A Practical Reference Architecture for Cyber Resilience Act (CRA) Compliance

30 October 2025

The better the question. The better the answer.
The better the world works.

Silitics

CUMULOCITY

EY

Shape the future with confidence

Table of contents

Abstract

The EU Cyber Resilience Act (CRA) introduces broad cybersecurity obligations for products with digital elements, posing significant challenges for manufacturers in areas such as vulnerability monitoring, secure updates, and device integrity. This paper presents a modular reference architecture to help manufacturers address these challenges and achieve CRA compliance.

About

Cumulocity GmbH offers an enterprise-grade AIoT platform that connects & manages assets efficiently, transforms raw device data into AI-ready data, and orchestrates innovation from cloud to edge, combined with a team of experts and a large ecosystem of device, technology, and implementation partners to achieve lasting customer success.

EY Law GmbH Rechtsanwaltsgesellschaft Steuerberatungsgesellschaft and its Digital Law practice group offer interdisciplinary, risk-based legal advice with global reach on the EU Cyber Resilience Act. We translate legal requirements into actionable, scalable and field-tested compliance solutions for products with digital elements. Our legal advisory and compliance support spans the entire product lifecycle – from design and conformity procedures to post-market obligations, including reporting and communications with regulators.

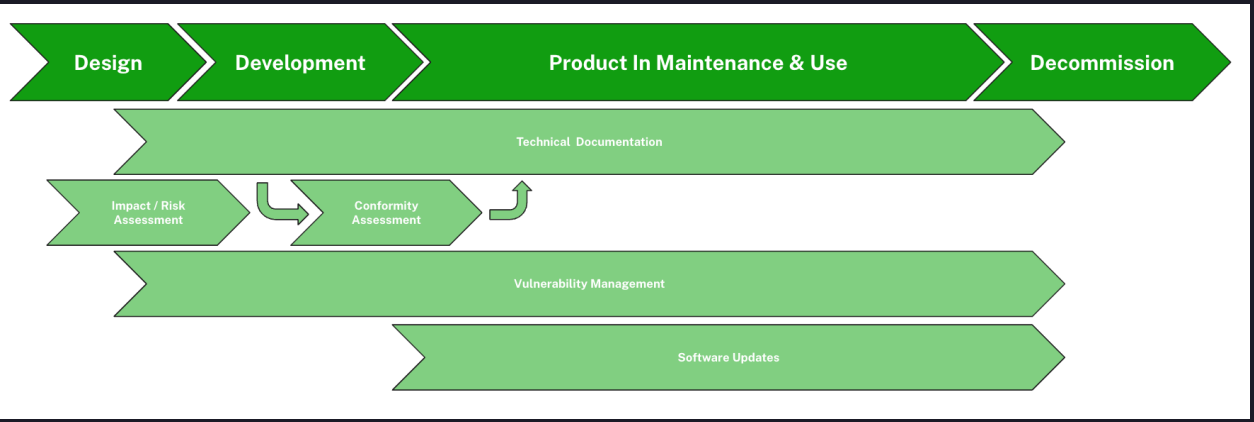
Silitics GmbH helps manufacturers build secure and reliable IoT devices by combining tailored engineering services with proven off-the-shelf solutions such as Rugix, an open-source project maintained by Silitics. Rugix provides a robust framework for building secure devices with efficient over-the-air update capabilities, forming a solid technical foundation for long-term security, maintenance, and regulatory compliance.

Introduction

The EU Cyber Resilience Act (CRA) introduces sweeping cybersecurity obligations for products with digital elements (hereinafter: PDE). It establishes and requires conformity with organizational and product specific obligations through common cybersecurity standards for PDEs in the EU, such as essential cybersecurity requirements relating to the properties of the PDE or vulnerability handling by the manufacturer, including secure development practices, establish incident reporting processes, and ensure ongoing product integrity and security throughout the product lifecycle.

For manufacturers of PDEs the CRA introduces both a challenge and an opportunity. The challenge lies in the breadth and rigor of the requirements, from vulnerability monitoring, device integrity & confidentiality, and update distribution to vulnerability disclosure policies and secure data deletion. The opportunity is the chance to modernize device infrastructure with proven tools and practices that not only meet legal requirements but also raise the bar for long-term product reliability and maintainability. As cybersecurity as a whole gains public visibility, this also becomes a significant factor for brand and product positioning.

The CRA will enter into full force on 11 December 2027, while its reporting obligations will already come into effect on 11 September 2026. For manufacturers of PDEs, the time to prepare is now. Delaying action risks non-compliance, which may lead to regulatory penalties, restricted access to the EU market, and reputational damage.



