

Secure innovation in automation

CYBER-SECURE MACHINES WITH BALLUFF COMPONENTS

Cybersecurity has become a fundamental requirement for reliable, sustainable machine operation – it is no longer an optional add-on. As industrial systems become increasingly connected, ensuring data protection, system integrity, and controlled interaction between components is essential. Future-proof machines go beyond functionality by embedding security by design from the start.

WHY CYBERSECURITY MATTERS FOR MACHINES

- Systems are interconnected across production, IT, and cloud layers
- Components must communicate reliably and predictably
- Machines must remain secure over long operational lifecycles

A security issue can disrupt operations, compromise safety and lead to costly downtime and reputational damage.

SECURE ARCHITECTURE

- Integrated system-level security replaces isolated product checks
- Continuous lifecycle security supersedes one-time validation
- Planned, controlled update strategies take the place of reactive updates

FUTURE-PROOF MACHINE DESIGN

- Secure firmware update mechanisms
- Controlled and predictable communication behavior
- End-to-end system integrity

CRA – FROM COMPLIANCE REQUIREMENTS TO ENGINEERING ADVANTAGES

The Cyber Resilience Act (CRA) makes cybersecurity a prerequisite for EU market access. Beyond compliance, it creates an opportunity for better structured systems, reduced integration risks, lower lifecycle costs, and higher reliability and trust. CRA demands a shift in approach to compliance, moving it from a one-time activity to a continuous system accountability.



DESIGNING CRA FROM THE START

Early design decisions define long-term success. By selecting the right components at the beginning, you can avoid costly redesigns, minimize integration complexity and ensure long-term compliance.

YOUR BALLUFF BENEFITS

- Reduced engineering complexity
- Faster and secure integration
- Lower lifecycle and maintenance costs
- Reliable compliance with CRA requirements
- A partner for secure, future-proof automation

WHAT TO FOCUS ON?

- Structured firmware update capabilities
- Controlled communication between components
- Defined system behavior and architecture

HOW BALLUFF SUPPORTS YOUR SYSTEMS

Balluff provides the technical foundation, processes, and expertise to integrate cybersecurity into your systems.



LIFECYCLE CAPABILITY BUILT INTO THE PRODUCT

Balluff products are designed for long-term secure operation.

- **Easily accessible updates** from the Balluff Update Platform
- **Reduced service effort:** System-level update management
- **Architectural stability** defined behavior already in design phase



COORDINATED VULNERABILITY HANDLING

Security challenges don't end at product release. Balluff ensures structured and reliable vulnerability handling.

- **Dedicated PSIRT** (Product Security Incident Response Team)
- **Cooperation with recognized institutions** (e.g., CERT@VDE)
- **Defined escalation** and communication processes



TRANSPARENCY AND PRACTICAL GUIDANCE

We translate regulatory requirements into usable engineering information.

- **Clear integration context:** Defined intended use and system limits
- **Practical documentation:** Regulatory requirements mapped to real applications



SECURE DEVELOPMENT YOU CAN RELY ON

Cybersecurity is embedded in our processes and integrated into product development from the outset.

- Secure Product Development Lifecycle (SPDLC) aligned with **IEC 62443-4-1**
- Information security based on **IEC 27001**

www.balluff.com