EU Cyber Resilience Act Compliance in Industrial Automation: Ensuring Readiness for CIP Devices

Jack Visoky
Principal Engineer & Security Architect, Rockwell Automation

Brian Batke
Engineering Fellow, Rockwell Automation

Jegajith P.T
Chief Technology Officer, Utthunga

Nithin S.P
EU Business Head, Utthunga

Chatrapathi G.V
Technical Director - Industrial Connectivity, Utthunga

Presented at the ODVA
2025 Industry Conference & 23rd Annual Meeting
March 19, 2025
Clearwater Beach, Florida, USA

As the European Union's Cyber Resilience Act (EU CRA) moves towards enforcement deadlines, vendors of industrial products face increasing pressure to ensure their products comply with cybersecurity requirements. This regulation emphasize the need for robust cybersecurity measures in industrial products, particularly focusing on communication protocols and secure development practices.

CIP (Common Industrial Protocol) Security plays a crucial role in securing Industrial Control Systems (ICS), offering confidentiality, integrity, authentication, and non-repudiation. The implementation of CIP Security involves key aspects such as device identity management, secure communication protocols, and vulnerability mitigation, which are essential for compliance with the EU CRA.

This paper explores CIP Security within the context of the EU CRA regulation, highlighting how it can be used as a cybersecurity technology to meet the imposed requirements. It identifies challenges faced by vendors in achieving compliance and discusses technology available to CIP-connected devices that can be used to meet various EU CRA requirements. Additionally, it surveys the functional requirements of Annex I Part 1 of the EU CRA.

The paper aims to serve as a key resource for industrial suppliers and machine builders navigating the evolving regulatory landscape, ensuring operational security, risk management, and long-term security of connected devices in industrial environments.

I. Introduction

i. EU Cyber Resilience Act

The European Union's Cyber Resilience Act (EU CRA) is a landmark regulation aimed at enhancing the cybersecurity of connected devices within the EU market. The bulk of the regulation is scheduled for enforcement by December 2027, although some aspects come into force before then. The EU CRA mandates that manufacturers of hardware, software, and digital services must identify and mitigate cybersecurity risks throughout the product lifecycle. This includes implementing secure development practices, maintaining continuous compliance, and ensuring that products remain resilient against evolving cyber threats. The act is designed to protect users and systems from potential cyberattacks, promoting a safer digital environment across various industries. Furthermore, the act identifies certain functional requirements for products to meet, laid out in Annex I.

ii. CIP Devices & EU Cyber Resilience Act

EtherNet/IP and Common Industrial Protocol (CIP) are widely used in the industrial space, according to a study by HMS, as of 2024 these protocols are used in 21% of industrial network nodes [5]. The EU CRA plays a pivotal role for devices using EtherNet/IP in industrial automation. The EU CRA mandates the integration of comprehensive cybersecurity measures, including secure communication protocols, device authentication, and vulnerability management, to meet compliance standards. By aligning with these regulations, device manufacturers not only provide capabilities to shield their devices from potential cyber threats but also foster greater trust and reliability within industrial automation systems.

iii. Cyber Resilience Act Significance for CIP Devices

Coming into effect in December of 2027, vendors do not have much time to ensure they are complying with this act. Given the short timeframe it is important for vendors to analyze the act in detail to understand how it affects their products. There are many aspects of this act, but some of the highly impactful aspects are the functional requirements given in Annex I, Part 1, clauses (1) and (2). This section of the legislation lays out specific requirements to which products must comply. For many EtherNet/IP devices, CIP Security can and should be used to meet many of these requirements.

Before getting into specifics regarding CIP Security, it is important to keep in mind the text in (1) and (2) of Annex I. The text in (1) states:

> 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.

This text is important but somewhat generic. It does not give any specific requirements regarding what a product must support or any types of protections. That said, for a product supporting EtherNet/IP, CIP Security provides the strongest cybersecurity protection for the EtherNet/IP communication. Therefore, it is likely that this clause itself implies support for CIP Security for many EtherNet/IP products.

