How to Deliver Cybersecure EtherNet/IP Devices: A Practical Approach for EU CRA Compliance

Sven Giesecke, Director Portfolio, CodeWrights GmbH
Andreas Winter, CySec Specialist, CodeWrights GmbH

Presented at the ODVA
2026 Industry Conference & 24th Annual Meeting
October 21, 2026
Vilamoura, Portugal

Abstract

The European Union Cyber Resilience Act (CRA) introduces mandatory cybersecurity requirements for products with digital elements that are placed on the European market. For manufacturers of industrial communication products and EtherNet/IP devices in particular, compliance is not only a regulatory obligation but also a practical necessity for reducing operational risk, protecting customer production environments, and preserving market access.
This paper provides a practical manufacturer-oriented approach to how to achieve CRA compliance and continue to deliver existing products into the EU market. It explains how CRA obligations intersect with industrial automation, secure industrial communication, IEC 62443, and product lifecycle management. It also proposes a step-by-step method for moving from product scoping to security context definition, threat analysis, risk assessment, countermeasure selection, documentation, and post-market vulnerability management.
The central argument is that CRA compliance should not be treated as a purely legal exercise. It should be used as a structured engineering discipline that strengthens product security, improves operational resilience, and creates clearer evidence for audits, customers, and internal development teams.

Keywords

Cyber Resilience Act (CRA), products with digital elements (PwDE), industrial automation and control systems (IACS), EtherNet/IP, CIP Security, IEC 62443, secure-by-design, threat analysis and risk assessment (TARA), software bill of materials (SBOM), vulnerability management, lifecycle security, CE conformity assessment

1. Introduction

Industrial automation is undergoing a profound transformation. Devices that once operated in relatively closed environments are now connected to plant networks, engineering workstations, cloud services, and remote maintenance infrastructures. EtherNet/IP devices, smart transmitters, gateways, controllers, and other industrial products therefore participate in increasingly interconnected operational technology landscapes. This connectivity improves visibility, flexibility, and efficiency, but it also exposes products to cyber threats that were not always considered in earlier generations of device design.
Against this background, the EU Cyber Resilience Act establishes a mandatory baseline for cybersecurity across products with digital elements. Its impact reaches well beyond consumer devices. Industrial components, embedded systems, and communication-capable field devices fall squarely into scope whenever they are placed on the EU market and possess a direct or indirect logical or physical data connection to a device or network. For manufacturers, the question is no longer whether cybersecurity

 ©2026 ODVA, Inc.

should be considered, but how to deliver secure products with adequate technical, organizational, and documentary evidence.
This paper focuses on a practical approach for manufacturers of EtherNet/IP and related industrial devices. The objective is not to restate the law in isolation, but to show how a manufacturer can embed the operationalize the regulation into their business and harness it as a driver for their business. The paper first explains the CRA and its relevance to industrial automation. It then connects CRA expectations with established industrial security practice, especially IEC 62443 and secure industrial communication concepts such as CIP Security. Finally, it lays out a pragmatic compliance workflow that can be implemented by engineering organizations developing new products or continuing to place existing products on the market.

2. Why the CRA Matters for Industrial Device Manufacturers

The CRA introduces binding cybersecurity obligations across the product lifecycle and is mandatory to sell a product on the European market after December 11th, 2027 (see Figure 1). Manufacturers must design and develop products with cybersecurity in mind, handle vulnerabilities appropriately, and provide security support during a defined support period. This makes compliance materially different from voluntary or customer-driven best practice programs. Non-compliance can lead to severe consequences, including loss of access to the EU market, reputational damage, production-related incidents at customer sites, and substantial financial penalties.

