30 YEARS!
2025 ODVA
Industry Conference and 23rd Annual Meeting

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

Jack Visoky, Brian Batke, Jegajith P.T, Nithin S.P, Chatrapathi G.V

Introduction

- The EU Cyber Resilience Act (CRA) goes into effect in December 2027
- The EU CRA places a number of requirements vendors who sell products in the EU, including industrial automation devices
- CIP Security can help to meet some EU CRA requirements. Vendors will also need to address requirements not met by CIP Security.

1st Takeaway: EtherNet/IP-enabled devices must meet EU CRA requirements in order to be sold in the EU after December 11, 2027

2nd Takeaway: Good luck selling an EtherNet/IP product in the EU without CIP Security!

Risk Assessment

- Annex I provides specific requirement text, broken down into clauses
  - Part (1) talks about products ensuring “an appropriate level of cybersecurity based on the risks”
  - Part (2) gives specific requirements, but they are preceded by the saying “On the basis of the cybersecurity risk assessment”
- Main point is that each product needs to have a risk assessment performed, “one size fits all” guidance cannot be given
- That said, some generalizations can be made that will likely apply to most EtherNet/IP Products

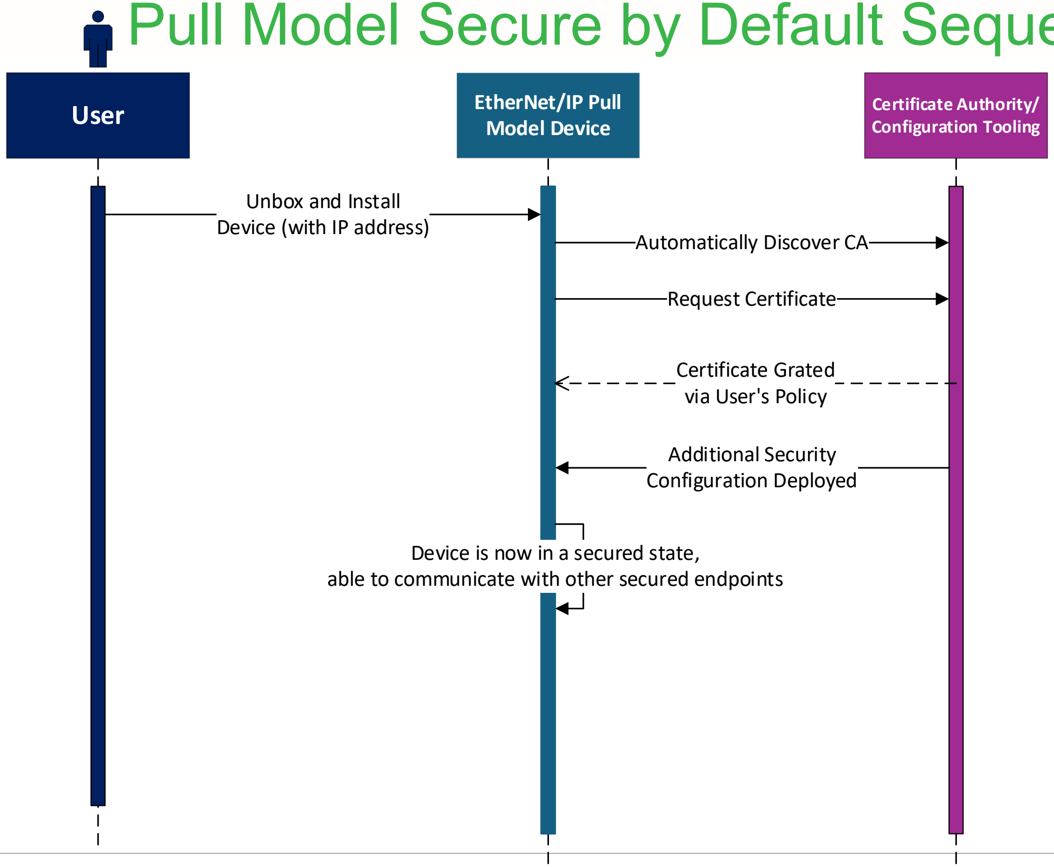
Main Requirements for CIP Security

- Four requirements in (2) of Annex I have a strong tie in to CIP Security
  - Secure by Default
  - Protection against Unauthorized Access
  - Data Confidentiality
  - Data Integrity
- Note: if a product supports protocols other than EtherNet/IP, then similar analysis needs to be done for those other protocols

