FRANK LEITNER CYBERSECURITY
SECURE BY DESIGN, TRUSTED IN PRACTICE

The ‘Pen Test and Ship’ Era Is Over: Engineering Security for CRA Readiness

A practical perspective on Secure-by-Design and ISA/IEC 62443 in the context of the EU Cyber Resilience Act

SECURE PRODUCT DEVELOPMENT
From Engineering Discipline to CRA Readiness

For a long time, security in software products was treated as a downstream activity.

- Penetration test.
- Fix findings.
- Ship.

That model is no longer sufficient. In fact, for many organizations, it is actively dangerous.

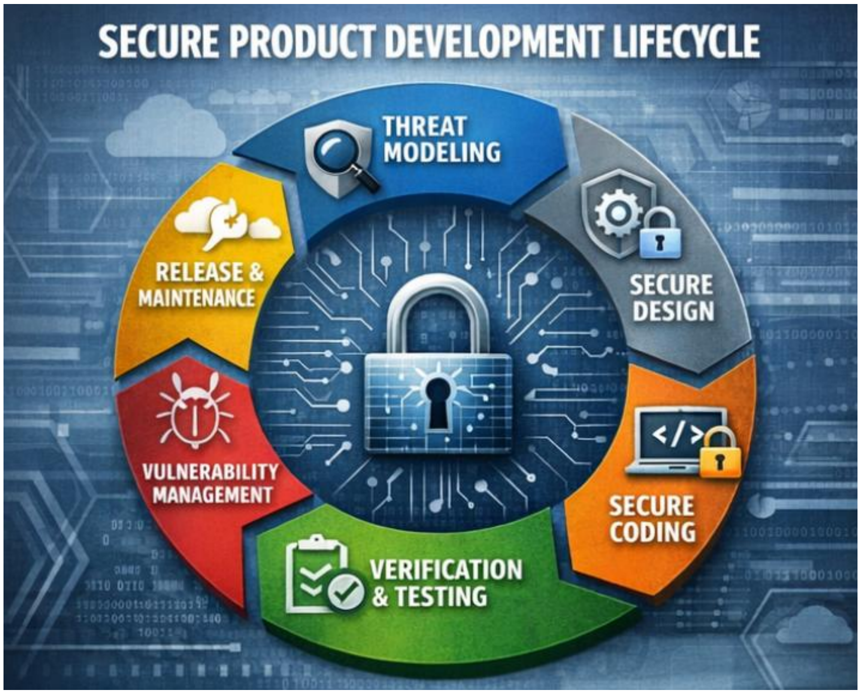
Modern software products are connected, updateable, API-driven, and deeply integrated into customer environments. Vulnerabilities are no longer just technical defects. They are business risks, regulatory risks, and reputation risks.

With the EU Cyber Resilience Act, expectations are becoming explicit:

- Security by design and by default
- Continuous vulnerability handling
- Structured risk management
- Clear accountability across the lifecycle

This shifts the conversation from “Did we test it?” to “Was security engineered into the product from the beginning?”

What Secure Product Development Really Means



Secure product development is not about adding controls at the end.

It means embedding security across the entire lifecycle:

- Threat modeling during concept and architecture
- Security requirements derived from structured risk analysis
- Secure design decisions with traceable rationale
- Development guidance aligned with product risk
- Verification and validation of security mechanisms
- Defined processes for vulnerability handling and updates

Security becomes part of engineering, not an external gate.This is where structured frameworks become essential.

Where ISA/IEC 62443 Fits In

For industrial and connected products, ISA/IEC 62443 provides a practical and structured foundation.

In particular:

- 62443-4-1 defines requirements for a secure development lifecycle
- 62443-4-2 defines technical security requirements for components

What makes this powerful is that 62443 does not stay at a high-level governance discussion. It translates directly into development practice. It requires defined processes for threat and risk analysis, security requirements management, secure design, implementation guidance, verification activities, and long-term vulnerability handling.

While originally rooted in industrial automation and control systems, its influence goes well beyond classic OT. Energy, manufacturing, rail, building automation, and critical infrastructure sectors actively reference or require 62443 alignment. In many cases, operators expect product suppliers to demonstrate conformity to 62443-4-1 processes and 62443-4-2 technical capabilities.

Beyond these sectors, the content itself is highly transferable:

- IoT and embedded product vendors use it as a baseline for secure device development
- Software-driven machinery manufacturers adopt it to structure their SDLC
- Organizations preparing for regulatory frameworks such as the EU Cyber Resilience Act use it as a concrete implementation backbone

In practice, 62443 helps translate abstract requirements such as “secure by design” into:

- Defined lifecycle checkpoints
- Traceable security requirements
- Verifiable technical capabilities
- Structured vulnerability management

Consider a connected building automation controller: 62443-4-1 would require documented threat modeling before the architecture is finalized, while 62443-4-2 would specify concrete technical controls—authenticated firmware updates, encrypted credentials storage, role-based access control—each mapped to specific threat scenarios and testable in verification.

This bridges the gap between compliance language and engineering reality. For many organizations, this makes ISA/IEC 62443 not just an OT standard, but a mature and field-tested blueprint for secure product development across industries.

The Real Challenge Ahead

The biggest challenge is not technical. It is organizational.

Picture a product team facing CRA compliance:

- The product manager needs to understand new market requirements.
- Architects must integrate security controls without breaking existing designs.
- Developers need practical guidance on secure implementation
- And the security team must ensure everything is verifiable and documented.

Without a shared framework, these groups speak different languages.

The difficulty lies in aligning product management, engineering, and security; translating regulatory language into actionable requirements; scaling secure development across product lines; and maintaining security throughout years of maintenance and updates.

Organizations that treat security as architecture, not as paperwork, will be significantly better positioned. Secure products are not built by compliance alone. They are built through disciplined engineering applied consistently across the entire lifecycle.

Translating Requirements into Practice

Security frameworks, regulatory expectations, and engineering reality rarely align automatically.

I work with software-driven product organizations to embed security directly into their development lifecycle, focusing on structured threat modeling and product risk analysis, pragmatic implementation of ISA/IEC 62443-4-1 and 4-2, definition and rollout of Secure-by-Design development processes, and translating EU Cyber Resilience Act requirements into concrete engineering activities.

The goal is not additional overhead. It is disciplined product engineering that stands up to real-world threats and regulatory scrutiny.

About the author

Frank Leitner is a product security specialist focused on Secure-by-Design development practices, structured threat modeling, and the implementation of ISA/IEC 62443 in software-driven and connected products.

He supports organizations in embedding security into their development lifecycle and translating regulatory expectations, such as those introduced by the EU Cyber Resilience Act, into structured engineering processes, traceable requirements, and verifiable technical capabilities.

His work centers on aligning security architecture, product management, and engineering disciplines to enable sustainable, compliance-ready product development.