For industrial device manufacturers, these consequences are especially significant because the impact of a security failure extends beyond data confidentiality. Compromised industrial products can alter control logic, manipulate process values, affect plant availability, damage equipment, or create safety-relevant conditions. A weak device in an automation network can become an entry point into a wider plant environment. As a result, CRA compliance should be seen not as external overhead but as a risk reduction measure aligned with the real operational consequences of industrial cybersecurity failures.
Another critical point is that the CRA applies to individual products, not abstract product types. A device design created before the regulation takes effect does not automatically remain marketable indefinitely. Products manufactured and placed on the market after the applicable date must comply as individual instances, even if the original product family predates the regulation. This has major implications for legacy portfolios. Manufacturers cannot assume that mature or widely deployed devices are exempt simply because the design is longstanding. Existing products that remain commercially relevant must be reassessed against current cybersecurity requirements.
The business implication is as strategic as technical. Product roadmaps, certification plans, component sourcing decisions, and service organization capabilities all become part of the cybersecurity discussion. Management therefore needs visibility into which products create the largest compliance exposure, which legacy designs can realistically be remediated, and which products may need redesign or retirement. Treating CRA preparation as a portfolio governance exercise helps avoid last-minute remediation under commercial pressure and supports earlier, more rational investment decisions.

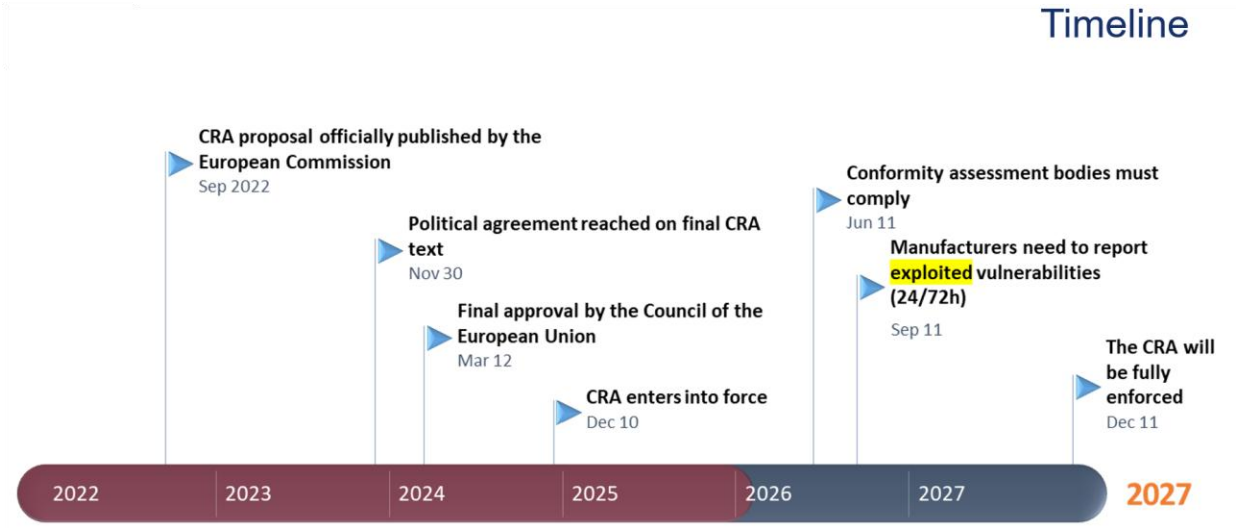


Figure 1: Timeline of the CRA enforcement.

3. Industrial Automation, OT, and the Need for Secure Communication

Industrial automation environments sit at the intersection of information technology and operational technology. Historically, industrial communication protocols and devices were optimized for deterministic control, interoperability, and long service life rather than for modern cybersecurity requirements. As a result, large parts of the installed base still rely on communication patterns that lack strong authentication, integrity protection, confidentiality, or secure update mechanisms.

This legacy is one reason why secure industrial communication is such an important design decision. Where manufacturers can adopt secure communication mechanisms directly, they should do so. For EtherNet/IP ecosystems, CIP Security offers a concrete path toward stronger authentication, integrity, and confidentiality. Enabling secure communication by default supports several CRA objectives at once: it reduces exploitable attack surface, provides protection for data in transit, and creates a more trustworthy baseline for product security claims.

At the same time, practical constraints must be acknowledged. Not every installed product can be redesigned around a new protocol stack with reasonable effort. Devices must interact with legacy systems, serve highly constrained use cases or are embedded in customer environments that have their own architectural limitations. The practical lesson is not that all products must be redesigned identically, but that each product needs a justified security strategy. When secure industrial communication can be integrated directly, it should be prioritized. When legacy constraints remain, the manufacturer must define compensating controls, deployment assumptions, and customer guidance with far greater precision.

