the power to control

bachmann.

The Cyber Resilience Act

Bachmann delivers the certified foundation.



energy.industry.maritime.

Cybersecurity requirements

Cyber Resilience Act (CRA)

With the Cyber Resilience Act, the European Union is establishing mandatory cybersecurity requirements for products containing digital elements. This also includes machines and automation solutions equipped with controllers, network interfaces, remote maintenance access, or cloud connections. Consequently, cybersecurity is shifting from a competitive advantage to a legal obligation.

When does the CRA take effect?

- September 11, 2026: Mandatory reporting of actively exploited vulnerabilities and serious security incidents
- December 11, 2027: Full implementation of the Cyber Resilience Act

Who is affected?

- Manufacturers of machines and equipment with digital components
- Manufacturers of software and automation solutions
- Integrators who develop their own products based on components

What does the CRA demand?

- Security by design and security by default
- Risk assessment during development
- Vulnerability management throughout the entire product lifecycle
- Security documentation for users
- Security updates during the defined support period
- Documentation and verification of implemented security measures
- Message about actively exploited vulnerabilities

When does the CRA apply to me?

- What matters is not when a product was developed, but when it is made available on the European market
- Even existing product lines that continue to be sold after December 11, 2027, must meet the requirements.

ENTER INTO FORCE
December 2024

REPORTING REQUIREMENTS
September 2026

FULL APPLICATION
December 2027

b.control

Automation

Scalable. Robust. Versatile.

SECURITY YOU CAN COUNT ON

We support you on your path to CRA compliance with certified products, security features and clear processes.

IEC 62443-4-1 CERTIFIED
Secure development processes since 2024

IEC 62443-4-2 CERTIFIED
M200 automation components

OVER 50 YEARS OF EXPERIENCE
In industrial automation

20 LOCATIONS WORLDWIDE
Support throughout the entire life cycle

Having a secure controller does not make your machine CRA-compliant

The use of a controller developed in accordance with IEC 62443 is an important component – but it does not constitute the entire proof of compliance. The responsibility for the end product's compliance remains with the machine manufacturer. That is precisely why we clearly outline what we provide and what remains your responsibility.

Here's what Bachmann offers

- Products developed in accordance with IEC 62443-4-1
- Components certified in accordance with IEC 62443-4-2
- Built-in security functions
- Security updates during the defined support period
- Documentation and evidence at the component level
- Information about relevant vulnerabilities

Here's what remains your responsibility

- Overall machine architecture
- Network design and segmentation
- Threat analysis for your machine
- Security documentation for the end user
- Remote maintenance concept
- User and permissions management
- Update management throughout the product lifecycle
- Technical documentation and CE compliance

You don't have to start from scratch

Those who rely on components that have already been developed in accordance with IEC 62443-4-1 and 4-2 can significantly reduce the effort required for implementation and compliance documentation.

Our offering: Getting you CRA-ready – step by step.

CRA Level	Definition	Delivery
1. Awareness	What exactly is the CRA and what does it imply for my business?	CRA webinar
2. Readiness	How prepared is my company for the CRA and where are the gaps?	1-2 day workshop
3. Implementation	How do I implement the required processes and provide evidence of CRA conformity?	1-2 day training session
4. Product Compliance	How do I develop and bring CRA-compliant products to market?	1-3 day workshop
5. Excellence	How can I demonstrate market leadership in cyber security?	Tailored to your project

What you can expect from us

The CRA affects the entire supply chain. As a component manufacturer, we lay the foundation on which you can build your own compliance.

Secure Products

Our controllers are developed in accordance with established security standards. Security is an integral part of product development, not an afterthought.

Security Features

Encrypted communication, role-based access rights, Secure Boot, secure updates, and end-to-end security logging – all integrated, not just tacked on.

Updates and Support

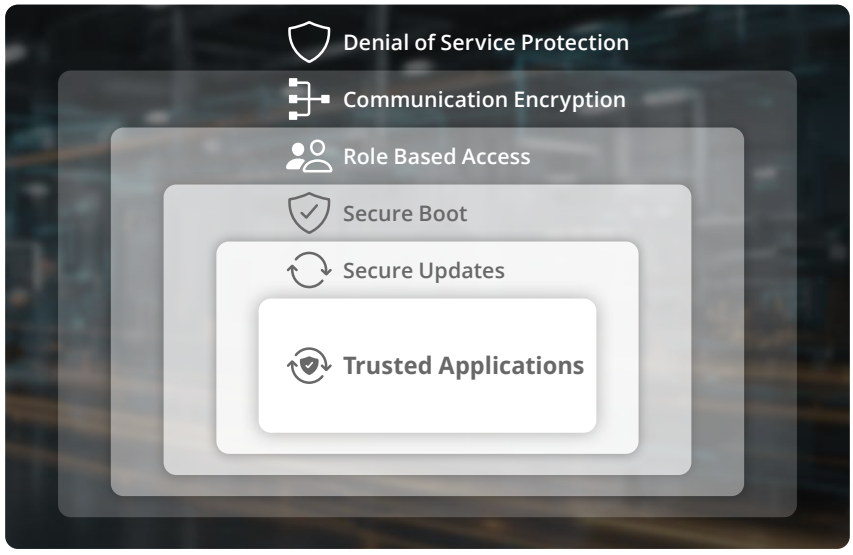
Security updates throughout the defined support period in full accordance with CRA requirements.

Documentation and Evidence

Certification records, security documentation, and information on vulnerabilities – as a basis for your own documentation.

Security at every layer – from communication to application

The CRA does not require a single security feature, but a holistic approach to protection. At Bachmann, protection is based on the principle of defense in depth: coordinated protection and hardening measures across different levels of the control system increase resilience and limit the impact of an attack.



SHOW MORE

The Cyber Resilience Act – get CRA ready with Bachmann

Whitepaper Cyber Resilience Act: The real challenges begin after product release



CONTACT

Christoph Scherrer

Product Line Management

T: +43 5522 3497-0
info@bachmann.info

bachmann.

www.bachmann.info

The Cyber Resilience Act EN | Subject to alterations without notice
© 11/2026 by Bachmann electronic