In (2) of Annex I, there is some text that precedes the enumerated requirements, which states:

> Based on the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:

Again, this text is generic, but the important point is that all of the requirements enumerated as part of (2) of Annex I are subject to a cybersecurity risk assessment. This means that each product must undergo a risk assessment to determine applicability of a given requirement. Therefore, it is not possible for this paper to provide universal guidance that applies to all EtherNet/IP products, as the risk assessment and intended use will vary between EtherNet/IP products. However, this paper can provide some generic guidance regarding risks and mitigations, as it applies to EtherNet/IP.

After this first clause of (2) describing a risk assessment, the rest of (2) describes 13 requirements, enumerated as (a) through (m). As mentioned, each of these requirements will need to be evaluated for how they pertain to a given product based on cybersecurity risk. However, four of these requirements likely have a strong tie-in to CIP Security and the functionality that the various profiles provide.

II. CIP Security in CIP Devices for EU CRA Compliance

The different facets of CIP Security are explored with regard to their mapping to EU CRA requirements.

i. Secure by Default

The first requirement with strong applicability to CIP Security is in Annex I, Part 1, 2(b), and the subject of it is making sure a product is shipped in a “secure by default” configuration. The full text of Annex I, Part 1, 2 (b) is as follows:

> 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;

The first thing to note is that the text in Annex I, Part 1, 2(b) regarding secure by default does not provide a lot of details regarding what is required to meet this. To that end, the following discussion presents a possible path for meeting secure by default for a CIP Security capable EtherNet/IP device. That said, this discussion exists at a snapshot in time and was based on current understanding of this requirement. As more is revealed the arguments here may need to be adjusted. Nevertheless, the hope is this provides some interesting thoughts on a possible path to compliance of the secure by default requirement.

The Pull Model (see Figure #1) operates automatically and by default on compliant devices, allowing them to independently locate a certificate authority and request a certificate for provisioning. While additional settings are needed to fully configure CIP Security, the certificate request can act as a trigger to deploy the complete security configuration to the device. There are already commercial solutions available that facilitate this process (for example, FactoryTalk™ Policy Manager), enabling full security configuration for an EtherNet/IP Pull Model device by default. It is important to note that devices typically can't be pre-configured with security settings tailored to a specific user, as they are generally produced for broader use and might be deployed across various environments and by various end users. Therefore, some user intervention is necessary for security setup. The CIP Security Pull Model simplifies this by allowing the device to automatically, and by default, initiate and complete the necessary steps for security configuration.