For industrial vendors, this creates a strong incentive to evaluate communication architecture earlier in development. Protocol choices influence certificate management, device onboarding, secure commissioning, interoperability testing, customer support, and long-term patchability. Security is therefore not just an add-on feature at the edge of the design. It directly affects the communication model, the user experience of commissioning and maintenance, and the overall cost of ownership of the product over its lifetime.

4. CRA, IEC 62443, and the Standards Landscape

Industrial organizations already use IEC 62443 as a reference framework for secure development and industrial control system security. The CRA does not replace that practice; instead, it changes the compliance context. IEC 62443 is an internationally recognized standard family that is often adopted through customer requirements, internal governance, or certification strategies. It does require security-

specific processes and artefacts, but many of them are well-known software quality principles. The CRA, by contrast, is a mandatory EU regulation tied to market access and reporting duties.

This distinction between CRA and IEC 62443 matters because there never was a simple one-to-one mapping between the two EC 62443-4-1 provides detailed secure product development lifecycle expectations, while IEC 62443-4-2 provides component-level security requirements. These are highly valuable for engineering practice. However, the CRA introduces additional legal expectations around conformity, vulnerability handling, support commitments, and incident reporting. A company that already follows IEC 62443 is in a stronger starting position, but it should not assume automatic CRA compliance.
The emerging harmonized standards under the EN 40000 series are intended to provide a horizontal structure for CRA requirements across products. For industrial manufacturers, these standards will likely become an important translation layer between regulation and assessable engineering evidence.
Until the new standards are fully established, organizations should use existing industrial cybersecurity frameworks, legal interpretation, and pragmatic engineering governance together. In practice, IEC 62443 can provide much of the development rigor, while the CRA defines the regulatory destination and required evidence model.
The practical consequence is that manufacturers should build a traceability model rather than chase perfect terminology alignment. Internal requirements, architecture decisions, test evidence, SBOM data, and support process records should be traceable both to engineering standards and to regulatory obligations. This makes audits more efficient and reduces the risk that important controls exist in practice but cannot be demonstrated coherently. In mature organizations, this traceability also improves reuse across product lines.

5. Reviewing the Product in Scope

A practical compliance effort begins with product scoping. This sounds straightforward, but it is often where organizations discover hidden complexity. The manufacturer must determine whether it is dealing with a new product, an existing product, or a family of products with differing software and communication characteristics. It must also assess how mature its own secure development practices already are, whether the product falls into a higher classification (products that fall under CRA are grouped into three classes) with additional assessment needs, and whether secure industrial communication mechanisms are feasible within the device architecture.
This product review stage should also identify the actual digital elements that matter for cybersecurity. Typical examples include firmware, embedded operating systems, web interfaces, engineering ports, remote management functions, protocol stacks, authentication certificates, secure elements, update mechanisms, and third-party software components. Hidden complexity often lies in interfaces that were historically treated as service functions rather than cybersecurity-relevant features: JTAG, factory programming, configuration software, maintenance ports, and update loaders all deserve explicit attention.
The goal is to create a product-specific compliance starting point rather than a generic category statement. Once this is done, the organization can decide whether the product should be modernized to meet current security and lifecycle requirements, retained under clearly defined operational and environmental constraints that mitigate its security risks or replaced by a solution that provides more secure communication capabilities and long-term lifecycle support.
Without this product-level clarity, later threat analysis and compliance documentation become inconsistent and difficult to justify.
It is also useful at this stage to name product variants that share a platform. A common hardware or firmware base may allow common controls, evidence, and lifecycle processes to be reused, but only if differences are clearly documented. Conversely, variants that look similar from a marketing perspective may differ substantially in connectivity, software composition, or exposure. Grouping products incorrectly can create false confidence and result in incomplete evidence for variants while overengineering others.

6. Establishing the Security Context

One of the most useful concepts methods for turning cybersecurity requirements into actionable engineering decisions is to define the security context. The security context describes the intended environment of the product and all security-relevant aspects of the system in which it is expected to operate. This includes internal elements, external systems, assets, trust boundaries, interconnections, and the assumptions on which product security claims depend.