Product Development Lifecycle (Sample, developed for this document)

The diagram above shows a typical product development lifecycle of a PDE from design & development through the actual usage of the product until its decommission. Documentation is crucial for CRA compliance from the initial design stage until the final decommission. **Technical Documentation** is tied together with the **Impact & Risk Assessment** as well as the initial **Conformity Assessment**. While the diagram shows both the risk assessment and the conformity assessment as happening once during the early stages of the product development, in fact they are iterative processes that need to be repeated throughout the product lifecycle if the product or the potential for risk changes. The two main technical processes are **Vulnerability Management** starting the design phase and **Software Updates** starting once the product is in use. In vulnerability management the manufacturer keeps track of known and newly identified vulnerabilities, assesses their impact, and discloses them if required. In software updates, the manufacturer implements fixes to identified & assessed vulnerabilities and distributes them to their customers.

In the next sections, we discuss selected regulatory and technical challenges manufacturers face when implementing the CRA and present a modular reference architecture addressing those challenges. Particular caution was spent on clear cut interface descriptions between functional blocks of the architecture, enabling readers to follow our recommended software components, but also integrate existing technologies to reach CRA compliance efficiently.

1. Selected Regulatory Challenges

1.1 Applicability and scoping

Before considering applying CRA requirements to PDEs, manufacturers face the challenge f assessing and identifying whether the product in question falls within the scope of the CRA.

Firstly, manufacturers need to identify their PDEs. Secondly, manufacturers need to ensure compliance with the CRA only for PDEs that can be connected to another device or network, or where this is reasonably foreseeable.

Special attention is needed for system integrators and Original Equipment Manufacturers (OEM), where either multiple PDEs and/or other hardware and software components are combined. In such cases, defining the responsible manufacturer and the scope and responsibility for conformity can be complex. Here, the 'Blue Guide' on the implementation of EU product rules 2022 by the European Commission can provide some guidance, also considering products that are subject to multiple product safety legislations under the 'New Legislative Framework'.

1.2 Risk-based Approach and Documentation

When placing a PDE on the EU market, manufacturers must perform an assessment of the cybersecurity risks associated with the PDE and integrate its results into design, development, and production. The goal of this assessment: manage and reduce risks, prevent incidents, and reduce impact on health, safety, and data integrity.

This assessment, along with the applied essential cybersecurity requirements (Annex I Part I of the EU CRA) and vulnerability handling measures (Annex I Part II of the EU CRA), must be documented in the technical documentation. This documentation is then also the basis for the conformity assessment.

As a result, the essential cybersecurity requirements (see also the technical challenges in the next section) need to be applied with a risk-based approach to the PDE, meaning proportionate and adequate in relation to the identified risks.

2. Technical Challenges

The CRA establishes a broad set of requirements. In the previous section, we discussed the legal framework in which these requirements are embedded and the implications resulting from this. In this section, we summarize key technical challenges manufacturers face and outline the corresponding obligations defined in the CRA. We base this on the TR-03183 technical guideline currently being developed by the German Federal Office for Information Security (German: Bundesamt für Sicherheit in der Informationstechnik, abbreviated as BSI), a federal agency responsible for managing cybersecurity for the German government.[1] For reference, we will explicitly state the TR-03183 requirements that give rise to the respective challenges.

As outlined above, the full scope of CRA compliance also includes process and documentation requirements, which are critical for overall compliance, here we specifically focus on the technical and product considerations. Manufacturers that do not equally prioritize the technical requirements of the CRA will find it increasingly challenging to adapt and execute on their compliance plan.

2.1 SBOM, Vulnerability Monitoring, and Vulnerability Correction

A key requirement of the CRA stipulates that manufacturers must maintain a software bill of materials (SBOM) and monitor for vulnerabilities in all components, including inbuilt dependencies such as third-party libraries. Identified vulnerabilities must be documented and addressed through updates or other mitigations. Furthermore, devices can't be shipped with known vulnerabilities. Although not strictly required by the CRA, being able to assess the impact of vulnerabilities on individual devices of a fleet provides a significant operational advantage, as any countermeasures and alerts can be more targeted, particularly for manufacturers operating large device fleets.

Requirements: REQ_VH1, REQ_VH6, REQ_VH7, REQ_ER2

Challenge: Establishing a reliable and automated process to generate and maintain SBOMs, match them against known vulnerability databases, and assess their applicability to deployed devices.