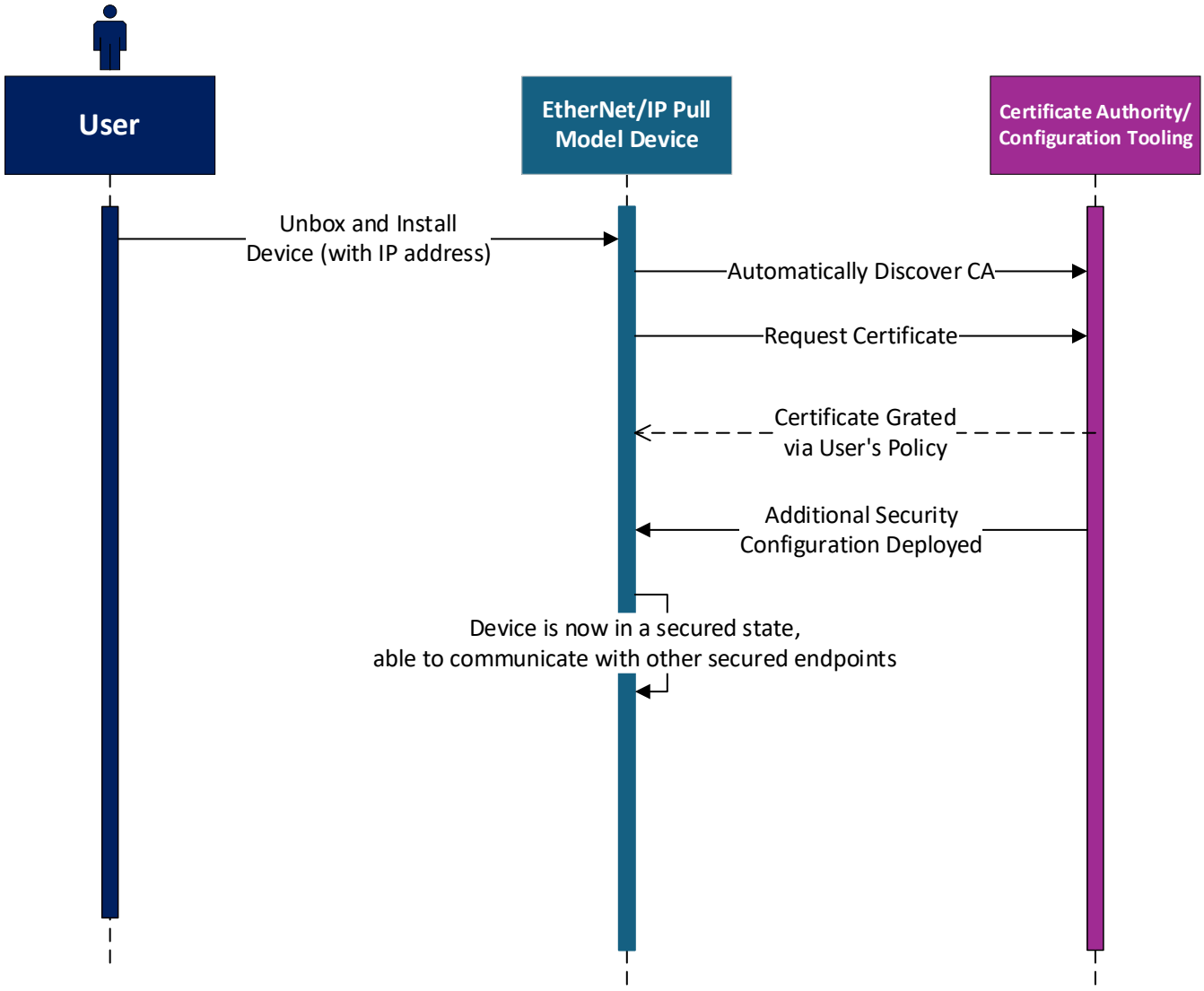

Figure 1. *Example workflow for Secure by Default with EtherNet/IP Pull Model Profile*

The CIP Security Pull Model is not mandatory for all CIP Security devices, yet implementing this profile will of course be important for the secure by default requirement.

Devices in a networked system need to trust other devices and/or software to perform their essential functions; an EtherNet/IP device would of course need some provisioning of trust to properly function. As such, it is not feasible for a device to simply power up with all the security configuration necessary for runtime communication, rather there needs to be one or more steps towards provisioning, and these steps need to be performed by default, which is exactly what the Pull Model does. However, there may still be a question about a device that does not find an EST server via the Pull Model and therefore is not configured for security. In this case the user has elected to install the device in a network without an EST server, and by doing so is making a decision to override the default behavior of the device. This is allowed via the EU CRA, as the user ultimately can make their own decision about what level of security is appropriate.

Devices must ship in a secure by default state and close all non-essential ports and services by default, which very impacts the EtherNet/IP ports without TLS/DTLS cannot be turned on by default. One port that does not use TLS/DTLS is 44818/UDP. In the case of 44818/UDP, this port is only used for very limited

functionality, mainly around device discovery, which in many plants is an essential function. Therefore, the risk of 44818/UDP being open is likely low, and it is reasonable to ship devices with this port open. The other EtherNet/IP ports that do not support TLS/DTLS are 44818/TCP, 2222/TCP and 2222/UDP. These ports do not support TLS/DTSL but support the general EtherNet/IP functionality. These ports will very likely need to be closed by default and require an explicit user action to enable them. That action could be via a software configuration tool that opens them using the TCP/IP Interface Object, or a hardware-based configuration (e.g. a physical switch on the product). The CIP Security Pull Model can also help with this, as it executes by default and can be used to automatically deliver security configuration including certificates and port state. The default execution of the Pull Model provides a mechanism for only secure functionality to be enabled. That is, once Pull Model executes and identity and trust are provisioned the device is in the appropriately secured state as determined by the user. Before this occurs, the device is essentially in an open state, so if the user choses they may enable the EtherNet/IP ports that don't have TLS/DTLS support, either via the Pull Model or via a different mechanism. The main point is that for the non-TLS/DTLS ports to be opened the user must take some explicit action; for ease of use this action can be tied to the CIP Security Pull Model and its operation.