For industrial products, defining this context is essential because security responsibilities are distributed. A manufacturer may control the firmware, protocol implementation, hardware root of trust, and update mechanism, but it does not control the customer network segmentation, account management, remote access governance, or plant incident response capabilities. If those environmental assumptions are left implicit, product security discussions quickly become vague and unproductive. A well-defined security context makes assumptions visible and therefore reviewable.

The example security context in Figure 2 illustrates the complexity of such diagrams. It provides an overview of all aspects of transmitter software allowing the manufacturer to make decisions about what will be assessed. The transmitter's security context may or may not include the configuration software, depending on how the system boundary is defined. The red part and red dotted line in this case demonstrate the decision for a security context without the configuration software.

Likewise, a secure plant architecture may create include external protections that change risk exposure without eliminating the manufacturer's product obligations. The right goal is not to push responsibility outward, but to define where product controls stop, where system assumptions begin, and what deployment conditions must be documented for the customer. This mutual understanding helps developers make proportionate design decisions and helps auditors understand the rationale behind them.

In practice, the security context is best expressed in a form that engineers can use repeatedly: a concise narrative, a communication diagram, an asset list, and an assumptions register are often enough. These artifacts help development teams reason about what the product must protect, what interfaces require hardening, which identities need trust anchors, and which external systems are relied upon. They also support conversations with customers and integrators by making deployment expectations concrete rather than implicit.

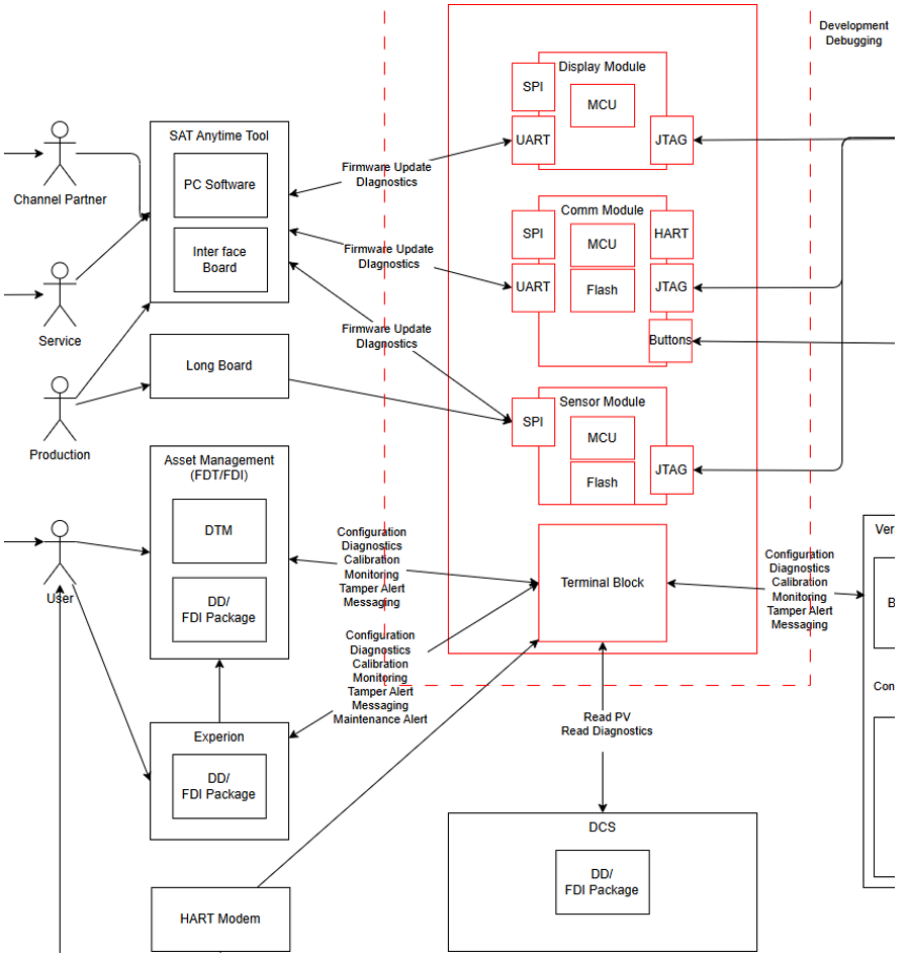


Figure 2: The security context of a Transmitter device can include or exclude the configuration software.

