AMKmotion

MEMBER OF THE ARBURG FAMILY

Cyber-Security at AMKmotion

Requirements. Responsibilities. Our solutions.

01 Introduction to the Cyber Resilience Act (CRA)

01 Cyber Resilience Act

- The CRA is the first European regulation to establish a minimum level of cybersecurity for all connected products available on the EU market.
- Its objective is to improve cybersecurity throughout the European Union.
- The new requirements apply in all EU member states.
- Implementation will take place in several stages through the end of 2027.

02 Why cybersecurity?

- **More connectivity = greater risk**
  - Nowadays, machines and production systems are closely connected to IT and OT systems.*
  - Technologies such as Ethernet, remote access and digital services have become standard
  - → As a result, new attack surfaces are created for cyberattacks
- **Potential consequences of cyberattacks**
  - Machine downtime and production outages
  - Data loss and loss of know-how
  - Cyberattacks can directly affect safety-related machine functions.
- **Cybersecurity is the foundation for**
  - functional safety and confidentiality
  - availability and reliability
  - competitiveness

*IT = Information Technology
OT = Operational Technology

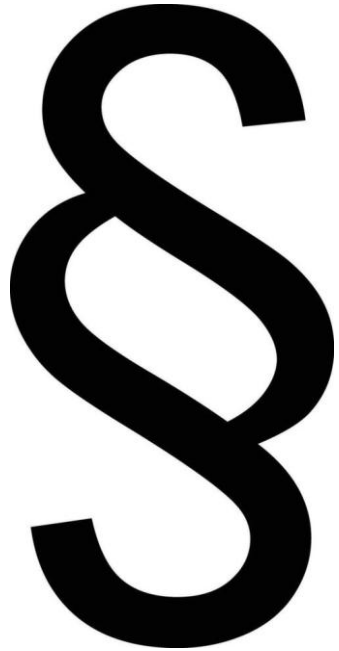
03 Relevance for machine manufacturers and operators

- **Cybersecurity is becoming a product requirement**
  - Relevant for machines, control systems and drive systems
- **Applies throughout the entire lifecycle**
  - Development → Commissioning → Service → Retrofit
- **Responsibility extends across multiple areas**
  - Not limited to IT
  - Machine builders and automation specialists also have responsibilities
- **Direct impact of security incidents**
  - Operator safety
  - Production continuity and delivery capability
  - Operational reliability
  - Reputation and liability

04 Regulatory framework for cybersecurity

- **Cybersecurity is becoming mandatory**

- **Overview of key frameworks**
  - **IEC 62443**
    → State of the art for industrial systems
  - **NIS2**
    → Requirements relating to organizational measures, operations and incident handling
  - **Cyber Resilience Act (CRA)**
    → Requirements for products with software and interfaces, as well as their manufacturers



02 Tasks and responsibilities

05 Manufacturer responsibilities

- **CE marking – the legal foundation**
  - CE marking is only permitted if all applicable CE-related EU requirements have been fulfilled
  - The manufacturer declares conformity on its own responsibility

- **CE-relevant directives and regulations**
  - Machinery Directives / Machinery Regulation
  - Low Voltage Directive and EMC Directive
  - Other product-specific requirements
  - **New: Cyber Resilience Act (CRA)**

- **Risks of incorrect CE marking**
  - Administrative offense or criminal offense
  - Market surveillance measures
  - Fines and liability risks

- **What changes under the CRA?**
  - Cybersecurity becomes **part of CE conformity**
  - Applies to all products with digital elements
  - Manufacturers bear responsibility throughout the **entire product lifecycle**

06 Cybersecurity in drive systems – responsibilities

Security requires collaboration

AMKmotion (component level)

- **Physical protection**
  - Service interfaces covered and protected
  - Central devices protected within the switch cabinet
- **Secure communication**
  - EtherCAT with single-master architecture
  - Controlled data flow through the master
  - No IP traffic -> reduced attack surface
- **Tamper protection**
  - Firmware authenticity verification
  - Prevents malware from being installed on drives
- **Access and data**
  - Only proprietary protocols are permitted
  - Communication via AIPEX 5 is encrypted

Machine manufacturers/operators (system level)

