BALLUFF

Cyber Resilience Act @Balluff – how we want to achieve CRA compliance

The European Union's Cyber Resilience Act (CRA) sets new, binding standards for the cybersecurity of products with digital elements. For us at Balluff, the CRA is of great importance because it not only strengthens the security of networked products but also ensures their conformity on the European market. Together, we are creating a more robust digital infrastructure.

We have carefully reviewed which of our products fall within the scope of the CRA. As of today, we consider that all our products that use BUS and IIoT protocols as well as IO-Link fall within the scope of the CRA. This affects a large proportion of our networked components that you use every day in your systems and machines.

Balluff is committed to proactively implementing and meeting these requirements throughout the product lifecycle, from development until phase-out. Our goal is to design all CRA-compliant products in accordance with the proven IEC 62443-4-1 family of standards. This approach ensures that our products not only meet CRA requirements but can also be optimally integrated into the security concepts of your plants and machine builders – for meaningful and practical application.

This is how we ensure implementation:

Dedicated project work:

We have established a dedicated cross functional project team that carefully analyzes the CRA requirements across global processes, methods, and products. and implement them in a timely manner.

Secure Development Processes

We are integrating a standardized Secure Product Development Lifecycle (SPDLC) into our existing product introduction process, ensuring that security considerations are anchored natively in product development.

Integration of Security Principles and Best Practices

We are integrating the principles and standards of the IEC62443-4-1 and IEC62443-4-2 into our processes and products, and closely aligning our development approach with these, to provide customers with safe and secure solutions.

We will seek certification according to IEC62443-4-1 standard for our processes and methods starting in 2026.

Coordinated vulnerability management:

To be able to react proactively to potential security gaps, we establish a central, dedicated Product Security Incident Response Team (PSIRT) and introduce a coordinated vulnerability management in cooperation with CERT@VDE. This will ensure coordinated intake, analysis, remediation and disclosure of any security-related vulnerabilities,

IT Security Certification

To support our internal processes, we are currently seeking certification of our IT security management processes in accordance with IEC 27001 which addresses the information security of our business processes and IT systems. This underscores our commitment to the highest safety standards in our internal processes and systems.

Your Feedback is Important!

We believe that strong product security is a core aspect of product strategy. We look forward to engaging in dialogue with you. If you have questions about CRA compliance or Balluff's product security approach or you have specific requirements that we can assist you with, please do not hesitate to contact your representative for further information or an exchange. We welcome your feedback and input!

i.A Heiko Mahr, Product Security Manager

i.V. Dr. Ingo Kleinschroth, CISO (acting)