A device may support multiple protocols beyond EtherNet/IP, and in such cases, similar security measures may be needed for those protocols, particularly if they pose significant risks as determined by the cybersecurity risk assessment (e.g. protocols that are used to control an industrial process might carry particular risk). One approach could be to disable these additional protocols by default, allowing them to be activated only by an authorized user. For protocols based on TCP and UDP, this can be managed through the CIP TCP/IP Interface Object. Once CIP Security is configured, access to this object is authenticated, enabling secure activation of other protocols. This method provides a simple way for an EtherNet/IP device to comply with the EU CRA's secure by default requirements, even when it supports other potentially high-risk protocols.

ii. Unauthorized Access

The next requirement relevant for CIP Security is in Annex I, Part 1, 2(d) and is the subject of preventing unauthorized access to the product. The full text of Annex I, Part 1, 2 (d) is as follows:

> ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and **report on possible unauthorized access;**

CIP Security offers several mechanisms to safeguard against unauthorized access. The EtherNet/IP Confidentiality Profile supports both certificates and pre-shared keys (PSKs), which can be authenticated through mutual TLS. Both options provide robust cryptographic protection to prevent unauthorized access. Users have the flexibility to choose which method to implement and where to manage trust. For many EtherNet/IP devices, this approach is likely sufficient.

The CIP Security Resource Constrained Profile is designed for low-end devices, enabling the use of one or more pre-shared keys (PSKs) for establishing trust. These PSKs are verified through mutual authentication during the DTLS handshake. Despite the limited capabilities of these devices, PSKs offer strong protection against unauthorized access. Ultimately, the adequacy of this protection depends on the cybersecurity risk assessment, but for many constrained devices, it is likely to be sufficient.

In some cases, the cybersecurity risk assessment may indicate that additional protections are necessary to prevent unauthorized access beyond just certificates and PSKs. The CIP Security User Authentication Profile offers an extra layer of defense by enabling Role-Based Access Control (RBAC) on EtherNet/IP devices and allowing integration with external Identity Providers. This aligns well with requirements related to identity and access management systems, as the profile supports integration with any OpenID Connect identity management system. For highly complex devices frequently accessed by multiple users with varying responsibilities, the cybersecurity risk assessment may determine that RBAC, which is provided by CIP Security User Authentication Profile, is a robust mitigation strategy.

Regarding the text in Annex I, Part 1, 2(d) about reporting unauthorized access, while the CIP specification includes error codes for such events, additional logging and reporting mechanisms are likely needed. Various options are available, including storing logs directly on devices. However, Syslog offers an appealing alternative, as it integrates seamlessly with many security monitoring services and solutions. Although Syslog is not currently a standardized component of CIP Security, it has been discussed at various ODVA forums and could potentially be incorporated in the future. In the meantime, vendors are encouraged to explore reporting options and consider Syslog as a viable solution and ODVA is also encouraged to consider standardizing Syslog as a new CIP Security Profile.

iii. Confidentiality of Transmitted Data

The next requirement relevant for CIP Security is in Annex I, Part 1, 2(e) and is the subject of data confidentiality The full text of (e) is as follows:

> 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;

This paper will focus specifically on data in transit, as data stored within a product fall outside the scope of CIP Security and depend on the product's design. However, it is worth noting that data can be encrypted through software mechanisms. Furthermore, many embedded hardware platforms offer partial or full encryption for stored data, which could be utilized in this context. Additionally, the product might employ physical methods to protect data at rest, such as internal and inaccessible non-volatile memory.

