

How to deliver cybersecure EIP device(s) – A practical approach for EU CRA compliance

Sven Giesecke, CodeWrights GmbH

October 21, 2026

Agenda



01	About CRA
02	Industrial Automation
03	Risk Based Approach
04	Examples
05	Apply

© 2026 ODVA, Inc.
All rights reserved.
Classified as Business

CRA - Regulation (EU) 2024/2847

- **Mandatory** EU cybersecurity requirements for hardware and software products throughout their life cycle
- **Guidelines** when bringing products or software to the EU market
- Ensure that products have fewer security vulnerabilities, and that manufacturers, importers, and distributors **properly manage cybersecurity**



© 2026 ODVA, Inc.
All rights reserved.
Classified as Business

Why should I comply to CRA regulation?



- It is about the risks …
  - production stop in your customer's facility
  - harming you company's public value or reputation
  - not being able to sell your products in the EU

- and there are regulatory fines:
  - Severe Non-Compliance - up to €15 million or 2.5% of the company's total worldwide annual turnover
  - Providing Misleading Information:
    up to €5 million or 1% of the company's worldwide turnover for **supplying incorrect, incomplete, or misleading information to authorities**.

© 2026 ODVA, Inc.
All rights reserved.
Classified as Business

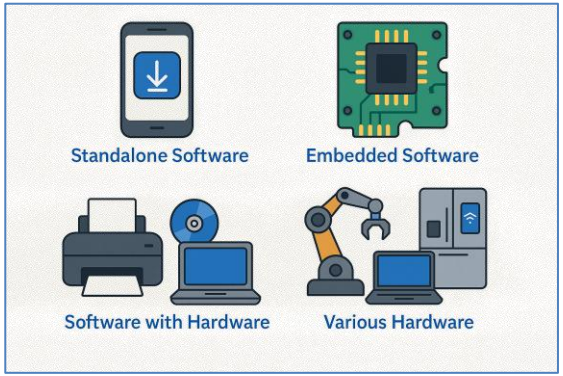
Timeline



© 2026 ODVA, Inc.
All rights reserved.
Classified as Business

Which products fall under the CRA?

- The CRA applies to “products with digital elements made available on the market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network”



➢ In Scope



➢ Not in Scope

© 2026 ODVA, Inc.

All rights reserved.
Classified as Business

Product or Product Type?

- A manufacturer developed a product type before the CRA applies, can he continue to manufacture products identical to that type after the CRA applies?

  - **The CRA applies to individual products, and not product types.**
  - Products that are manufactured according to a type that is not compliant with the CRA **cannot be placed on the market** on or after **December 11th 2027**, even if the first instance of that product "type" has been placed on the market before.

© 2026 ODVA, Inc.
All rights reserved.
Classified as Business

Latest Updates (June 2026)

- A horizontal **standard** will specify CRA **requirements** across products, written by CEN/CENELEC Committee JTC13, WG9 with the goal to be ready on October 2026 (harmonized norm)
  - EN 40000-1-1—Vocabulary
  - EN 40000-1-2—Principles, Product Risk Management, and Lifecycle Activities (corresponds to CRA Annex I, Part I, No. 1)
  - EN 40000-1-3—Vulnerability Handling (corresponds to CRA Annex I, Part II)
  - EN 40000-1-4—Generic Security Requirements (corresponds to CRA Annex, Part I, No. 2)

- **Wireless?** The cybersecurity requirements of the Radio Equipment Directive Delegated Act (RED-DA will be repealed with effect on December 11, 2027— the same day the Cyber Resilience Act (CRA) comes into force.
  The background is that products covered by the Radio Equipment Directive also fall under the CRA—and the CRA contains much more extensive cybersecurity requirements. So there would have been an overlap.