7. Threat Analysis and Risk Assessment

Only once the product scope and security context are documented, can the manufacturer perform a meaningful threat analysis and risk assessment. The CRA requires a risk-based approach: relevant essential requirements must be implemented based on identified cybersecurity risks. In industrial practice, this means evaluating realistic threats, estimating their likelihood and impact, and prioritizing controls accordingly.

Typical threats for an industrial EtherNet/IP or smart device include lack of authentication and access control, unauthorized access through weak credentials or insecure remote paths, tampering with measurement or control data in transit, modification of firmware before deployment, compromise during manufacturing, abuse of service interfaces, and exploitation of vulnerable third-party software components. These threats are not theoretical. In industrial settings they can lead to production disruption, process instability, incorrect operator decisions, equipment damage, and safety incidents.

A useful risk assessment should be conducted by a cross-functional team rather than by a single compliance owner. Development, system architecture, product management, quality, manufacturing, service, and cybersecurity specialists all contribute different perspectives. The manufacturer should deliberately evaluate risk from the customer's point of view because the real-world consequences occur in the user's operational environment. A structured risk matrix can then be used to classify and prioritize threats, but the value lies in the discussion and justification behind the ratings, not only in the matrix itself.

For certain product classes, external assessment may also be required. CRA groups the products into three main categories based on cybersecurity risk: **Default**, **Important (Class I and Class II)**, and **Critical**.
Even where not mandatory, independent review can improve confidence in both the technical decisions and the conformity evidence. The key practical principle is that risk assessment is not a one-time workshop artifact. It should drive planning, design, development, production, delivery, and maintenance decisions throughout the product lifecycle.
A mature risk process also records why certain threats were deprioritized or treated disregarded through due to environmental assumptions rather than product changes. These decisions are often revisited later during audits, incident investigations, or product updates. Capturing the reasoning at the time of assessment reduces ambiguity and allows the organization to react faster when assumptions change, for example when a formerly isolated interface becomes remotely reachable in a customer deployment.