Secure by Default

- This requirement states products “be made available on the market with a secure by default configuration…”
- EtherNet/IP Pull Model can help!
  - Pull Model runs automatically and by default
  - Pull Model discovers a CA and requests a certificate and trust anchor
  - Other CIP Security configuration can be sent as part of this interaction (using Pull Model as a trigger)
- Essentially, a user can unbox a device, place it on the network and have it automatically and by default get security configured appropriate to their system
- However, non-secure ports will still need to be accounted for (e.g. closed by default, as per risk assessment), TCP/IP Interface Object can help management
  - Basic analysis: probably can leave 44818/UDP open for discovery as this is an “essential function”, but 44818/TCP and 2222/TCP and 2222/UDP will have to be closed

Pull Model Secure by Default Sequence Diagram


User
EtherNet/IP Pull Model Device
Certificate Authority/ Configuration Tooling
Unbox and Install Device (with IP address)
Automatically Discover CA
Request Certificate
Certificate Grated via User's Policy
Additional Security Configuration Deployed
Device is now in a secured state, able to communicate with other secured endpoints

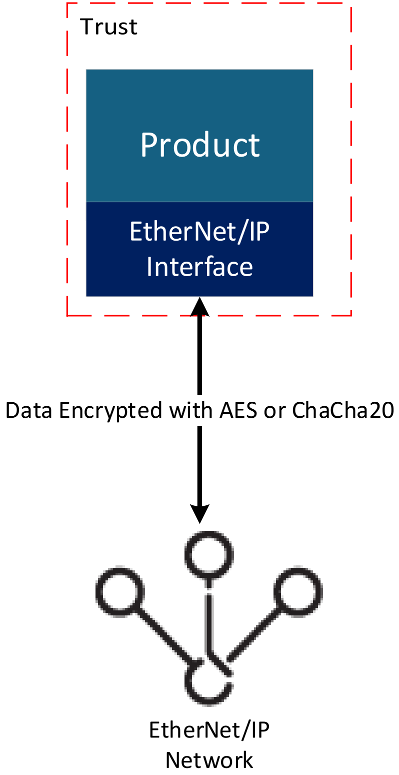
Assumes that non-secured ports are closed until security is configured (exception of udp/44818, which enables discovery)

Protection Against Unauthorized Access

- This requirement states "ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems…"
- TLS and DTLS with mutual authentication use PSKs or Certificates to authenticate endpoints
  - Provided in the EtherNet/IP Confidentiality Profile and the CIP Security Resource Constrained Profile
- But maybe that still isn't enough?!
  - CIP Security User Authentication Profile adds Role-Based Access Control and integration into an OpenID Connect Provider
  - Whether or not this is necessary is of course based on the Cybersecurity Risk Assessment

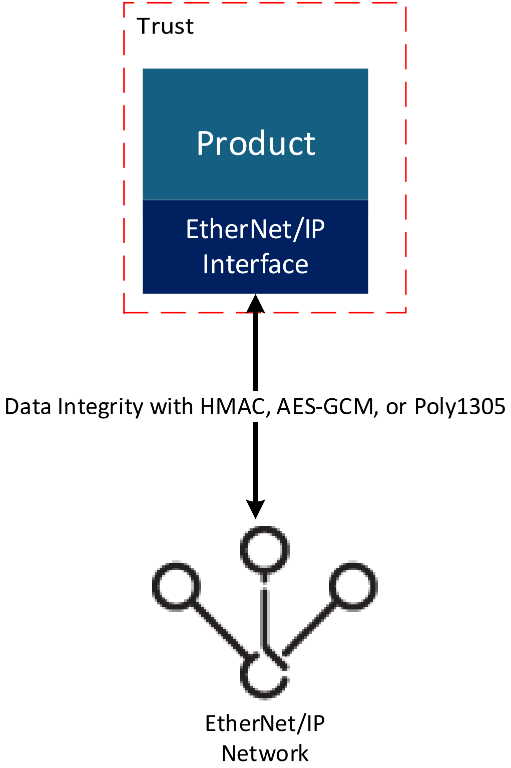
Data Confidentiality

- This requirement states “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;”
- Consider transmitted data (EtherNet/IP)
- TLS and DTLS provide this
- EtherNet/IP Confidentiality Profile requires support for AES cipher suites
- CIP Security Resource Constrained Profile support for AES cipher suites and ChaCha20 cipher suites



Data Integrity

- This requirement states “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…”
  - Note this is very similar to the previous requirement
  - Also note the additional text; this implies more data is to have integrity protections
- All required TLS/DTLS cipher suites provide cryptographic integrity protections for EtherNet/IP Confidentiality Profile and for CIP Security Resource Constrained Profile
  - HMAC, AES-GCM, and Poly1305



Appropriate Level of Security

- This requirement 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”
- Vendor impact:
  - Leverage the cybersecurity risk assessment for the product
  - Each product will be unique
  - Volume 8 has a sample Threat Model for an EtherNet/IP Product with CIP Security
  - Risk assessment needs to consider product functions in addition to EtherNet/IP

Known Vulnerabilities

- This requirement states, “[products shall] be made available on the market without known exploitable vulnerabilities”
- Vendor impact:
  - Vendor responsibility to be aware of known vulnerabilities (e.g., in protocols, operating system, network stack, etc.)
  - ODVA can help; we will provide a CIP vuln reporting/tracking process
  - Good practice to perform penetration testing
  - Note: ODVA Conformance Test is NOT a penetration test!