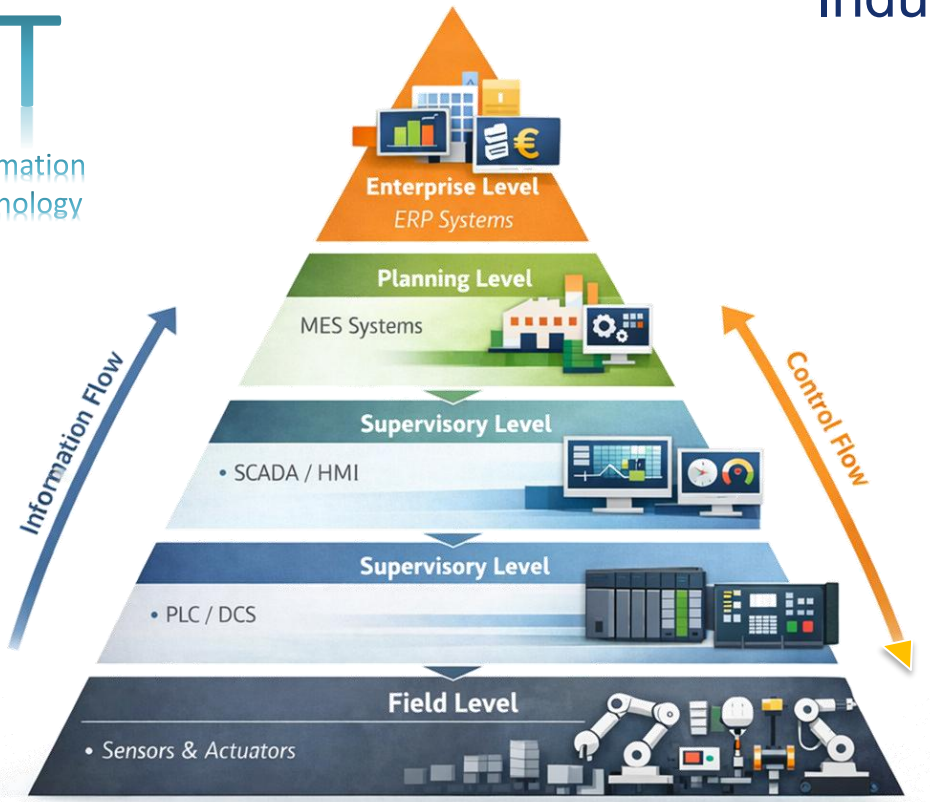
© 2026 ODVA, Inc.
All rights reserved.
Classified as Business

Industrial Automation

IT
Information Technology

Convergence

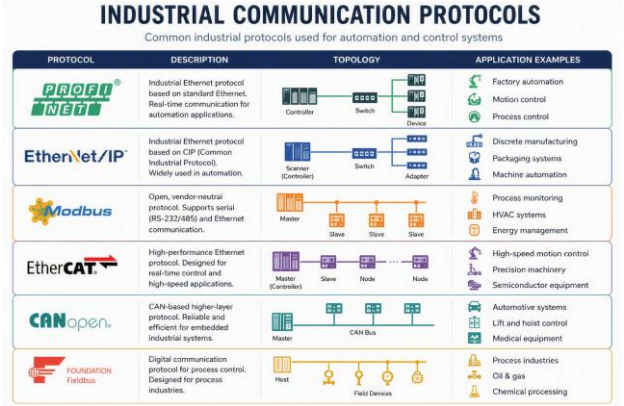
OT
Operational Technology



© 2026 ODVA, Inc.

All rights reserved.
Classified as Business

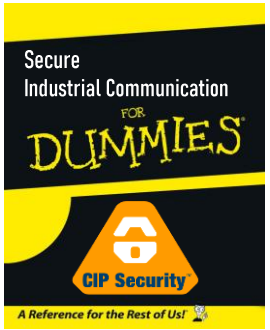
Industrial Communication



- Enable interoperable, real-time control
- Most were not originally designed with cybersecurity in mind
- Many deployments lack built-in security mechanisms

❖ **Easy Advise: Use Secure Industrial Communication ☺**

➢ **EtherNet/IP (CIP Security)**



© 2026 ODVA, Inc.
All rights reserved.
Classified as Business

Guidance by the Industrial Security Harmonization Group

• Secure Deployment of Industrial Communication Protocols - A Risk Management Based Approach (Release 2026)	Simon Merklin PI
• Whitepaper FAQ on Industrial Ethernet Security Concepts (2022)	Joakim Wiberg ODVA
• Whitepaper Common IA IDevID Requirements (Release 2025)	Randy Armstrong OPC Foundation
• Whitepaper Authentication in the OT-Environment (Release 2025)	Frank Fengler FCG

© 2026 ODVA, Inc.
All rights reserved.
Classified as Business

Cybersecurity for Industrial Automation and Control Systems (IACS)

- **IEC 62443-4-1 Secure Product Development Lifecycle (SPDL)**
- **IEC 62443-4-2 Secure Product (Component) Requirements**

- IEC 62443-4 defines secure development life-cycle (SDL) requirements related to cyber security for products intended for use in the industrial automation and control systems environment
- The life-cycle description includes security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management and product end-of-life

© 2026 ODVA, Inc.
All rights reserved.
Classified as Business



…Now Into Practice….As a Manufacturer, what should I be doing now with all this… ?