2.2 Coordinated Vulnerability Disclosure

In addition to monitoring for known vulnerabilities, manufacturers are also required to implement and document a vulnerability disclosure policy. This policy must outline procedures for third-parties to responsibly disclose vulnerabilities to the manufacturer that they discover in the product. Upon resolution of a vulnerability, advisory information should be provided, preferably in a machine-readable format, to inform affected users about vulnerabilities and their mitigation. It is important to note that while disclosure to users is mandatory, public disclosure is not always explicitly required.

Requirements: REQ_VH4, REQ_VH5

Challenge: Creating a clear, reliable disclosure process that allows internal and external parties to report vulnerabilities and ensures that users receive meaningful updates and security advisories for the group of devices relevant to them when issues and recommendations are announced.

[1] We believe the BSI guidelines are a starting point for fully harmonized standards for CRA compliance at least in Germany.

2.3 Secure and Robust Update Process

The CRA requires that devices support secure, timely, and user-controllable software updates. While the CRA does not explicitly require updates to be delivered over-the-air, manufacturers relying on manual update processes, e.g., via USB sticks, will find it difficult and costly to provide timely updates at scale. According to the BSI guidelines, updates must be authenticated and integrity-protected and installable without compromising device functionality. Furthermore, security updates must be installed automatically. Users must be able to postpone functional updates, and any update failures must be clearly communicated.

Requirements: REQ_ER4, REQ_VH2, REQ_ER7.2, REQ_VH6

Challenge: Designing an update system that not only delivers new software versions but does so securely, atomically, and with rollback capabilities in case of failure, all while giving users transparency and control over the process.

2.4 Device Integrity and Confidentiality

Another key area targeted by the CRA is device integrity. Manufacturers must ensure that the device maintains integrity throughout its lifecycle. The CRA requires mechanisms to detect tampering and unauthorized modifications and to protect critical data such as keys, credentials, and personal data.

Requirements: REQ_ER6, REQ_ER7

Challenge: Providing a root of trust and secure boot process that prevents unauthorized system modifications and ensures that security-relevant and other sensitive data remains protected even in the case of physical access or malicious updates.

2.5 Logging and Security Monitoring

The CRA mandates that security-relevant events, such as configuration changes, failed login attempts, or service disruptions, be recorded and made available for retrospective analysis. These mechanisms must be active by default and resilient against common disruptions.

Requirements: REQ_ER13

Challenge: Implementing a comprehensive, tamper-resistant logging mechanism on the device and integrating it with backend systems for centralized monitoring, alerting, and long-term analysis.

2.6 Secure Factory Reset and Data Deletion

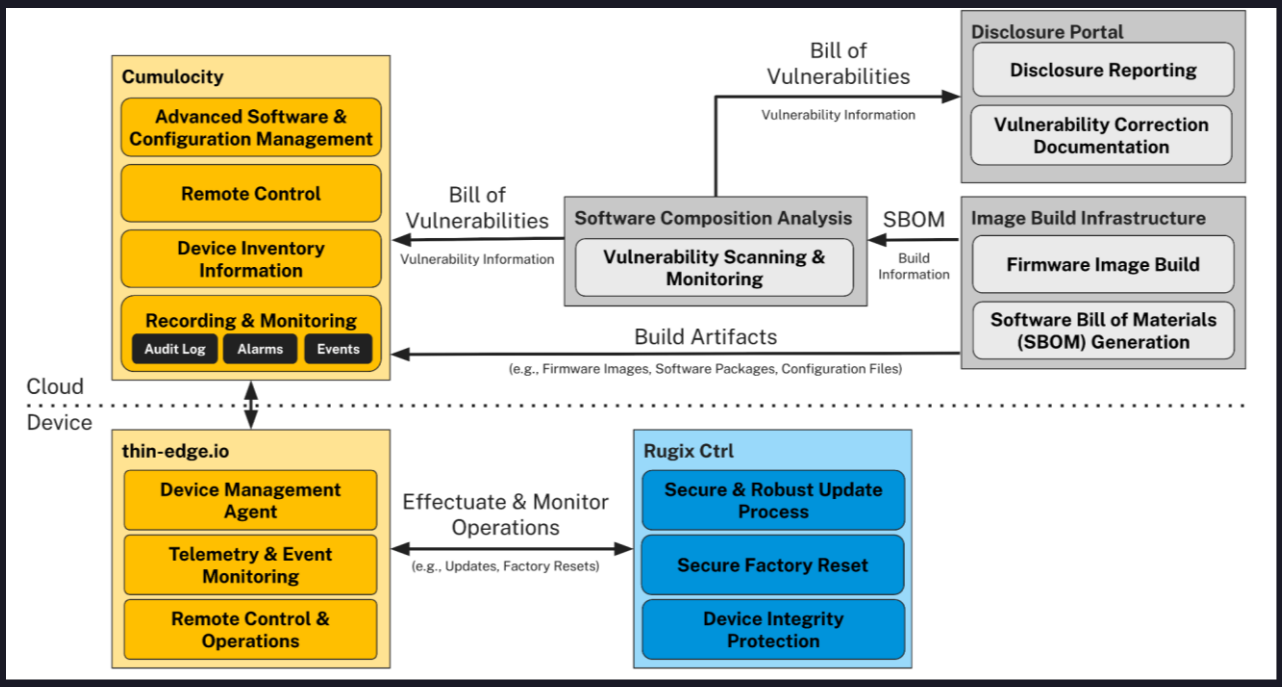
Devices must support secure deletion of personal and system data and allow users to reset the device to a clean and secure state. Where data is transferred off-device (e.g., to cloud services), secure deletion must be ensured at these remote locations as well.

