

Cyber Resilience Act (CRA)

What manufacturers of products with digital elements should do now and how Sotronik supports them.

For whom?

Persons responsible and manufacturers (including software providers) of products with digital elements

What is it about?

The CRA requires security by design, vulnerability management, secure updates and robust evidence of the cybersecurity of your hardware and software products.

Sotronik focus:

Embedded systems, firmware development, PC applications, industrial communication, test systems

Why the CRA is relevant

The EU Cyber Resilience Act applies to hardware and software products with digital elements that are made available on the EU market. Its goal is to achieve a higher level of cybersecurity across the entire product life cycle, from development to product end-of-life, including the treatment of vulnerabilities and the provision of security updates.

The CRA regulation enters into force step by step:



Act now!

- The transition period is currently still in effect, but architecture, processes and documentation cannot be retrofitted at the last minute.
- Market risk: Non-compliant products risk bans, recalls, heavy fines and reputational damage.
- Competitive advantage: Early CRA compliance is increasingly demanded by OEMs, system integrators and operators.

Core obligations under the CRA

- Security by Design & Default in development and in the standard configuration
- Documentation including technical evidence and SBOM (software-bill-of-materials)
- Conformity assessment and CE marking
- Continuous risk analysis, vulnerability handling, security updates and provision of patches over the entire product life cycle
- Reporting obligations for actively exploited vulnerabilities and serious security incidents (early warning within 24 hours, report to the EU within 72 hours, final report within 14 or 30 days minor or major incident)

What this means for companies

- The CRA is binding and therefore not just a pure compliance topic.
- The CRA affects the architecture, development process, supply chain and operation of hardware/software products with digital elements that are sold in the EU.
- Early implementation reduces rework, accelerates approval and strengthens the trust of customers and partners.
- The technical implementation must fit the product reality not just the regulation.

Cyber Resilience Act (CRA)

Sotronik as implementation partner

Thanks to our many years of experience in hardware and software development, we understand the challenges that manufacturers and their products face over an entire product life cycle.

Our employees trained on the Cyber Resilience Act actively support you in further developing your products to be future-proof while at the same time meeting the new regulatory requirements.

Approach model for CRA readiness with Sotronik

1. Clarify scope and impact

Classification of whether the product falls under the CRA, which components are relevant and which roles are assumed by manufacturers, integrators or distribution partners.

2. Perform product and risk analysis

Evaluation of architecture, interfaces, data flows, remote access, update mechanisms and third-party components; prioritization of critical vulnerabilities and attack surfaces.

3. Implement technical measures

Application of security-by-design and security-by-default principles; implementation of hardening measures, secure communication protocols, authentication mechanisms and cryptographic methods, as well as ensuring the products update and patch capability.

4. Build evidence and processes

SBOM, technical documentation, test evidence, vulnerability management, release and support processes, and clear definition of internal responsibilities.

5. Secure verification and operation

Establish tests, reviews and repeatable test procedures; prepare reporting and response processes and actively support products over the support period.

Added value for persons responsible and manufacturers

Faster implementation

Thanks to our many years of development experience, standardized processes and employees trained in the CRA.

Lower project risk

Because security, update capability, communication, reporting processes and tests are considered together right from the start.

Practical rather than abstract

Because Sotronik has been implementing technical solutions for many years in real products, plants and IoT/remote control systems.

Sotronik supports CRA readiness where it is decided: in architecture, firmware, communication, testing and technical implementation – partially or completely from A to Z.

Cyber Resilience Act (CRA)