Assess Industrial Cybersecurity

Product, Environment and Processes



We have to go through these steps…

© 2026 ODVA, Inc.

All rights reserved.
Classified as Business

Review Product In Scope

- Are we developing a **new product ?**
- Or do we want to **continue to ship** an existing product?

- How far is my organization developed for **secure development principles**?

- How do we **classify** the product?
- Can we use a **secure** industrial communication **protocol**?

Remember: individual products, not types!

© 2026 ODVA, Inc.
All rights reserved.
Classified as Business

Establish the Security Context

The Security Context describes the environment and all security relevant aspects of a system. It includes assumptions that refer to the security of the system or asset.

Goal:

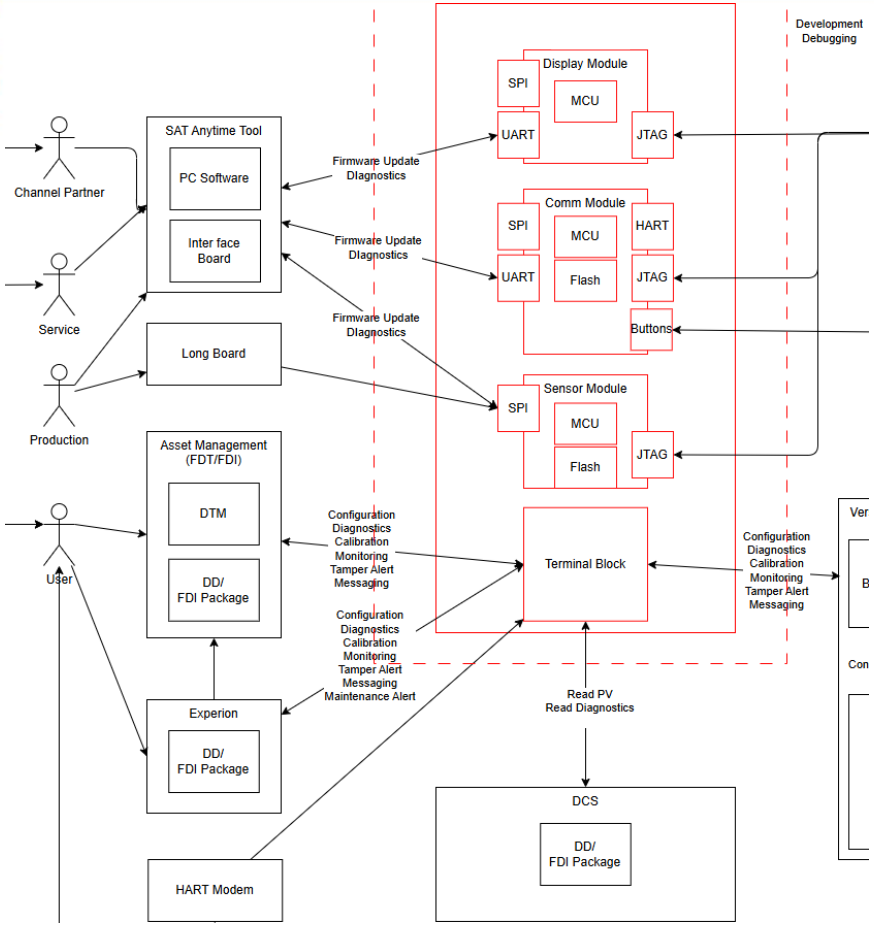
- Create common understanding about how a product is intended to be installed and used
- Help product developers to make appropriate design decisions

Includes:

- all internal elements
- all external elements
- Assets
- Trust Boundaries
- Interconnections
- Assumptions that refer to the security of the system or asset

© 2026 ODVA, Inc.
All rights reserved.
Classified as Business

Establish the Security Context



Example 1:

The security context of a Smart Transmitter device can include or exclude the configuration software

