EU regulation on cybersecurity

AMKmotion
MEMBER OF THE ARBURG FAMILY

Another new regulation?

- Cyber Resilience Act (CRA), Regulation (EU) 2024/2847 of October 2024.
- EU regulations have direct legal effect.
- The CE marking framework has been expanded to include the CRA. Compliance with the CRA therefore complements requirements such as the EMC Directive, the Low Voltage Directive and the Machinery Directive as evidence of compliance with EU digital security requirements.

What is new about this regulation?

- The CRA is the first regulation to address the cybersecurity of products with digital elements that include interfaces enabling direct or indirect connectivity with other devices. It applies to both hardware and software.

What are the objectives of the regulation?

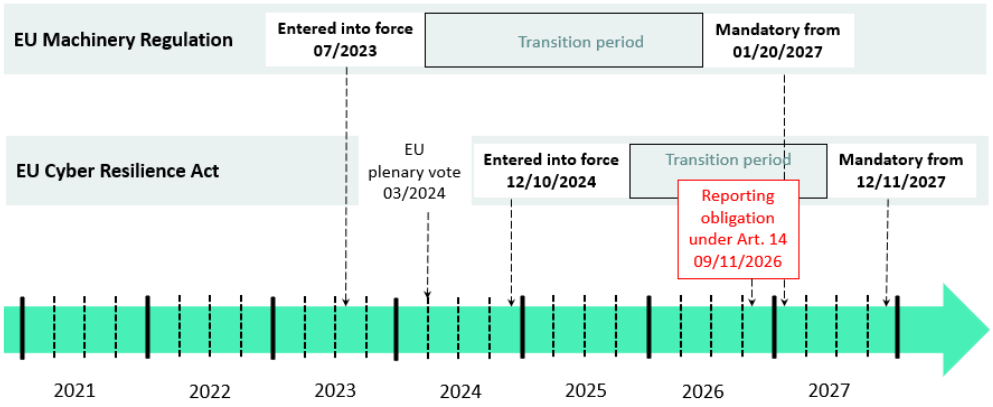
- Increase cybersecurity across the board.
- Establish minimum cybersecurity requirements for products placed on the EU market.
- Require manufacturers to adopt a security-by-design approach.
- Ensure product security throughout the entire lifecycle:
  - Product monitoring obligations for manufacturers and incident reporting mechanisms.
  - Vulnerability management by manufacturers for the product lifetime, and for at least five years.

Why is this necessary?

- Cyberattacks are placing an increasing burden on industry and the economy.
- The high degree of connectivity creates significant risks and potential attack vectors.

Who and what is affected in industry?

- Manufacturers and distributors of components with digital elements
- Machine manufacturers:
  - The new Machinery Regulation (2023/1230) also requires protection against threats posed by malicious third parties and emphasizes compliance with additional cybersecurity requirements.
- IT and IoT devices and systems, control technology.
- Networks and communication interfaces (physical, logical and wireless)
- Software and hardware interfaces

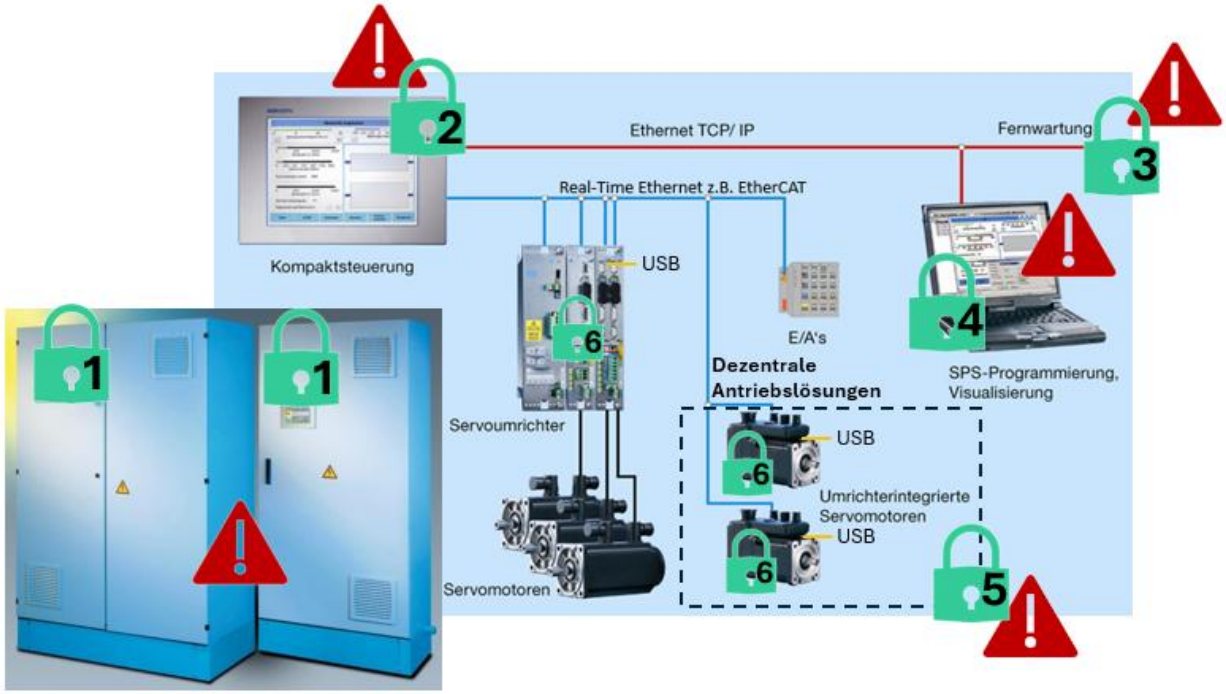


What CRA deadlines must be observed?

- The reporting obligation applies from September 11, 2026, and this includes products that are already on the market!
  Manufacturers are subject to mandatory reporting and notification requirements for actively exploited vulnerabilities and security incidents in accordance with Article 14 of the CRA.

AMKmotion
MEMBER OF THE ARBURG FAMILY

Affected interfaces in machines, systems and components



Potential areas of exposure
Protective devices

Risk assessment by the plant operator
Examples of potential areas of exposure and protective measures:

1 Restrict access to production facilities, equipment and switch cabinets to authorized personnel only.
2 Protect control systems against malware and secure fieldbus networks.
3 Implement IT security measures to protect both corporate and plant networks.
4 Protect PCs against malware and avoid the use of inadequately secured hotspots for wireless connections.
5 Protect systems against unauthorized access by means of distributed devices.
6 AMKmotion secures areas of exposure at the drive component level:
  a. Service interfaces on decentralized drives are protected with screw-on covers.
  b. Central devices are protected against unauthorized access within the switch cabinet.
  c. EtherCAT is an open, high-performance interface secured through the
    - single-master architecture.
    - Only the EtherCAT master can secure the EtherCAT interface and controls all data exchanged with the drives.
    - No IP traffic.
  d. Firmware packages are verified for authenticity within the drive. This prevents malware from being hidden within the drives.
  e. Drives accept only data packets based on the AMKmotion communication protocol, and AIPEX 5 communicates with the drives exclusively through this protocol.
  f. All AIPEX 5 communication is encrypted and ultimately depends on the protection level of the PC and the underlying IT infrastructure.

Additional measures

- Do not create global administrator accounts for your systems.
- Prevent the use of inadequately secured remote access connections.
- As part of your risk assessment, analyze foreseeable misuse scenarios and implement measures to prevent them wherever possible.