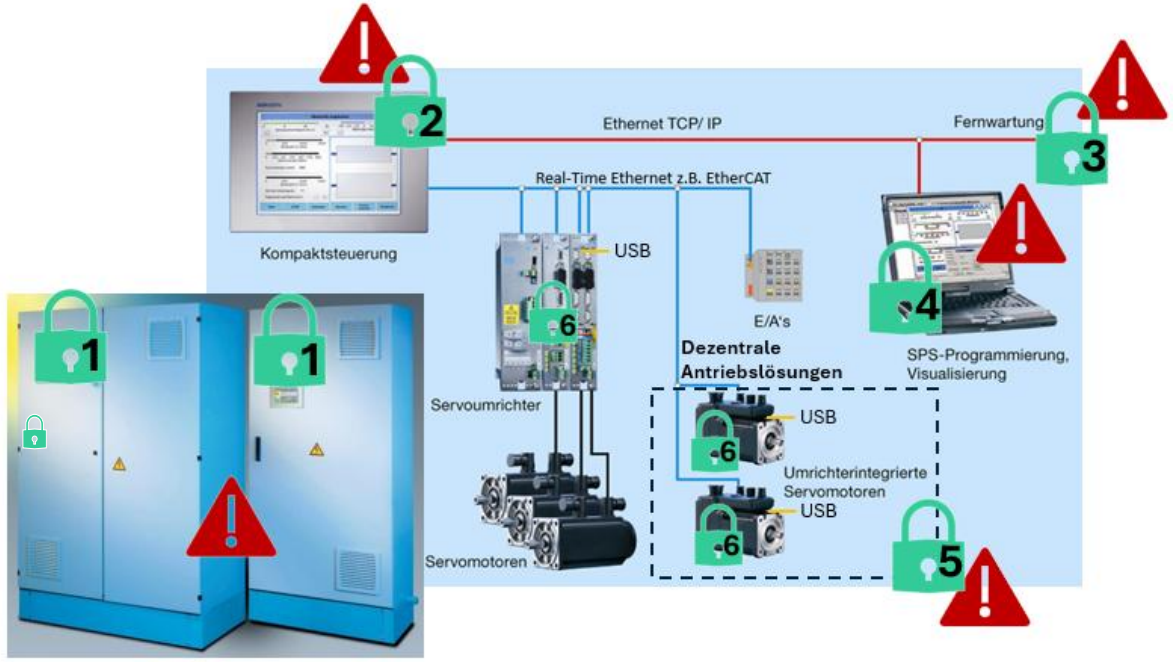
- **Access management**
  - No global administrator accounts
- **Remote access**
  - Avoid unsecured connections
- **Risk management**
  - Analyze security risks at an early stage
  - Consider and prevent foreseeable misuse
- **Holistic security**
  - Ensure secure interaction between components and the overall system

07 Risk and threat analysis for machines

Relevant interfaces – checklist for machine manufacturers' risk assessments

Typical areas of exposure:

1. **Physical access**
   – Restrict access to production facilities, equipment and switch cabinets to authorized personnel only
2. **Control systems and fieldbus networks**
   – Protect control systems against malware and secure fieldbus networks
3. **IT and network infrastructure**
   – Implement IT security measures to protect corporate and plant networks
4. **Industrial PCs and wireless connections**
   – Protect industrial PCs against malware and avoid unsecured Wi-Fi or hotspot connections
5. **Decentralized systems**
   – Protect systems against unauthorized access by means of decentralized devices
6. **AMKmotion secures key areas of exposure at the drive component level**



Potential areas of exposure

Protective devices

08 Vulnerability management and transparency

Why is this important?