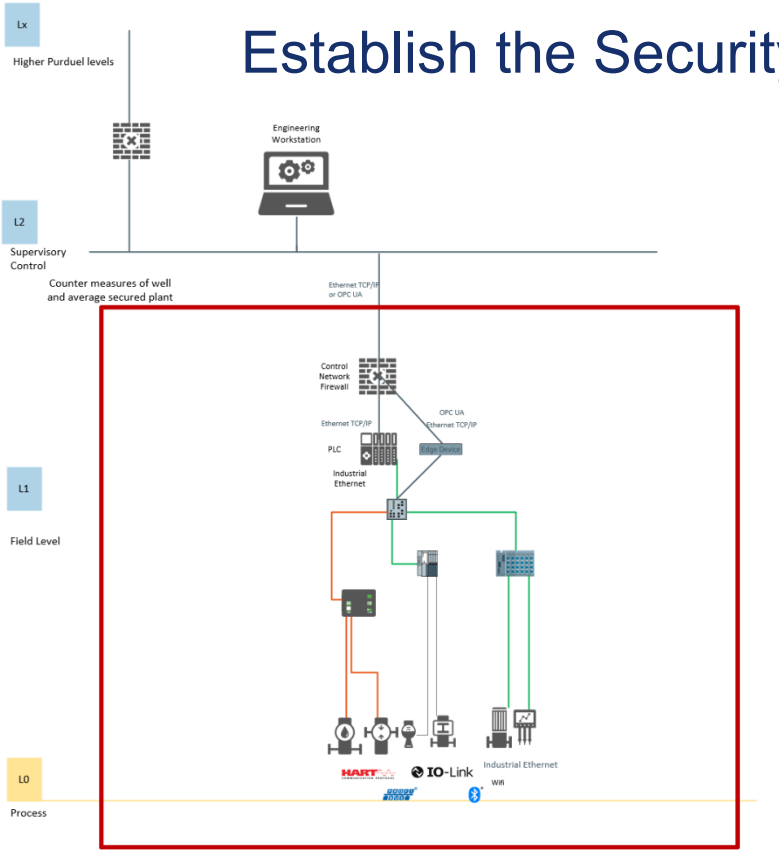
© 2026 ODVA, Inc.

All rights reserved.

Classified as Business

Establish the Security Context

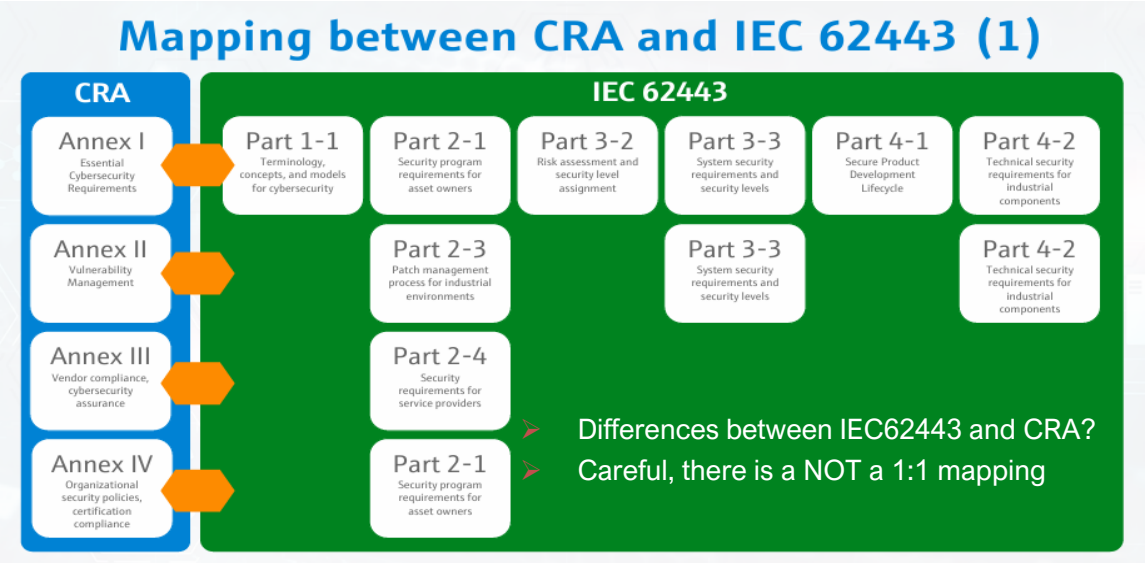
Example 2: OT Secure Plant



© 2026 ODVA, Inc.

All rights reserved.
Classified as Business

„Secure by Design“ - Requirements



"While both frameworks cover the full product lifecycle (including support and decommissioning), the **CRA is a mandatory EU law** for market access with strict reporting duties, whereas **IEC 62443 is a global industry standard** tailored to operational security in automation (OT)."

© 2026 ODVA, Inc.
All rights reserved.
Classified as Business

Threat Analysis

Examples:

1) Unauthorized Access

- Attackers exploit weak passwords, default credentials, or insecure remote-access paths to gain control of the transmitter.
- This can allow them to change configuration settings, calibration values, or communication parameters.

