures data in transit, encryption for stored data falls under the manufacturer’s responsibility.

4. **Integrity of Transmitted Data (Annex I, Part 1, 2f)**
   Requirement: “protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorized by the user, and report on corruptions;”
   CIP Security Contribution: Data integrity within CIP Security is ensured through TLS and DTLS, with all cipher suites defined by CIP Security incorporating strong integrity protections via SHA-based HMACs. Additionally, specific data elements - such as digital certificates and access tokens - are further protected using digital signatures. While CIP Security provides robust integrity measures for data in transit, ensuring data integrity at rest is the manufacturer’s responsibility.

For a more in-depth discussion on CIP Security’s role in meeting CRA requirements, see https://www.odva.org/library_proceedings/eu-cyber-resilience-act-compliance-in-industrial-automation-ensuring-readiness-for-cip-devices/.

Summary / Conclusion

The CRA introduces comprehensive cybersecurity regulations for digital products in the EU, requiring compliance by December 11, 2027. Covering a broad range of products and markets including Operations Technology (OT), the CRA mandates strict security standards, vulnerability management processes, and robust documentation practices.

Manufacturers are responsible for implementing secure development processes, maintaining technical and end-user documentation, and ensuring proper vulnerability handling mechanisms.

For CIP products, including EtherNet/IP, compliance with CRA requirements is critical. CIP Security helps meet key regulatory obligations by leveraging industry standards like TLS, OpenID Connect, and strong encryption protocols. Specifically, CIP Security enhances protection against unauthorized access, ensures secure data transmission, and supports integrity mechanisms, aiding manufacturers in meeting CRA’s cybersecurity mandates. As the enforcement date approaches, companies must proactively align their cybersecurity frameworks with CRA requirements to maintain market access and enhance digital resilience across industrial automation and connected systems.