AMKmotion

MEMBER OF THE ARBURG FAMILY

Cyber-Security at AMKmotion

Security by design for modern drive systems

01 Introduction to the Cyber Resilience Act (CRA) and its relevance for machine manufacturers and operators

01 Why cybersecurity?

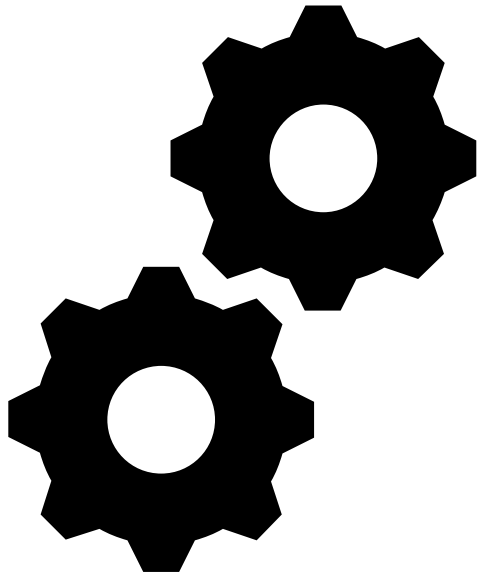
- The increasing connectivity of machines and equipment is resulting in ever closer integration between IT and OT systems*. **Ethernet-based communication, remote access and digital services are now integral components of modern automation solutions.** At the same time, this creates new attack surfaces for cyberattacks.
- As a result, cybersecurity is no longer limited to traditional IT systems: it is becoming increasingly important for machines and production facilities as well. Potential consequences include **machine downtime, production outages and the loss of data and application-specific know-how**.
- As such, cybersecurity is becoming a fundamental prerequisite for functional safety, availability, reliability and competitiveness. Tampering and cyberattacks can directly affect safety-related machine functions.

* IT (Information Technology): Systems used to process, store and transmit data, such as office IT, servers, networks and cloud services.
OT (Operational Technology): Systems used to control and monitor machines and equipment, such as controllers, drives, sensors and industrial networks.

02 Relevance for machine manufacturers and operators

Cybersecurity as an obligation and a responsibility

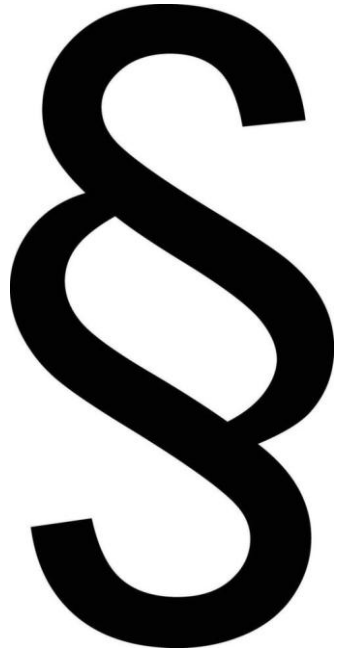
- Cybersecurity protects the **functional safety, availability, integrity** and **confidentiality** of machines and equipment
- Machines and drive systems are increasingly becoming part of connected overall systems. Security incidents have a direct impact on:
  - operator safety
  - production continuity and delivery capability
  - operational reliability
  - reputation and liability
- Cybersecurity affects the **entire lifecycle** of a machine – from development and startup through service and retrofit
- Responsibility lies not just with IT departments, but also with **machine builders and automation specialists**



03 Regulatory framework for cybersecurity

Cybersecurity is becoming a regulatory requirement

- Overview of key frameworks
  - **DIN EN IEC 62443 series**
    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
- Cybersecurity is not solely an IT issue; it is also **highly relevant to products and machines**



02 CE marking as the legal foundation

CE marking – the manufacturer’s responsibility

- **CE marking may only be applied if a product complies with all applicable EU legislation**
- By applying the CE mark, the manufacturer declares compliance on its own responsibility, for example with:
  - the Machinery Directive / Machinery Regulation
  - the Low Voltage Directive and EMC Directive
  - other product-specific legislation
  - and now also with the Cyber Resilience Act
    As a result, CRA compliance is now part of CE conformity for all products with digital elements, including components and machines.
    Manufacturers bear responsibility throughout the entire product lifecycle.