Requirements: REQ_ER3, REQ_ER14

Challenge: Implementing factory reset and decommissioning processes that reliably remove sensitive data and restore a known-good system image free of residual configuration on device and in the cloud.

3. Reference Architecture[2]

Tackling the technical challenges introduced by the CRA, we present a reference architecture that addresses each of them by combining Rugix, Cumulocity, and complementary third-party tools. Each component plays a clearly scoped role in ensuring compliance.



Suggested Reference Architecture (by Cumulocity GmbH and Silitics GmbH)

3.1 Components

The reference architecture consists of five main components, each providing essential functionality towards meeting the outlined technical requirements of the CRA. Together, they form a modular, extensible system for building, operating, and maintaining secure connected devices at scale.

3.1.1 Rugix Ctrl

Rugix Ctrl provides the runtime foundation for building secure and maintainable embedded Linux devices. At its core is a robust system manager that combines over-the-air update functionality with built-in state management and lifecycle control. It is designed to operate reliably under real-world conditions and to enforce system integrity throughout the entire device lifecycle. Rugix Ctrl is compatible with a wide range of systems and Linux distributions, and comes with ready-made Yocto layers to get users started quickly.

Rugix Ctrl installs updates in an atomic and verifiable way, using cryptographic signatures to authenticate update payloads before applying them. The system supports A/B updates with automatic rollback in case of failure, as well as streaming and delta updates to reduce bandwidth and storage demands. Rugix integrates with secure boot processes to verify the system state at startup and can validate boot artifacts before handing over control.

Rugix Ctrl also provides secure factory reset functionality that restores the system to a known, trusted baseline and ensures that user data and credentials are reliably erased. Through its scriptable interface and integration capabilities, Rugix can be used with external fleet management systems like Cumulocity to coordinate updates, monitor device health, and react to vulnerabilities in the field.

[2] Some of the features described here are still under development and available as early previews. Contact us to learn more.

Key CRA-relevant capabilities:

- Secure, cryptographically verified software updates
- Atomic A/B deployments with rollback and streaming support
- Integrated state management for lifecycle control and recovery

  Boot-time integrity checks and secure boot integration
- Event logging for update actions and system transitions
- Secure factory reset with reliable data wiping
- Integration with backend systems for coordinated update and security management
- Written in a memory-safe language (see REQ_ER7.4)

3.1.2 System Build Infrastructure

The foundation for meeting many CRA requirements—especially around vulnerability monitoring, testing, and technical documentation—is a transparent and reproducible system build process. This includes not only the base operating system but also the applications and components developed by the manufacturer. A well-structured build pipeline must produce traceable artifacts, generate SBOMs, and automate testing to ensure that deployed systems are consistent, verifiable, and maintainable over time.

Manufacturers may use a variety of tools to build their systems, including Rugix Bakery, Yocto, or Buildroot. Regardless of the tooling, the build process must be tightly integrated with version control, testing infrastructure, and SBOM-aware vulnerability monitoring.

Rugix Bakery, another tool developed under the umbrella of the Rugix project, provides a streamlined and developer-friendly approach to building embedded Linux systems. It supports the creation of reproducible system images based on well-known base distributions, includes SBOM generation out of the box, and integrates with system testing and virtualization tools. Its container-based build environment enables teams to manage multiple system variants and embed the entire build process into CI/CD pipelines with minimal friction. While Rugix Ctrl is a core piece of the proposed architecture, Rugix Bakery is entirely optional as Rugix Ctrl can also be used with other build systems. In particular, the Rugix project provides ready-made, open-source Yocto recipes and layers.