CIP Security (Figure #2) enhances data confidentiality for EtherNet/IP by utilizing well-established encryption algorithms. The CIP Security EtherNet/IP Confidentiality Profile employs TLS and DTLS, requiring support for AES encryption, a globally trusted standard for safeguarding data. The Resource Constrained Profile also uses DTLS and supports both AES and ChaCha20, another highly regarded encryption algorithm. These algorithms are included in cipher suites within TLS and DTLS and offer strong protection for the confidentiality of EtherNet/IP data during transmission. Users have the flexibility to choose which cipher suites to enable and may even opt for ciphers that do not provide confidentiality if desired, although the capability for data confidentiality is required for all CIP Security compliant devices. Ultimately, while CIP Security provides the tools for robust data protection, the choice of which measures to implement depends on the user's assessment of cyber risk.

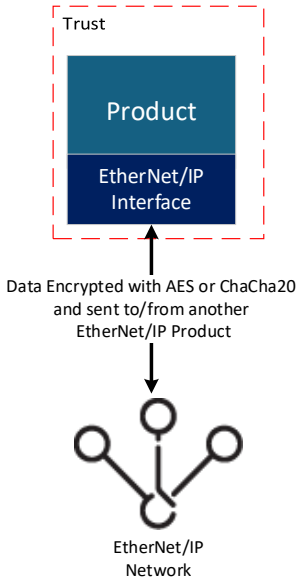

Figure 2. *Trust for Data Confidentiality*

iv. Integrity of Transmitted Data

The final requirement relevant for CIP Security is in Annex I, Part 1, 2(f) and is the subject of data integrity The full text of Annex I, Part 1, 2(f) is as follows:

> protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions;

This requirement closely resembles the previous one concerning data confidentiality, with the added inclusion of "commands, programs, and configuration." While both requirements still fall under the scope of a cybersecurity risk assessment, the expanded list in the data integrity requirement suggests that most data should be protected with integrity measures. The discussion here will once again focus on data in transit, specifically EtherNet/IP. While there are well-established methods for protecting data integrity at rest within a product, numerous options are available.

Data integrity is safeguarded through TLS and DTLS within CIP Security (Figure #3), with all the cipher suites required by the EtherNet/IP Confidentiality Profile offering strong integrity assurances via the SHA HMAC. Similarly, the cipher suites mandated by the CIP Security Resource Constrained Profile also guarantee data integrity, but through Poly1305 and AES-GCM authenticated encryption.

Even though the TLS/DTLS transport provides data confidentiality and data authenticity protections, it is important to note that some data has specific protections beyond the secure transport provided by TLS and DTLS. For instance, digital certificates used to establish the TLS and DTLS session, or Access Tokens in the User Authentication Profile, are individually protected by digital signatures, ensuring the integrity of this data. These mechanisms further enhance protection for critical information, forming the foundation for the security of the protocols themselves.

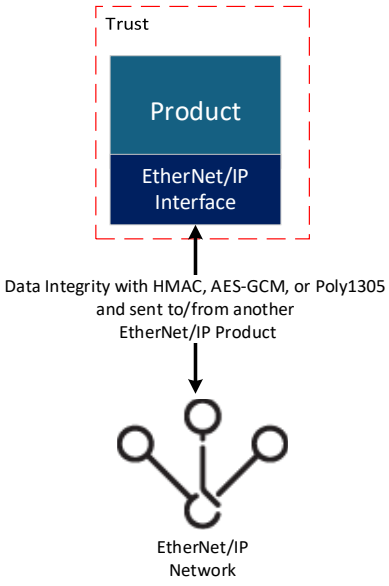

Figure 3. *Trust for Data Integrity*

III. EU CRA Compliance Beyond CIP Security

i. Overview

As noted in this paper's Introduction, Annex I of the EU CRA contains a set of requirements that apply to "products with digital elements." Section II of this paper outlines how CIP Security can enable devices to meet some of the requirements related to network communication of the EU CRA. ODVA vendors should however be aware of the additional requirements that must be met in order to comply with the EU CRA.

The following subsections present a summary of the Annex I requirements, with brief commentary on the potential implications for ODVA devices. More detailed analysis is required in order to more fully guide vendors in achieving EU CRA compliance. It is beyond the scope of this paper to fully analyze all of the EU CRA requirements in detail at this time. Note that there are requirements around technical documentation in Annex II and Annex VII, however these are not discussed in this paper.

ii. Appropriate Level of Security

Requirement

(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.