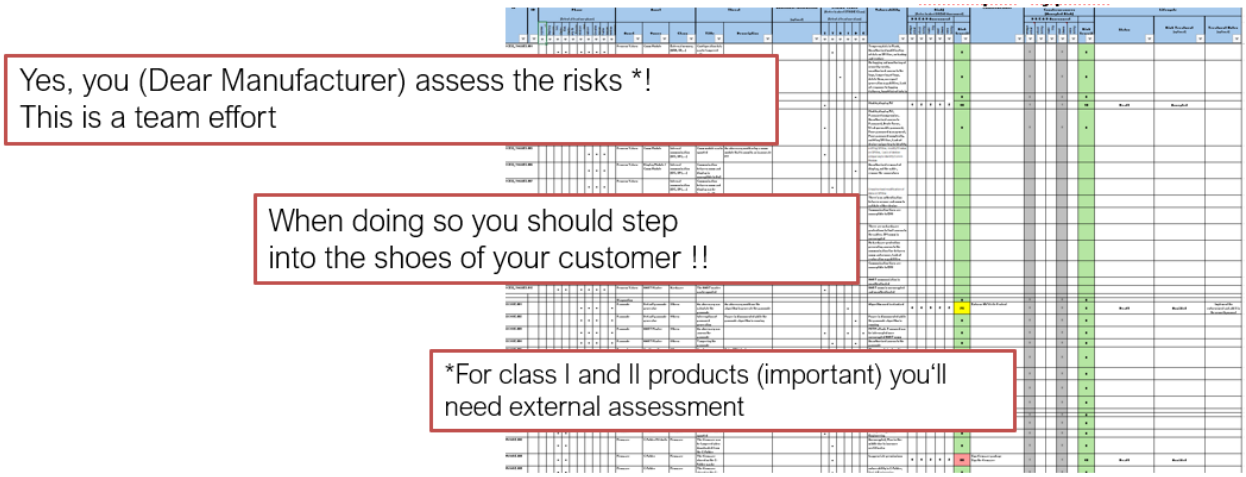


Figure 3: Typical Risk Matrix

8. Selecting and Implementing Countermeasures

The risk assessment is the basis on which the most critical findings will be used to develop specific countermeasures. For industrial devices, those countermeasures often span hardware, firmware, communications, manufacturing, and operations. Examples include disabling or protecting JTAG and debug interfaces in deployed products, implementing secure boot, signing and encrypting firmware, enforcing strong authentication, protecting update delivery, verifying component authenticity during production, and enabling encrypted communications for data in transit.
Let us look at the confidentiality of stored, transmitted or otherwise process data. Ideally the manufacturer fulfills this technically by enabling CIP Security or an equivalent secure communication mechanism as the default communication mode. This is the most direct solution because it reduces reliance on external assumptions. However, where legacy protocols remain necessary, the manufacturer must provide a secure deployment approach and clear customer guidance. In other words, if the product cannot intrinsically satisfy a security requirement to the fullest degree, the compensating security architecture must be explicit and supportable.
This decision point is especially important for long-lived industrial portfolios. A company may be tempted to avoid product changes and rely entirely on external network protections, but that strategy becomes increasingly difficult to justify when equivalent secure communication options exist. The better approach is usually a phased model: improve intrinsic product controls wherever feasible, document the residual risk assumptions transparently, and plan migration paths for older architectures. Countermeasures should therefore be prioritized by both risk reduction and lifecycle sustainability.
User-centered design matters as much as control selection. Strong security features that are difficult to commission, poorly integrated into the device workflow, or disabled by default often provide limited real-world benefit. Manufacturers should therefore evaluate usability, service impact, and recoverability

alongside security strength. In industrial environments, controls that align with existing commissioning and maintenance practices are more likely to remain active over the lifetime of the product.

9. Documentation, SBOMs, and Conformity Evidence

Cybersecurity compliance is not complete when the engineering work is finished. The manufacturer must be able to demonstrate what was designed, why it was designed that way, and how it was validated. Documentation is therefore a core deliverable rather than an administrative afterthought. For CRA-related audits and CE marking activities, the organization needs evidence describing the design, development, and manufacturing of the product from a security perspective.

This documentation should include at least the product security design description, the threat and risk assessment, the selected security measures and their rationale, records of security testing, and a software bill of materials in electronic form. The SBOM is particularly important because post-market vulnerability monitoring depends on knowing exactly which software components and versions are present in the shipped product. Without a correct SBOM, vulnerability handling becomes reactive, incomplete, and difficult to scale.

Customer-facing documentation is equally important. A support period statement, security guidance, secure deployment recommendations, update instructions, and operational assumptions must be communicated in a way the customer can use. Industrial products are rarely deployed in a vacuum. Integrators, operators, and maintenance teams need enough information to install, configure, and keep the device securely. Clear documentation therefore functions as both audit evidence and practical risk control.

Good documentation practice also reduces friction across internal teams. Service personnel need update and recovery procedures, manufacturing teams need authenticity and provisioning instructions, sales teams need accurate claims, and legal or compliance teams need consistent evidence packages. A single controlled documentation set, structured around the product's security context and risk decisions, supports all these groups and makes later maintenance far more manageable.

10. Lifecycle Management and Vulnerability Handling

The CRA's practical impact extends well beyond product launch. Once a product is placed on the market, the manufacturer enters a support period during which vulnerabilities must be monitored, assessed, and addressed. This requirement is particularly demanding for industrial products with long service lives. A device that remains in operation for years or even decades cannot be treated as finished at shipment. Its security posture must be ensured over time.

Effective lifecycle management starts with regular monitoring of software components and threat intelligence sources. For Linux-based or otherwise software-rich devices, the volume of relevant vulnerability information can be high, sometimes reaching dozens of potential findings per day. This does not mean that every vulnerability is equally relevant. Manufacturers need a triage process that distinguishes detected issues from exploitable issues and then determines product applicability, customer impact, and mitigation options. SBOM-driven tooling is essential here.