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

03 Tasks and responsibilities

05 Tasks and responsibilities

Legal framework	CRA	NIS2
Legal responsibility	AMKmotion Machine manufacturers	Machine operators AMKmotion Only in their capacity as operators of their own machine fleet
Applies to products, components and machines	Products • Firmware (hardware-integrated software) • Software Machine designs	Corporate infrastructure • IT and OT networks • Production and logistics • Office areas

AMKmotion as a component manufacturer

- Supports machine manufacturers in implementing cybersecurity requirements by means of appropriate products and functions
- Complies with **applicable legal and standards-based requirements**
- A dedicated **Product Security Incident Response Team (PSIRT)** provides fast and targeted support in the event of security incidents
- Acts as a **technical expert and trusted partner**

Machine manufacturers as system manufacturers

- Develops the **cybersecurity concept for the machine** and the overall system
- Is responsible for protecting both its own data and operator-relevant data and know-how at machine level
- Implements technical and organizational measures to **ensure machine availability and security**
- Complies with applicable **legal and standards-based requirements** (e.g. CE marking, CRA obligations for machines, establishment of a PSIRT team)
- Establishes processes for **handling security incidents** during machine operation

06 Vulnerability management and transparency

Managing vulnerabilities, reporting obligations and transparency throughout the product lifecycle

Timeline

Starting September 2026

- Mandatory reporting of **actively exploited vulnerabilities and security incidents**

Starting December 2027

- Implementation of a **permanent and structured vulnerability management process**

Objectives:

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

Requirements for machine manufacturers

In the future, machine manufacturers will be required to:

- **systematically monitor vulnerabilities in machines and the components used**
- establish **assessment and decision-making processes** for security-related information
- **communicate relevant cybersecurity risks transparently to operators and customers.**

Key building blocks for implementation

PSIRT – Product Security Incident Response Team

- The central organizational unit for handling security-related 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 indispensable and is increasingly required by regulation

07 Cybersecurity in drive systems – responsibilities

Security requires collaboration

AMKmotion (component level)

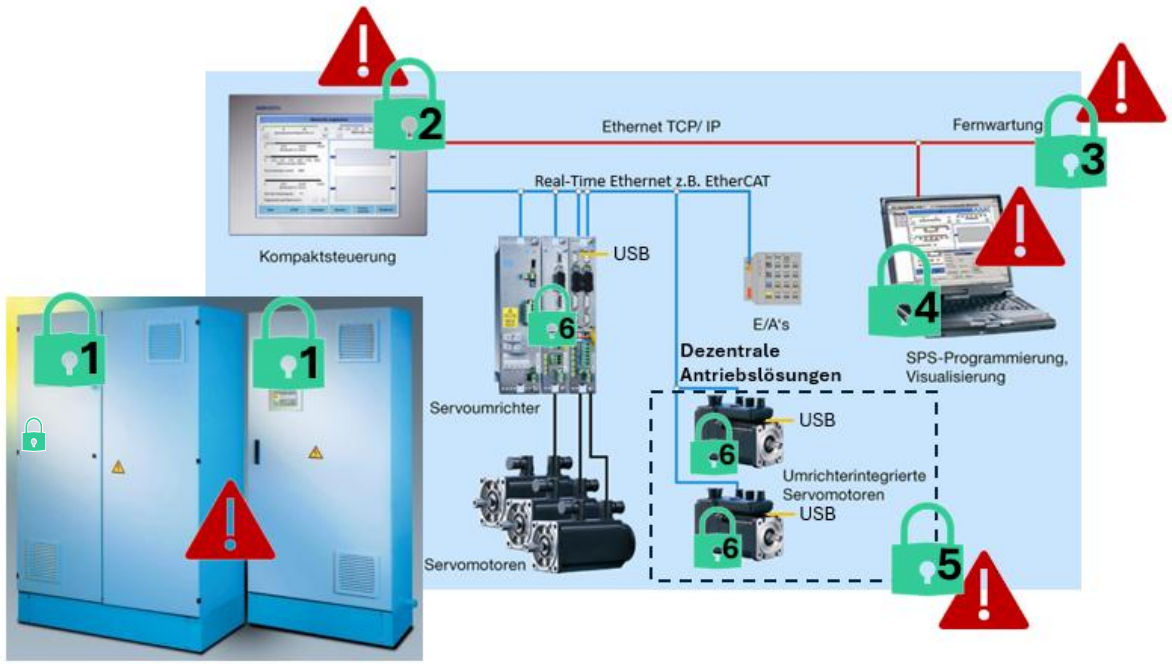
- **Physical protection**
  - Service interfaces covered and protected
  - Central devices protected within the switch cabinet
- **Secure communication**
  - EtherCAT with single-master architecture
  - Controlled data flow through the master
  - No IP traffic -> reduced attack surface
- **Tamper protection**
  - 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