2) Data Tampering / False Data Injection

- An attacker intercepts or modifies measurement data in transit, causing operators or automated controls to act on incorrect pressure, temperature, flow, or level readings.
- This can lead to process instability, production losses, safety incidents, or equipment damage.

3) Firmware Tampering

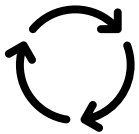
Hence threats can be e.g. firmware changes in the OEM factory

© 2026 ODVA, Inc.
All rights reserved.
Classified as Business

Risk Assessment

- **Legislation requires manufacturers to carry out a risk assessment on the basis of which they need to implement the relevant essential requirements**

  - Look at the threats and classify and prioritize them into risks
  - Assess the risks

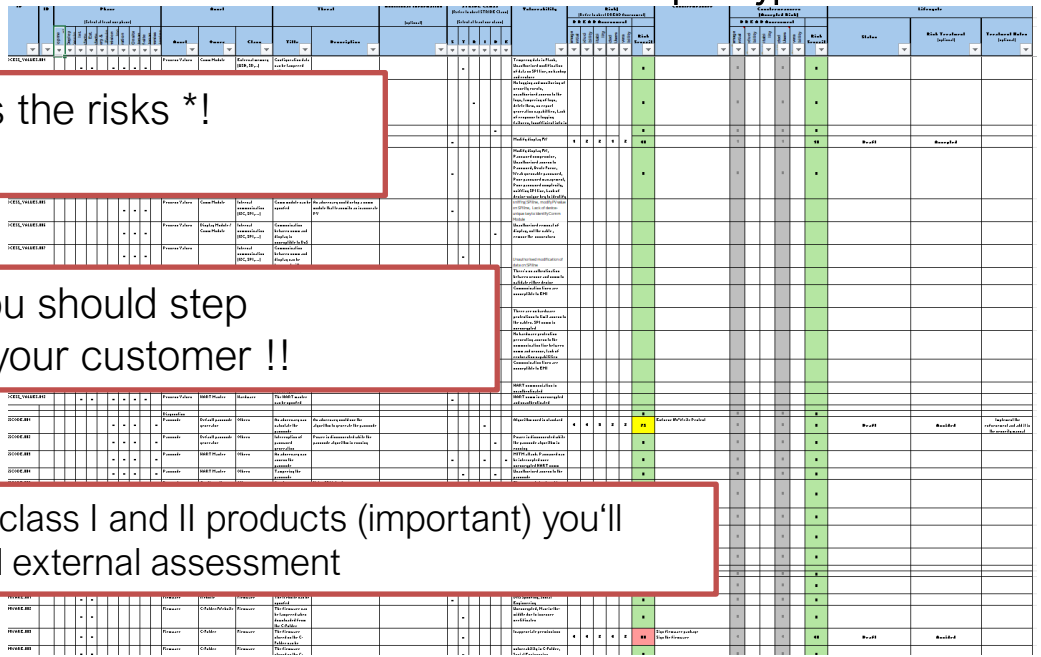


…take the outcome of that assessment into account during the **planning, design, development, production, delivery and maintenance phases** of the product with digital elements with a view to **minimising cybersecurity risks, preventing incidents and minimising their impact**….

© 2026 ODVA, Inc.
All rights reserved.
Classified as Business

Risk Assessment

Example: Typical Risk Matrix



Yes, you (Dear Manufacturer) assess the risks *!
This is a team effort

When doing so you should step
into the shoes of your customer !!

*For class I and II products (important) you'll need external assessment

© 2026 ODVA, Inc.

All rights reserved.
Classified as Business

Risk Assessment

Example: 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

- *Data stored in a product's internal memory should be encrypted at rest using current nondeprecated technology*
- *Transmission protocols used to send/receive data should support encrypted communications and enable them by default*
- *The product should implement symmetric or asymmetric encryption schemes (including PKIs) to ensure that confidentiality of exchanged data is protected*

A) Fulfill the requirement technically:

⇒ Enable CIP Security as default communication protocol

B) Don't change the existing product or protocol (e.g. HART)

➢ Use Secure Plant Approach, provide security guidance to the customer:

