

Greater security in industrial automation

Technology report

New Cyber Resilience Act regulation (CRA (EU) 2024/2847)



The Cyber Resilience Act focuses on new requirements for digital, networked products. Find out how Leuze is making its sensor solutions ready for the future – and what customers need to know.

In 2024, the EU enacted the Cyber Resilience Act (CRA (EU) 2024/2847), a cybersecurity regulation that will come into effect in phases:

**09
26**

Starting September 11, 2026, manufacturers of products with digital elements will be required to report serious security incidents and actively exploited vulnerabilities to a central EU platform (Single Reporting Platform).

**01
27**

In January 2027, the new Machinery Regulation (EU) 2023/1230 will take effect, setting specific requirements for cybersecurity and digital safety components.

**12
27**

From December 2027, all new digital products placed on the market must be CRA-compliant. For manufacturers, this means they must assess and document cyber risks, establish a “Secure Development Life Cycle,” and may only bring products to market that are protected against cyber-attacks in accordance with the current state of the art.

Cybersecurity for connected industrial systems

This is particularly important for industrial automation: In many industrial environments, legacy systems operate alongside modern digital systems. As machinery and control systems usually remain in use for many years, vulnerabilities can persist for a long time. At the same time, as connectivity increases, so does the attack surface. Even minor security vulnerabilities can result in production downtime or the loss of sensitive operational data. This is exactly where the CRA comes in: It is designed to ensure the security of devices with digital components – including many Leuze sensors – during development, operation, and throughout the entire product lifecycle. An important factor here is the ability to receive updates. The CRA requires that security updates be technically feasible and that manufacturers make them available as needed. Users thus benefit from products that are developed, operated, and supported in accordance with the latest security standards.

For which system components is the CRA relevant?

The CRA applies to all products with digitally networked components available on the EU market. These include networked hardware such as sensors and control systems, as well as software solutions in automated systems' networks. The regulation requires manufacturers such as Leuze to conduct a systematic risk assessment to determine whether products are potentially vulnerable to cyberattacks. If risks are identified, countermeasures are taken. Proof of CRA compliance will be an integral part of the EU Declaration of Conformity in the future.

For newly developed sensors, the manufacturer guarantees through the EU Declaration of Conformity that they are protected against cyberattacks. When integrating sensors, machine builders must assess the risks to the entire system – similar to safety processes – and, if necessary, adapt their existing security concepts. Operators and integrators define a security level and the corresponding technical requirements, such as network segmentation with firewalls, user management, or logging systems. The sensors support this architecture to achieve the system's defined security level. This provides end customers with machines that are reliable in the long term and resilient against attacks, production downtime, and the loss of sensitive data. Existing products that have already been installed in systems or are in storage do not necessarily need to be modified.

The CRA lays the foundation for secure, connected industrial facilities – from development through the entire product lifecycle.

How manufacturers implement the requirements

Leuze began integrating the CRA's requirements into its development and production processes at an early stage. The company's many years of expertise in the field of safety – that is, workplace safety and personal protection – facilitated its expansion into security processes that ensure the protection of systems and networks against external attack scenarios. Both fields require comparable strategies and processes. The cornerstones of implementation are:

- **Security by design** – digital products are developed in accordance with cybersecurity's current state of the art. In the context of sensors, this specifically means that their architecture has been enhanced for security and includes, among other things, secure boot and file systems: Upon startup, the loaded software is validated and verified using security features on the device hardware. Data on the sensors is protected against tampering, and the system architecture enables encrypted data transmission over the sensors' communication channels.
- **Security by default** – the factory settings are designed to be cyber-secure by default, and all optional interfaces are disabled. Every user access must be authenticated. Sensors can be reset to factory settings at any time, and customer-specific data can be deleted.
- **Update capability** – digital products in operation can be updated to the latest security standards. Where appropriate, updates are enabled via the process interface. If an update fails, the system reverts to the previous secure state.

Wie der CRA die Produktentwicklung verändert

Im Entwicklungsprozess neuer Sensoren werden alle Phasen um Security-Aspekte ergänzt. Dazu gehören:

- **Systematische Bedrohungsanalyse:** Leuze erstellt eine Risikomatrix, die mögliche Angriffsszenarien prüft und bewertet.
- **Minimierung von Angriffsflächen:** Bereits bei der Produktentwicklung werden strenge Sicherheitsanforderungen integriert.
- **Bereitstellen von Sicherheitsupdates:** Für die Nutzungsdauer ihrer Sensoren definiert Leuze Lebenszyklen. Sie legen die Supportdauer fest und regeln die Produktnachfolge. Leuze sorgt dafür, dass Kunden während der geplanten Nutzungsdauer der Produkte regelmäßig Updates erhalten. Diese sichern die Funktionalität und schließen erkannte Schwachstellen. Außerdem werden Mechanismen entwickelt, um alle Leuze-Produkte innerhalb einer Anlage gesammelt updaten zu können.
- **Dokumentation:** Für jedes Produkt werden umfassende Dokumentationen erstellt, die Kunden bei der sicheren Anwendung unterstützen.
- **Schwachstellenmanagement und Schwachstellenmeldung:** Leuze hat Prozesse etabliert, um Schwachstellen zu identifizieren, zu verwalten und im Ernstfall innerhalb der im CRA formulierten Fristen schnell zu melden.

So unterstützt Leuze bei der CRA-Umsetzung

Als Partner für sichere Sensorlösungen begleitet Leuze die Anwender der Produkte durch die Übergangszeit bis zur vollständigen Umsetzung des CRA. Der Sensorhersteller informiert über die Anforderungen und vermittelt Best-Practice-Ansätze. Kunden erhalten Beratung zu ihren Fragen rund um den CRA – von der Auswahl geeigneter Produkte bis zur sicheren Integration in bestehende Anlagen. Das Informationsangebot umfasst:

- **Individuelle Beratung:** Experten stehen bereit, um Kunden bei der Bewertung ihrer Anlagen und Komponenten zu unterstützen.
- **Anwendungsempfehlungen:** Leuze gibt konkrete Hinweise, wie Sensoren und Steuerungen sicher betrieben werden können.
- **Unterstützung bei der Dokumentation:** Kunden erhalten Hilfe bei der Erstellung der notwendigen technischen Dokumentationen.
- **Informationen zu Meldeprozessen:** Leuze erklärt, wie Sicherheitsvorfälle gemeldet werden und welche Schritte im Ernstfall zu beachten sind.



Herbert Köbel

**Senior Expert –
R&D Software**

Leuze electronic GmbH + Co. KG

In der Braike 1, 73277 Owen

T +49 7021 573-0

F +49 7021 573-199

info@leuze.com

www.leuze.com