SERVICE & DISTRIBUTION GmbH
INDUSTRIAL AUTOMATION

WHITE PAPER: CYBER RESILIENCE ACT

WHAT MACHINE AND CONTROL CABINET MANUFACTURERS NEED TO KNOW

The increasing digitalization and interconnection of industrial systems not only offers numerous opportunities, but also significant risks. Cyber attacks on industrial control systems and networks can lead to production downtime, financial losses and loss of customer confidence, which is why the European Union has adopted the Cyber Resilience Act (CRA).

The CRA is a comprehensive set of regulations designed to improve the cyber security of products with digital components. The CRA is of great importance to machine builders and enclosure manufacturers, as it defines binding security requirements that companies must comply with in order to sell their products in the EU.

This white paper provides an overview of the CRA requirements, key dates and deadlines, as well as specific recommendations for implementation.

WHAT IS THE CYBER RESILIENCE ACT?

The Cyber Resilience Act has been developed to harmonise security requirements for products with digital elements and to create a more resilient digital infrastructure in the European Union.

THE KEY OBJECTIVES OF THE CRA:

- Improving the cyber security of products with digital components.
- Strengthening resilience to cyber attacks.
- Minimise vulnerabilities in networked systems.
- Increasing consumer confidence in digital products.

The CRA affects all companies that manufacture, sell or operate products with digital elements - from smart home appliances to complex industrial control systems.

IMPORTANT DATES AND DEADLINES

ADOPTION AND ENTRY INTO FORCE

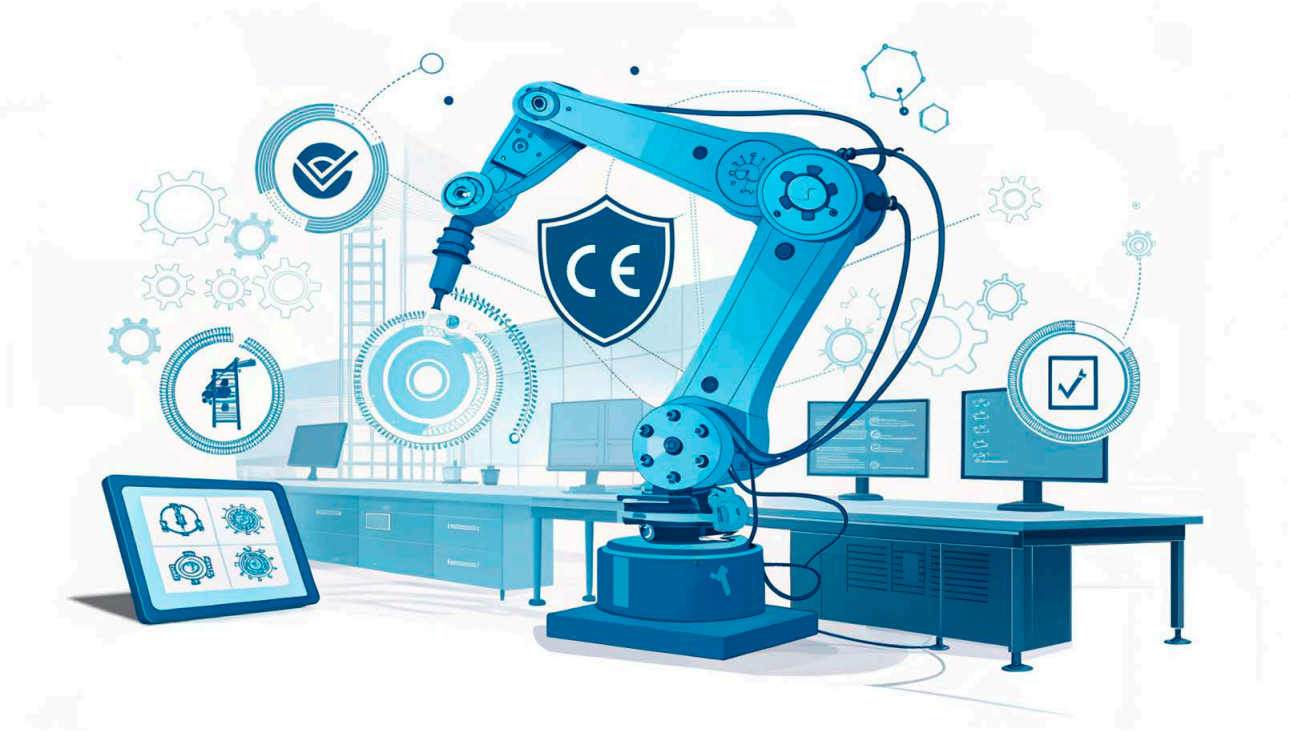
- The CRA was adopted in 2024 and officially came into force on 10 December 2024.