The organization must also perform regular security reviews and testing, particularly for components and interfaces with elevated risk. Secure distribution of updates, ideally using digital signing and robust authenticity checks, is another critical control. Where serious incidents or actively exploited vulnerabilities occur, the CRA introduces reporting obligations with demanding timelines. These obligations require preparation: defined roles, decision paths, evidence collection, communication workflows, and interfaces to the relevant reporting platforms.

From a budgeting perspective, lifecycle management should be planned as a sustained operational function, not a residual activity squeezed into product maintenance. In future manufacturers must define and communicate the lifetime of their product and plan for a multi-year continuous budget. Monitoring, assessment, reporting, retesting, and updating delivery all consume recurring effort. Organizations that ignore this early will struggle to meet support commitments once the installed base grows.

Lifecycle readiness is often where organizational maturity becomes visible. Companies with strong asset knowledge, reproducible builds, reliable release pipelines, and disciplined change management can respond faster and with higher confidence. Companies without those foundations may understand the

vulnerability but still struggle to answer basic questions such as which products are affected, which customers should be notified, and whether an update can be shipped securely. CRA preparation therefore strengthens core product operations as well as security.

11. Organizational Effort and Budgeting

A practical CRA program requires both technical work and organizational planning. The budget example in Table 1 is useful because it reframes cybersecurity as a visible engineering investment.

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…

Table 1: Budget Example

Communication model analysis, software component review, threat modeling, risk assessment, countermeasure implementation, documentation, and lifecycle management all need dedicated effort. For a representative device program, the total can easily reach about one hundred person-days or more, with recurring annual effort for monitoring and vulnerability handling.

These numbers should not be interpreted rigidly, because product complexity differs widely. A compact embedded device with limited functionality may require much less effort than a Linux-based gateway with multiple interfaces, web services, remote management, and third-party packages. Still, the budgeting logic is sound. Manufacturers need explicit resourcing for training, tooling, penetration testing, secure development process improvement, and recurring lifecycle tasks. If cybersecurity stays unfunded or hidden within general engineering overhead, compliance quality and sustainability will both suffer.

Leadership involvement is essential. Management decisions decide release priorities, platform strategy, component selection, maintenance funding, and acceptable risk treatment. If leadership treats cybersecurity as an isolated engineering topic, teams will struggle to make the tradeoffs needed for long-term compliance. If leadership instead integrates cybersecurity into product governance, budgeting, and roadmap reviews, the organization can make earlier and more coherent decisions across the portfolio.

12. Market Feedback and Customer Expectations

Although specific market feedback varies by sector, one clear trend is that customers increasingly expect evidence, not just claims. Asset owners, integrators, and procurement teams want to understand how a product is secured, what support period applies, how vulnerabilities are managed, and whether secure communication and update mechanisms are available. In this sense, CRA readiness can become commercially differentiating. Manufacturers that can explain their security model clearly are often easier to trust and easier to integrate into formal procurement processes.

This shift also changes the tone of customer conversations. Security questionnaires, contractual cybersecurity clauses, and requests for SBOMs or vulnerability disclosure practices are becoming more common. A manufacturer that already operates with a well-defined security context, documented risk decisions, and repeatable lifecycle processes can answer these requests with less friction. Market pressure therefore reinforces the same capabilities required for regulatory compliance, making early investment strategically valuable.

13. Practical Recommendations for Manufacturers

Several practical recommendations emerge from the material.
First, start with the products that are commercially important and cybersecurity-relevant rather than waiting for full portfolio perfection.
Second, prefer intrinsic product security controls over purely environmental assumptions wherever technically feasible.
Third, use the security context to make responsibilities, assumptions, and trust boundaries explicit.
Fourth, maintain a living SBOM and vulnerability triage capability from the beginning instead of trying to reconstruct product composition later.
Fifth, connect engineering and compliance teams closely and make sure secure-by-design principles become the standard in every development process. Regulatory interpretation by compliance teams without specific product knowledge leads to weak implementation, while product engineering without regulatory support can miss critical evidence and reporting obligations.
Sixth, plan for the products support period as a long-term commitment. Secure product delivery is not only about the first release; it is about maintaining a strong and trustworthy security posture throughout the product's expected lifetime.
Finally, communicate clearly with customers. In industrial environments, manufacturer guidance influences real deployment outcomes and therefore materially affects risk.