Implications

Vendors should perform risk assessments and threat models of their products in order to determine the appropriate level of cybersecurity that is needed. Volume 8 (CIP Security) of the CIP Networks Specification is a good starting point, as it includes a threat model for CIP Security. Vendors also need to consider risks based on the industry segments and applications in which their products are used, and to consider threats beyond those addressed by CIP Security.

iii. Known Vulnerabilities

Requirement

(2)(a) [products shall] be made available on the market without known exploitable vulnerabilities;

Implications

Vendors should implement a vulnerability awareness and tracking process, specifically applied to their own products, and also as applied to technology (network protocols, SDKs, operating systems, etc.) that their products incorporate. ODVA can in the future assist by providing a CIP vulnerability reporting and tracking process. Note that ODVA conformance test does not perform penetration testing on devices. To this end vendors must ensure they are taking responsibility for penetration testing and monitoring for vulnerabilities in any components they use, like a TLS library.

iv. Secure by Default

Requirement

(2)(b) [products shall] 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;

Implications

Section II of this paper describes "secure by default" in the context of CIP Security. Vendors should also apply "secure by default" to any other protocols or interfaces that their devices support. For example, a device with an embedded web server should have HTTPS enabled by default with a process to bootstrap initial security for HTTPS.

v. Security Updates

Requirement

(2)(c) [products shall] ensure that vulnerabilities can be addressed through security updates […];

Implications

Vendors need a mechanism by which they can update firmware and/or software in their devices or applications. It is assumed that ODVA vendors already provide this capability. To meet EU CRA requirements, firmware/software updates need to be done in a secure manner (i.e., following requirements for authorization, integrity, confidentiality, etc.).

vi. Unauthorized Access

Requirement

(2)(d) [products shall] ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;

Implications

Refer to Section II for a discussion of CIP Security in the context of preventing unauthorized access. Vendors should also be aware to apply this to any protocols or interfaces in addition to CIP (e.g., HTTPS).

vii. Confidentiality of Stored, Transmitted, or Processed Data

Requirement

(2)(e) [products shall] 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;

Implications

Refer to Section II for a discussion of CIP Security in the context of confidentiality of transmitted data. For stored or processed data, vendors need to evaluate the risks and attack vectors that are relevant to their products. For example, stored customer or application data may need to be encrypted, which can potentially be provided via the product's hardware platform.

viii. Integrity of Stored, Transmitted, or Processed Data

Requirement

(2)(f) [products shall] protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions;

Implications

Similar to data confidentiality, refer to Section II for a discussion of CIP Security for transmitted data. For stored or processed data, vendors need to evaluate the risks and attack vectors that are relevant to their products.

ix. Data Minimization

Requirement

(2)(g) [products shall] process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product […];

Implications

This requirement is more difficult to apply to CIP-based products and needs to be evaluated by vendors on a per-product basis. For example, the requirement could be interpreted to mean that a product should not storing customer application information or user authentication information beyond what is explicitly needed by the application.

x. Essential Function Availability

Requirement

(2)(h) [products shall] protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;

Implications

Protections provided by CIP Security contribute to protecting essential and basic function availability. There are additional considerations that vendors may need to address. At a minimum, in the event of a DoS attack such as a network storm, devices should not fault such that they require a restart to continue to function. Note that the EU CRA does not precisely define “availability of essential and basic functions”. Vendors will first need to define the “essential and basic functions” for their devices. In addition futher investigation is needed in order to know more precisely what “protecting the availability” means in practice (e.g., as a certification body would interpret it). It may be that devices may require explicit measures to mitigate the effects of DoS attacks such as network storms and resource exhaustion attacks, e.g., via rate limiting.

xi. Minimize Negative Impact

Requirement

(2)(I) [products shall] minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;

Implications

Vendors should ensure that the product itself cannot be used as an attack vector in the system, e.g., via triggering of a storm of traffic or other unnecessary or unwanted communications. Products should limit their connections or communications to only that which is necessary for the application. This could result in the need to allow users to disable certain functions such as network discovery.