TRANSITIONAL PERIODS

- By June 11, 2026: Conformity Assessment Bodies must start working in accordance with the new requirements.
- By September 11, 2026: Vendors are required to report exploitable vulnerabilities.
- By December 11, 2027: The CRA will become fully applicable. From that date, only products that meet the new requirements will be allowed to be sold on the EU market.

These staggered deadlines give companies time to prepare for the new requirements and make any necessary adjustments.

THE CRA REQUIREMENTS



CYBERSECURITY FROM THE START

The CRA calls for cyber security measures to be built into the design of a product (‚security by design'). Manufacturers must identify and address potential vulnerabilities at an early stage.

CE MARKING

The CRA's security requirements will become part of the CE mark. Only products that meet the new cyber security requirements will be allowed to be sold on the EU market.

DOCUMENTATION AND EVIDENCE

Manufacturers must provide technical documentation to demonstrate that their product complies with the requirements of the CRA. This includes safety assessments, technical reports and documentation on safety updates.

REQUIREMENTS FOR EXISTING PRODUCTS

Products already on the market also need to be tested when safety updates are required or new risks emerge. This is especially true for machines and systems that have been in use for years.

IMPORTANCE OF THE CRA FOR MACHINE AND CONTROL CABINET MANUFACTURERS

SECURITY REQUIREMENTS IN PRODUCTION

Machine builders and enclosure manufacturers must ensure that their products are protected against cyber attacks. This includes:

- Protection of network communication.
- Safeguarding data integrity.
- Implementation of security protocols.

SECURITY ASSESSMENTS AND AUDITS

The CRA requires regular security analyses to identify and eliminate vulnerabilities. Companies should conduct internal audits and consider external audits to ensure compliance.

INTEGRATING SECURITY SOLUTIONS

To meet CRA requirements, technologies can be used to increase the protection of OT environments and machines.

EXTENDING RESPONSIBILITY

The CRA applies not only to new machinery and equipment, but also to products that have already been supplied. Manufacturers are required to regularly review and update safety measures.

HOLISTIC SECURITY PORTFOLIO FOR OT SECURITY

Our portfolio of services and solutions helps organisations make their OT environments, machines and products resilient and secure. We take a holistic approach, combining preventative and reactive measures:

OUR SERVICES:

Threat modelling:	Identify potential threats and vulnerabilities.
Proactive vulnerability analysis:	Product architecture review.
Network and asset analysis:	Detailed recording of the OT network. Creation or review of documentation (topology, concepts).
Risk analysis according to IEC 62443:	Vulnerability and threat assessment.
OT Firewall Review:	Effectiveness review and optimisation of firewall rules.
Switch configuration analysis:	Identification of configuration vulnerabilities.
Training:	Awareness training for networked production systems.

OUR SOLUTIONS:

Intrusion Detection System (IDS):	Passive monitoring of OT networks with alerting in the event of anomalies.
Management Security Dashboard:	Overview of production data and cyber security measures.
IoT Honeypot:	Notification of unauthorised access to simulated vulnerabilities.
Network Access Control (NAC):	Prevent unauthorised access to endpoints.
Industrial Firewall:	Control traffic and protect against unauthorised access.
Industrial Remote Access:	Secure remote maintenance via hardware or software solutions.

Our services and solutions provide the foundation for secure, transparent and future-proof OT networks and connected machines - tailored to your needs.

PRACTICAL EXAMPLES FROM INDUSTRY

EXAMPLE 1:

Network segmentation in a manufacturing environment

A manufacturer was struggling to protect critical production areas from cyber attacks. By implementing VLANs, using managed switches and setting up security zones according to IEC 62443, the risk was significantly reduced.

EXAMPEL 2:

Secure remote access for service engineers

Insecure remote access was a security risk. Using a VPN tunnel and multi-factor authentication, maintenance technicians were able to access machines securely. Tools such as Secomea GateManager made it easy and secure.

MORE INFORMATION

CONTACT DETAILS

UMER BHATTI

Business Development Manager OT-Security
(TÜV cert. Information Security Officer)

+49 151 27648814
bhatti@sud-gmbh.de

PATRICK POBERITZ

Head of Business Development & Marketing

+49 151 27648842
poberitz@sud-gmbh.de

https://sud-gmbh.de/en/industrial-cyber-security

SERVICE & DISTRIBUTION GmbH
INDUSTRIAL AUTOMATION

S&D Service & Distribution GmbH
Bischofstraße 113, 47809 Krefeld
Carl-Zeiss-Str. 8, 72124 Pliezhausen
Fuggerstraße 1b, 04158 Leipzig

+49 2151 4576-600
+49 2151 4576-777
info@sud-gmbh.de
www.sud-gmbh.de

Value-Add Distributor
A ROCKWELL AUTOMATION PARTNER