14. Conclusion

The EU Cyber Resilience Act changes the baseline for industrial products with digital elements. For manufacturers of EtherNet/IP devices and related automation components, compliance requires more than a checklist. It demands a structured, risk-based approach that begins with understanding the product in scope, defining the security context, and analyzing realistic threats. It then continues through technical countermeasures, rigorous documentation, and sustained lifecycle management.
The good news is that much of the necessary discipline already exists in industrial cybersecurity practice. Secure communication technologies, IEC 62443 development principles, SBOM-based transparency, secure boot, signed updates, and structured vulnerability handling all contribute directly to a robust compliance strategy. The challenge is to integrate these elements into a coherent product and organizational model that can withstand audit scrutiny and deliver real customer value.
Manufacturers that act early can use CRA preparation to improve both compliance and product quality. By treating cybersecurity as an engineering and lifecycle capability rather than a late-stage legal obligation, they can reduce risk, preserve market access, and deliver industrial devices that are better suited to the realities of modern connected automation environments.

References

[1] ODVA, *The CIP Networks Library, Volume 1: Common Industrial Protocol*, Ann Arbor: ODVA, Inc., 2001-2026.
[2] European Union, *Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)*, Brussels: Official Journal of the European Union, 2024.
[3] IEC, *IEC 62443-4-1: Security for Industrial Automation and Control Systems - Part 4-1: Secure Product Development Lifecycle Requirements*, Geneva: International Electrotechnical Commission, 2018.
[4] IEC, *IEC 62443-4-2: Security for Industrial Automation and Control Systems - Part 4-2: Technical Security Requirements for IACS Components*, Geneva: International Electrotechnical Commission, 2019.
[5] ODVA, *ODVA Security Concepts*, Ann Arbor: ODVA, Inc., 2022.
[6] PI (PROFIBUS & PROFINET International), *PI Protocols - A Risk Management Based Approach*, Karlsruhe: PI, 2026.
[7] OPC Foundation, *Common IA IDevID Requirements*, Scottsdale: OPC Foundation, 2025.
[8] FCG, *Authentication in the OT Environment*, Bonn: FieldComm Group, 2025.
[9] CEN-CENELEC JTC 13 WG 9, *EN 40000-1-1 Vocabulary (Draft Harmonized Standard for CRA)*, Brussels: CEN-CENELEC, 2026.
[10] CEN-CENELEC JTC 13 WG 9, *EN 40000-1-2 Principles, Product Risk Management, and Lifecycle Activities (Draft Harmonized Standard for CRA)*, Brussels: CEN-CENELEC, 2026.
[11] CEN-CENELEC JTC 13 WG 9, *EN 40000-1-3 Vulnerability Handling (Draft Harmonized Standard for CRA)*, Brussels: CEN-CENELEC, 2026.
[12] CEN-CENELEC JTC 13 WG 9, *EN 40000-1-4 Generic Security Requirements (Draft Harmonized Standard for CRA)*, Brussels: CEN-CENELEC, 2026.

****
The ideas, opinions, and recommendations expressed herein are intended to describe concepts of the author(s) for the possible use of ODVA technologies and do not reflect the ideas, opinions, and recommendation of ODVA per se. Because ODVA technologies may be applied in many diverse situations and in conjunction with products and systems from multiple vendors, the reader and those responsible for specifying ODVA networks must determine for themselves the suitability and the suitability of ideas, opinions, and recommendations expressed herein for intended use. Copyright ©2026 ODVA, Inc. All rights reserved. For permission to reproduce excerpts of this material, with appropriate attribution to the author(s), please contact ODVA on: TEL +1 734-975-8840 FAX +1 734-922-0027 EMAIL odva@odva.org WEB www.odva.org. CIP, Common Industrial Protocol, CIP Energy, CIP Motion, CIP Safety, CIP Sync, CIP Security, CompoNet, ControlNet, DeviceNet, and EtherNet/IP are trademarks of ODVA, Inc. All other trademarks are property of their respective owners.