Security Updates

- This requirement states, “[products shall] ensure that vulnerabilities can be addressed through security updates”
- Vendor impact:
  - Out of scope for ODVA
  - Vendors need to provide the ability to do a secure software/firmware update
  - Likely needs Authorization, Integrity, Confidentiality, etc.

Data Minimization

- This requirement states “[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”
- Vendor impact:
  - Analyze their products and ensure that only the necessary data is processed
  - Not storing customer application information beyond what is strictly necessary

Essential Function Availability

- This requirement states, “[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”
- Vendor impact:
  - Questions remain on how to interpret this requirement, in practice. Further investigation is needed
  - Identify the product’s “essential and basic functions”
  - Ensure that the product recovers from any DoS attacks
  - May need to implement additional mechanisms such as network bandwidth filtering

Minimize Negative Impact

- This requirement states, “[products shall] minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks”
- Vendor impact:
  - Analyze product behavior with respect to communications the product may initiate (both CIP and non-CIP)
  - Limit connections/communication to only what is necessary
  - Ensure the product cannot be used as an attack vector (e.g. cannot trigger a network traffic storm)

Limit Attack Surface

- This requirement states, “[products shall] be designed, developed and produced to limit attack surfaces, including external interfaces”
- Vendor impact:
  - Disable any non-essential TCP and UDP ports
  - Disable any non-essential services or functions
  - Require the user to explicitly enable non-essential ports and services

Reduce Impact of an Incident

- This requirement states, “[products shall] be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques”
- Vendor impact:
  - Consider mitigation mechanisms that could be put in place
  - E.g., event logging that can be monitored by a security monitoring system
  - E.g., raise an alarm or shutdown if the device is able to detect that it has been compromised

Recording and Monitoring

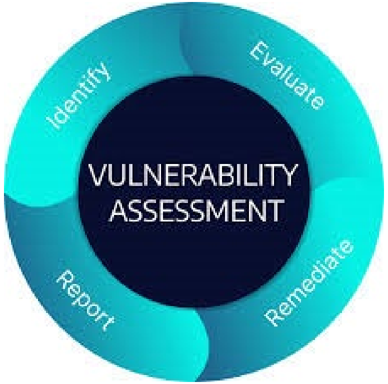
- This requirement states, “[products shall] provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user”
- Vendor impact:
  - Products likely need some form of logging of events especially as related to security
  - E.g., setting of security configuration, but may also include user access logs
  - Syslog is one possible solution; may require on-device log as well

Secure Reset

- This requirement states, “[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”
- Vendor impact:
  - Identity Object already includes the Reset service (return to factory default)
  - May be necessary to ensure complete erasure of stored application data or settings. This is a practical impossibility for many existing devices. Needs further investigation.

Vulnerability Handling

- Part II of Annex I contains requirements of manufacturers with respect to managing vulnerabilities
- Vendor impact:
  - Device vendors will need to establish a formal process to:
    - Identify and document known vulnerabilities,
    - Address and remediate,
    - Provide for software and/or firmware updates,
    - Regularly test and review devices for security vulnerabilities,
    - Disclose and communicate information about reported vulnerabilities to end users



Summary

- The EU CRA has the potential to prevent a product from being sold
- Most important: do a detailed Cybersecurity Risk Assessment
- Close second most important: adopt CIP Security
  - Use the Risk Assessment to determine which profile(s) are appropriate
- For the Annex I requirements:
- Secure by Default:
  - EtherNet/IP Pull Model Profile & close/manage ports (TCP/IP Interface Object)
- Protection Against Unauthorized Access:
  - EtherNet/IP Confidentiality Profile
  - CIP Security Resource Constrained Profile
  - CIP Security User Authentication Profile
- Data Confidentiality:
  - EtherNet/IP Confidentiality Profile
  - CIP Security Resource Constrained Profile
- Data Integrity:
  - EtherNet/IP Confidentiality Profile
  - CIP Security Resource Constrained Profile

Summary

- For the remaining Annex I requirements:
  - Product risk assessment is step 1
  - Requirements need to be assessed and applied on a per-product basis
  - Most of the requirements are good practices that should be in place regardless of EU CRA
  - May need new capabilities such as logging, network traffic filtering
  - Vendors will need a vulnerability management process

30 YEARS!

2025 ODVA

Industry Conference and 23rd Annual Meeting