- Managing vulnerabilities is becoming a mandatory requirement
- Transparency throughout the entire product lifecycle is essential

Timeline

- **Starting September 2026 → Mandatory reporting of actively exploited vulnerabilities**
- **Starting December 2027 → Mandatory implementation of a structured vulnerability management process**

Objectives

- Identify vulnerabilities at an early stage
- Assess risks in a transparent and verifiable manner
- Implement mitigation measures quickly

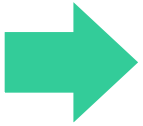
09 Vulnerability management and transparency

Requirements for machine manufacturers

- Actively monitor vulnerabilities affecting machines and components
- Establish clear assessment and decision-making processes for security-related information
- Communicate cybersecurity risks transparently to customers and operators

Key building blocks

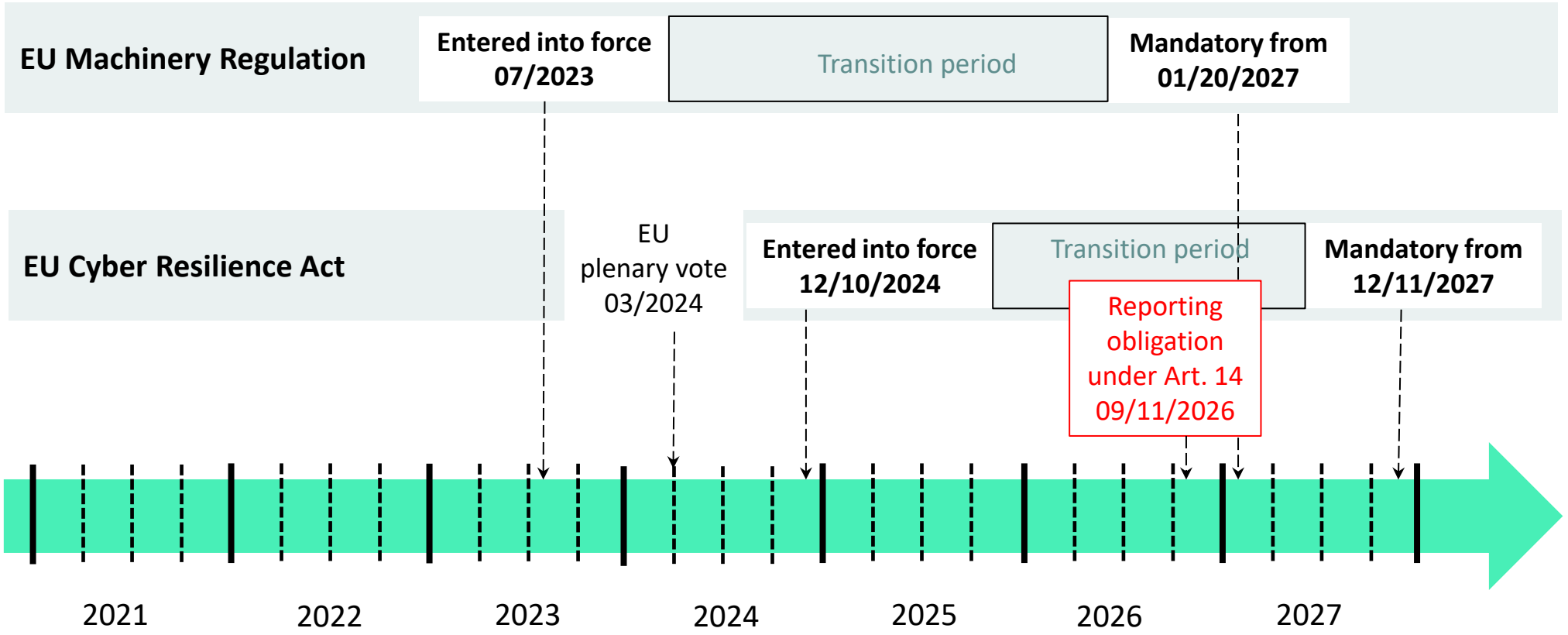
- **PSIRT** (Product Security Incident Response Team) → central unit responsible for handling security incidents
- **SBOM** (Software Bill of Materials)
  - Structured inventory of software components used
  - Visibility into dependencies within a product



The structured identification and tracking of security risks is becoming a mandatory and integral part of product responsibility

02 Timeline of relevant EU regulations

10 Timeline of relevant EU regulations



03 Cybersecurity at AMKmotion

11 Cybersecurity at AMKmotion – current status and next steps

Already implemented

- Rapid response through the PSIRT (Product Security Incident Response Team)
- Clearly defined processes for:
  - reporting, assessing and prioritizing security incidents
  - continuous monitoring of security-relevant topics
- Central security contact point with ticketing system
  - structured tracking and management of security cases
  - clearly defined PSIRT responsibilities