08 Risk and threat analysis for machines

Relevant interfaces – checklist for machine manufacturers' risk assessments



Potential areas of exposure

Protective devices

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. **Distributed systems**
   – Protect systems against unauthorized access by means of distributed devices
6. **AMKmotion secures key areas of exposure at the drive component level**

09 Risk and threat analysis for machines

AMKmotion protects drive components through security-by-design measures:

- Service interfaces on decentralized drives are protected with screw-on covers
- Central devices are protected against unauthorized access within the switch cabinet
- EtherCAT is an open, high-performance interface secured through its architecture:
  - **Single-master architecture**, which virtually eliminates risks associated with sub-devices
  - Only the EtherCAT master can secure the EtherCAT interface and controls all data exchanged with the drives
  - **No IP traffic**, significantly reducing the attack surface of the components

- Firmware packages are verified for authenticity within the drive. This allows tampering attempts to be detected and prevents malware from being hidden within the drives
- In addition to control communication, AMKmotion drives accept only data based on the company's proprietary communication protocol. This protocol is used by the AIPEX 5 startup software. As a result, potential attack vectors are minimized.
- All AIPEX 5 communication is encrypted and ultimately depends on the protection level of the PC and the underlying IT infrastructure

09 Risk and threat analysis for machines

AMKmotion protects drive components through security-by-design measures

- Service interfaces on decentralized drives are protected with screw-on covers
- Central devices are protected against unauthorized access within the switch cabinet
- EtherCAT is an open, high-performance interface secured through its architecture:
  - **Single-master architecture**, which virtually eliminates risks associated with sub-devices
  - Only the EtherCAT master can secure the EtherCAT interface and controls all data exchanged with the drives
  - **No IP traffic**, significantly reducing the attack surface of the components
- Firmware packages are verified for authenticity within the drive. This allows tampering attempts to be detected and prevents malware from being hidden within the drives
- In addition to control communication, AMKmotion drives accept only data based on the company's proprietary communication protocol. This protocol is used by the AIPEX 5 startup software. As a result, potential attack vectors are minimized.
- All AIPEX 5 communication is encrypted and ultimately depends on the protection level of the PC and the underlying IT infrastructure

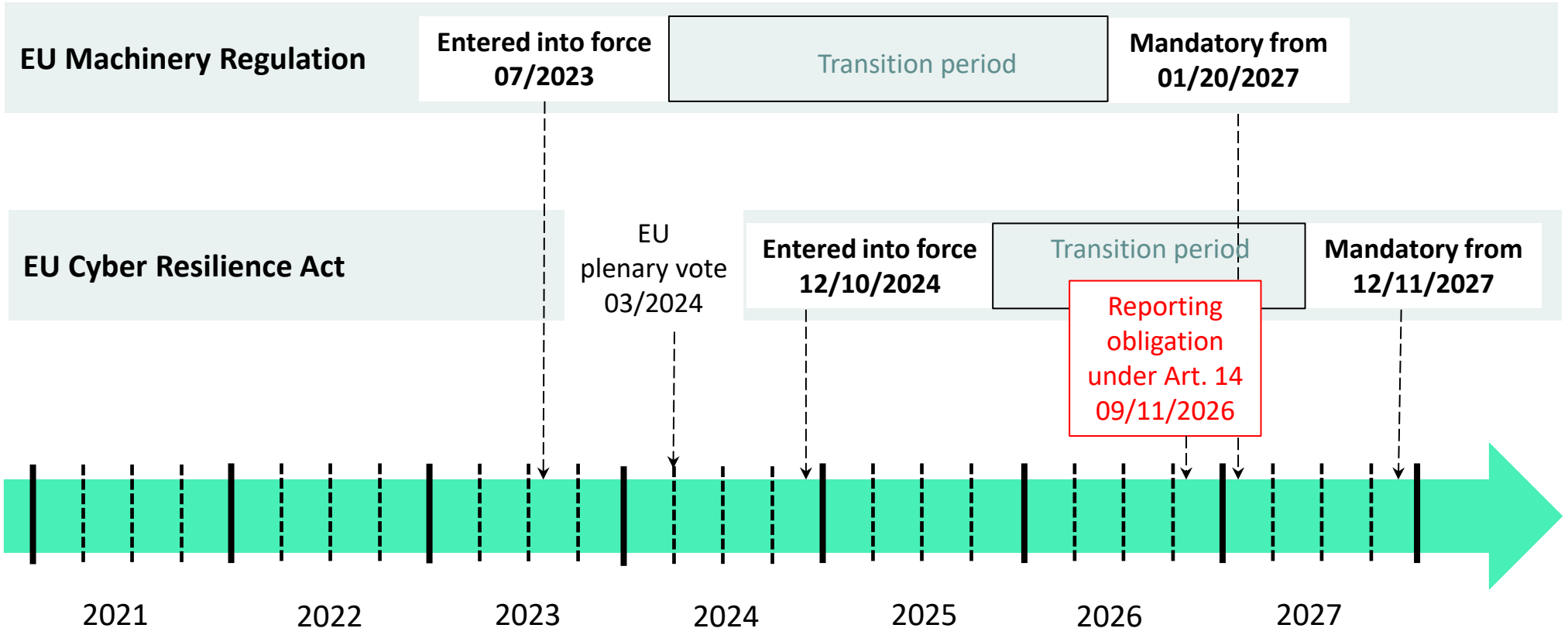
10 Risk and threat analysis for machines