© 2026 ODVA, Inc.
All rights reserved.
Classified as Business

Counter Measures



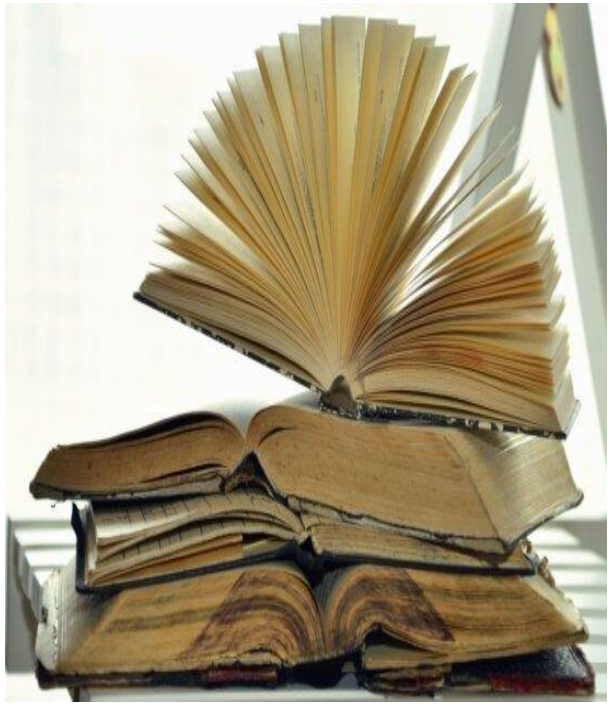
- Modify firmware or device on location => Disable JTAG interface
- Modification of firmware before production => Sign and encrypt firmware
- Modification of firmware before or in production => Secure Boot Process
- Unauthorized access to device => Implement Authentication
- Firmware can be downloaded by unauthorized person => Encrypt Firmware
- Chip-Supplier delivers tampered firmware => Check authenticity e.g. with hash at factory

© 2026 ODVA, Inc.
All rights reserved.
Classified as Business

Documentation

Necessary for Auditing (and CE Marking)

- Description of the design, development and manufacturing of the product (with regard to Security)
- Documentation of the security risks relevant to the product as well as the security measures used (TRA)
- Details of security tests carried out
- Description of the components using the Software Bill of Materials (SBOM) in electronic form
- Support Period Information*
- Managing the Product (Customer Process)*



*External (Customer) Documentation

© 2026 ODVA, Inc.
All rights reserved.
Classified as Business

Life Cycle Management

Bringing the product onto the market starts a support period during which….

- You have to **monitor** the software for known vulnerabilities
- Apply effective and **regular** tests and reviews of the security of the product with digital elements
- Provide appropriate security **updates** during the expected product lifetime free of charge
- **Periodic** vulnerability assessments should be executed, especially towards those components that present the highest risk
- Securely distribute software updates e.g. by digital signing

© 2026 ODVA, Inc.
All rights reserved.
Classified as Business

Life Cycle Management

⇒ Goal of the CRA is NOT to destroy the market, **but to increase the overall level of cyber security in the EU**

Plan for a product lifecycle budget (for at least 5 years!) that should include:

1) Regular Monitoring (SBOM!) based on tooling
2) Regular Assessment of Vulnerabilites (e.g. for Linux devices ~30 / day)
   => Detected, Exploited, Exploitable?
   => Assess and Decide about relevance and mitigation
3) Reporting => Within 24h to Single Reporting Platform (SRP) | ENISA
4) Regular Cyber Security (Penetration) Testing

You can outsource activities to Industrial Cyber Security experts

© 2026 ODVA, Inc.
All rights reserved.
Classified as Business

Budget Example

Risk Based Approach	
Communication Model (SW components)	10 Pdays
Threat Modeling & Risk Assessment	10 Pdays (ideal 3 persons)
Counter Measures Implementation	20 Pdays (depending…)
Documentation (Internal & Customer facing)	15 Pdays
Life Cycle Management (Monitor, Assess, Report)	Up to 50 Pdays (annually over lifetime)
Total Effort	~ 105 PDays…

Additional: Training, Tooling, Penetration Testing



© 2026 ODVA, Inc.

All rights reserved.
Classified as Business

Key Takeaways

Step 1

- **Set Up Vulnerability Management & Reporting Processes (+ Secure Development Processes)**

Step 2

- **Identify and Classify your Products with Digital Elements (PwDE)**
- **Create your Security Context (for each product)**

Step 3

- **Perform Threat Analysis and Risk Assessment**
- **Provide Counter Measures**
- **Create Documentation including SBOM and User Security Manual**

© 2026 ODVA, Inc.
All rights reserved.
Classified as Business



Thank you !!!

Sven.Giesecke@CodeWrights.de

www.linkedin.com/in/svengiesecke