Currently being implemented

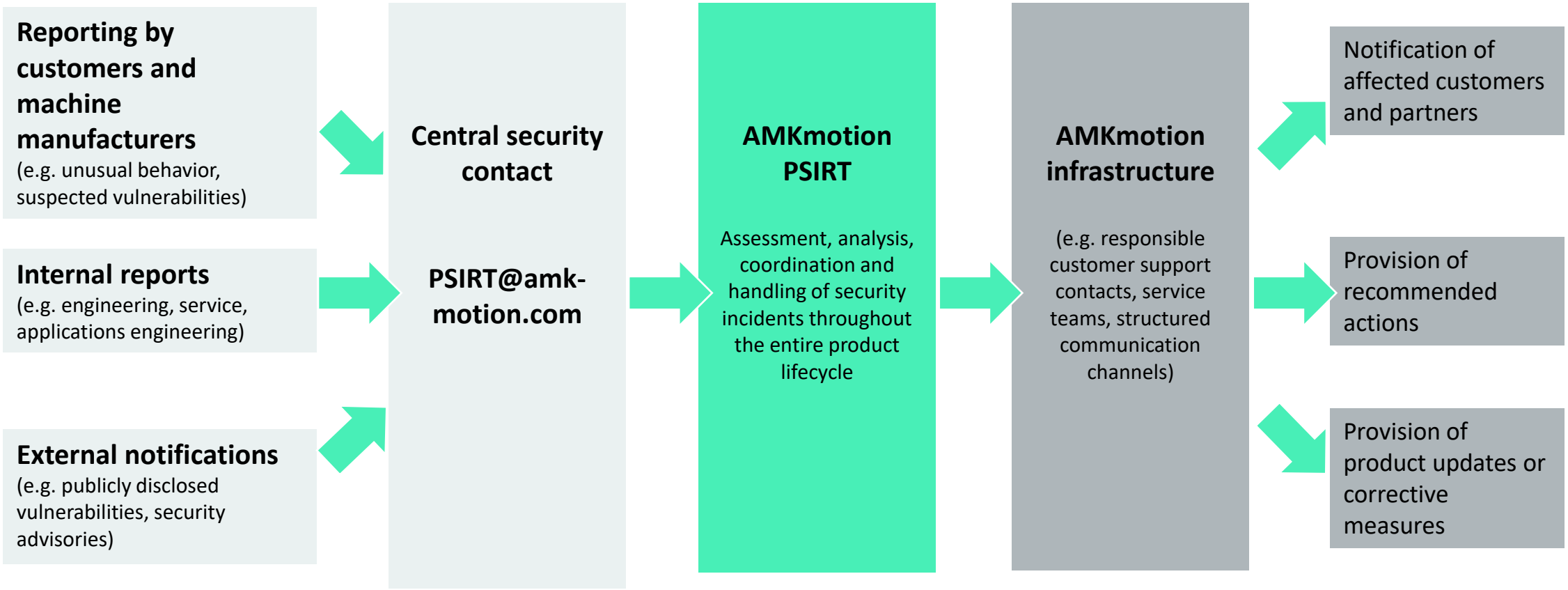
- Risk assessments for AMKmotion products
- Creation of Software Bills of Materials (SBOMs)
- Development of a customer-focused patch and update strategy
- Implementation of structured security testing
- Regular code reviews for security-critical functions

Further development

- Structured external communication of security-related information
- Gradual expansion of processes and transparency throughout the product lifecycle
- Close coordination between internal departments, including engineering, product management, applications engineering and IT.

AMKmotion has established the organizational and technical foundations for cybersecurity and is already aligning its processes with future regulatory requirements under the Cyber Resilience Act (CRA).

12 Security incident reporting process



13 AMKmotion PSIRT team

PSIRT@amk-motion.com

AMKmotion

MEMBER OF THE ARBURG FAMILY

AMKmotion GmbH + Co KG

Gaußstraße 37-39
73230 Kirchheim unter Teck
Germany

+49 7021 5005 0
info@amk-motion.com