xii. Limit Attack Surface

Requirement

(2)(j) [products shall] be designed, developed and produced to limit attack surfaces, including external interfaces;

Implications

Vendors should disable any non-essential TCP and UDP ports and/or other services and interfaces, by default, and require the user to explicitly enable any that are non-essential.

xiii. Reduce Impact of an Incident

Requirement

(2)(k) [products shall] be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;

Implications

Vendors should consider mitigation mechanisms that could be put in place to minimize impact in the event of the device being compromised. For example, unauthorized access by one user account should not allow an attacker to compromise other accounts or data. This requirement could

be considered related to a number of other requirements. E.g., by providing confidentiality and integrity of data, impact of an incident can be reduced.

xiv. Recording and Monitoring

Requirement

(2)(l) [products shall] provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user;

Implications

Products need to have some form of secure logging capability used to record actions especially as they relate to security capabilities and activities. A recommended solution is to use Syslog, as it is widely supported and used in the IT space.

xv. Secure Reset

Requirement

(2)(m) [products shall] provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.

Implications

The CIP Identity Object already includes the Reset service, which allows a device to be returned to its factory-default settings. It may also be necessary, depending on the product and application, to ensure complete erasure of any stored application data or settings in embedded memory.

xvi. Vulnerability Handling Requirements

Part II of Annex I contains requirements of manufacturers with respect to managing vulnerabilities. It is beyond the scope of this paper to examine each of the vulnerability-handling requirements. In summary, device vendors will need to establish a formal process to:

- Identify and document known vulnerabilities,
- Address and remediate any vulnerabilities,
- Provide for software and/or firmware updates that address reported vulnerabilities,
- Regularly test and review devices for security vulnerabilities,
- Disclose and communicate information about reported vulnerabilities to end users.

IV. CONCLUSION

As the EU's Cyber Resilience Act (EU CRA) approaches enforcement deadlines, industrial product vendors must prioritize cybersecurity to ensure compliance with this important regulations. CIP Security plays a pivotal role in protecting CIP-connected devices and Industrial Control Systems (ICS), providing essential features like confidentiality, integrity, authentication, and non-repudiation. By adhering to the principles of secure by default, ensuring data confidentiality and integrity during transmission, and minimizing unnecessary data exposure, manufacturers can safeguard against unauthorized access and mitigate cyber risks.

Furthermore, it is important to note that although CIP Security can be used to meet some of the EU CRA requirements, there are requirements which are not within the scope of a communication protocol like EtherNet/IP with CIP Security. Vendors will need to perform a cybersecurity risk assessment to determine all of the necessary features and technology for ensuring compliance to all requirements in the EU CRA. To assist with this, part III of this paper provides an introductory discussion of the Annex I Part 1

requirements and how they might apply to an EtherNet/IP device. However, each device will have its own specific nuances which need to be accounted for by the vendor.

In summary, by leveraging CIP Security mechanisms for compliance with the EU CRA, industrial product vendors can meet regulatory requirements, protect critical infrastructure, and ensure the long-term security of their connected devices in increasingly complex industrial environments. Although this is not the only work that is needed for a given product, it does represent significant technological solutions to meeting the requirements of the EU CRA..

V. REFERENCES

[1] ODVA, The CIP Networks Library, Volume 1: Common Industrial Protocol, Ann Arbor: ODVA, Inc., 2001-2024.
[2] ODVA, The CIP Networks Library, Volume 2: EtherNet/IP Adaptation of CIP, Ann Arbor: ODVA, Inc., 1999-2024.
[3] ODVA, The CIP Networks Library, Volume 8: CIP Security, Ann Arbor: ODVA, Inc., 1994-2024.
[4] EU CRA http://data.europa.eu/eli/reg/2024/2847/oj
[5] Industrial network market shares 2024 according to HMS Networks https://www.hms-networks.com/news/news-details/17-06-2024-annual-analysis-reveals-steady-growth-in-industrial-network-market

Keywords
EU CRA; CIP Security; CIP Connected Devices; Regulatory Compliance; Device Identity Management; Patch Management; Access Control; Encryption