The manufacturer's own software stack—whether implemented in C, C++, Rust, or other languages—must also be built in a way that contributes to the overall transparency of the system. This includes tracking dependencies, generating SBOMs where applicable, and ensuring that every change can be traced back to a signed artifact.

Key CRA-relevant capabilities:

- Automated generation of complete, machine-readable SBOMs
- Reproducible builds and traceable artifact generation
- Integration of the manufacturer's application code and dependencies
- Automated testing of system images and update behavior
- CI/CD integration for continuous validation and release control

3.1.3 Cumulocity

As IoT platform, Cumulocity serves as the cloud-based management and analytics platform in the architecture. As a part of its device management capabilities, Cumulocity collects, stores, and analyzes device metadata like software versions and update status. In addition, Cumulocity collects runtime telemetry data including security relevant events.

By centralizing this information and providing a fleet-wide view, Cumulocity enables manufacturers to evaluate system health, correlate vulnerabilities to deployed devices, and coordinate remediation across fleets.

The platform integrates directly with vulnerability tracking systems, allowing operators to identify which devices are impacted by a newly disclosed CVE. Logs streamed from devices (e.g., failed authentications, configuration changes, update failures) can be used to detect anomalies and trigger alerts. Cumulocity also supports controlled software rollouts, device provisioning, and access control.

Key CRA-relevant capabilities:

- Fleet-wide visibility into software versions and configurations
- Orchestrated updates of connected devices
- Device-centric vulnerability impact analysis, alerting, and reporting
- Collection & archival of security logs and runtime anomalies

3.1.4 Software Composition Analysis

To detect and evaluate known vulnerabilities in system components, the architecture incorporates SBOM-based monitoring tools such as Dependency-Track, BlackDuck, or similar platforms. These systems ingest SBOMs and continuously monitor public vulnerability databases like the NVD or GitHub Advisories. When a vulnerability is found in a known component, an alert is triggered, and affected devices can be identified by matching the SBOM against deployment metadata within Cumulocity.

These tools play a central role in supporting the CRA's requirement for ongoing vulnerability identification and risk assessment. By automating the detection and triage process, they reduce manual overhead and enable faster remediation workflows.

Key CRA-relevant capabilities:

- Continuous CVE monitoring and matching against SBOMs
- Generation of vulnerability reports and BOVs (Bills of Vulnerabilities).
- Risk scoring and prioritization for remediation
- Integration with CI/CD pipelines

3.1.5 Disclosure Infrastructure

The architecture assumes a lightweight but standards-compliant vulnerability disclosure platform. This can either be hosted directly by the manufacturer or delegated to an external provider. In Germany, for example, the Association for Electrical, Electronic & Information Technologies, in German VDE Verband der Elektrotechnik Elektronik Informationstechnik e. V., offers this through its CERT@VDE platform.

Manufacturers are expected to publish a vulnerability disclosure policy, maintain a security contact point, and issue security advisories when vulnerabilities are discovered and addressed.

Advisories should ideally be published in a machine-readable format such as CSAF (Common Security Advisory Framework) to support downstream automation. CERT@VDE can act as a disclosure intermediary, helping manufacturers manage coordinated disclosures and advisory publication, especially in the industrial and embedded domains.

Key CRA-relevant capabilities:

- Public vulnerability disclosure policy and reporting contact
- Publication of security advisories in structured formats

4. Call to Action

Manufacturers should not see the CRA as a regulatory hurdle but as an opportunity to modernize device infrastructure, adopt secure-by-design practices, and strengthen long-term product quality. Systems that meet CRA requirements are not only compliant—they are also more robust, more maintainable, and better protected against real-world cybersecurity threats.

Especially for manufacturers, strong product governance, including roles and responsibilities for risk assessments and vulnerability handling, as well as stringent development procedures with technical documentation is key to ultimately ensure compliance and product conformity under the EU CRA.

This white paper outlines a practical and modular reference architecture to achieve CRE compliance by addressing the challenges of vulnerability management and software updates. It proposes the use of proven tools: Cumulocity for device management and telemetry, Rugix for secure system operation and update management, and complementary components for vulnerability monitoring and disclosure. Together, these technologies form a scalable foundation that addresses the CRA's requirements without compromising development agility or operational flexibility.

Silitics and Cumulocity are ready to support you in evaluating your current architecture, identifying gaps, and implementing a solution that aligns with the CRA and your product roadmap as well as your current IT infrastructure and processes. Whether you need technical guidance, system integration support, or a tailored compliance strategy, we can help you get there.

Start today—because compliance in 2026 begins with architecture decisions you make now.

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EYG no. 008189-25Gbl

ED None

ey.com/de

Silitics

CUMULOCITY