Additional system-level measures for machine manufacturers and operators

- Effective protection depends on coordinated security measures at both the component and system levels
- Do not create global administrator accounts for the machine or system
- 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.

04 Timeline of relevant EU regulations

11 Timeline of relevant EU regulations



05 Cybersecurity at AMKmotion

12 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

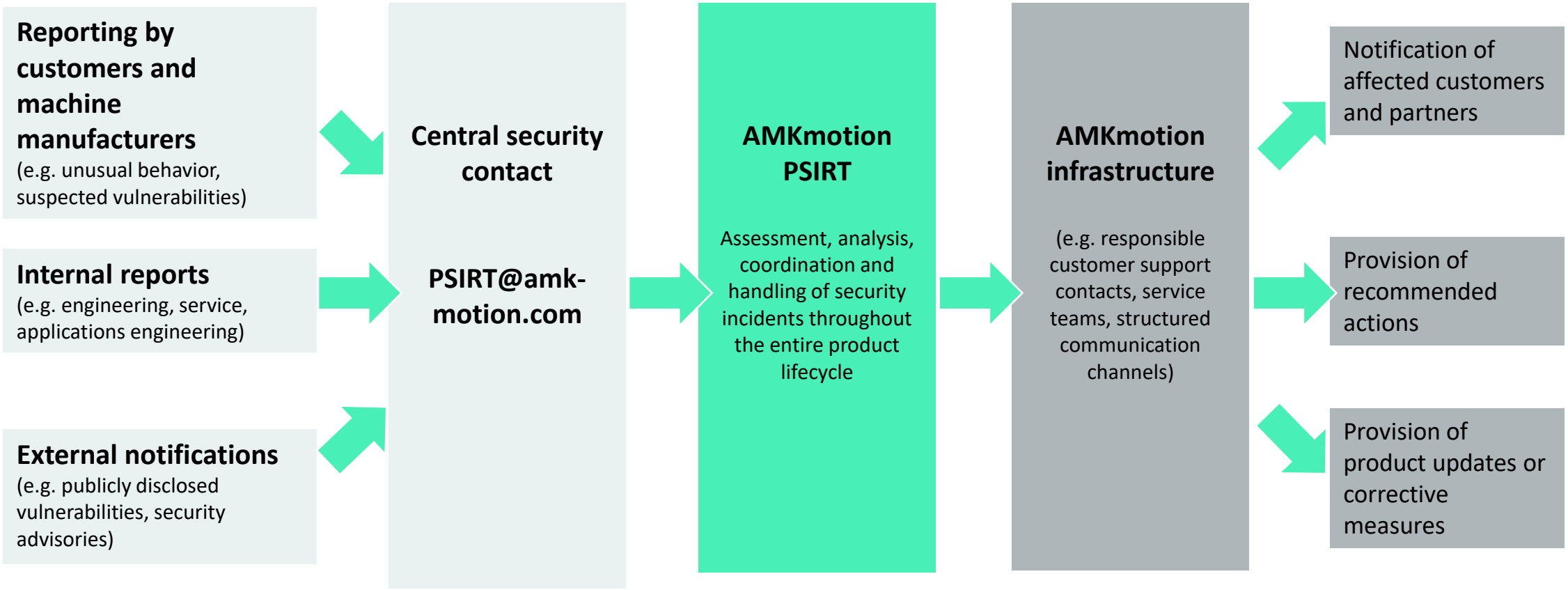
- Risk assessments for AMKmotion products
- Creation of Software Bills of Materials (SBOMs)
- Development of a customer-focused patch and update strategy
- Implementation of structured security testing
- Regular code reviews for security-critical functions

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).

13 Security incident reporting process



14 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