

Sichere Innovationen in der Automatisierung

CYBERSECURITY IN MASCHINEN MIT BALLUFF KOMPONENTEN

Cybersecurity wird zu einem Standard für einen zuverlässigen und nachhaltigen Maschinenbetrieb und ist längst kein optionales Zusatzfeature mehr. Da industrielle Systeme zunehmend vernetzt sind, ist die Gewährleistung von Datenschutz, Systemintegrität und einer kontrollierten Interaktion zwischen den Komponenten von entscheidender Bedeutung. Zukunftssichere Maschinen gehen über die reine Funktionalität hinaus, indem sie Sicherheit von Anfang an in ihre Konzeption integrieren.

WARUM CYBERSECURITY FÜR MASCHINEN WICHTIG IST

- Systeme sind über Produktions-, IT- und Cloud-Ebenen hinweg miteinander vernetzt
- Komponenten müssen zuverlässig und vorhersehbar kommunizieren
- Maschinen müssen über lange Betriebszyklen hinweg sicher bleiben

Ein Sicherheitsproblem kann den Betrieb stören, die Sicherheit gefährden und zu kostspieligen Ausfallzeiten sowie zu Reputationsschäden führen.

SICHERE ARCHITEKTUR

- Integrierte Sicherheit auf Systemebene ersetzt isolierte Produktprüfungen
- Kontinuierliche Sicherheit über den gesamten Lebenszyklus anstatt einmaliger Validierung
- Geplante und fortlaufende Update-Strategien ersetzen reaktive Updates

ZUKUNFTSSICHERES MASCHINENKONZEPT

- Sichere Mechanismen zur Firmware-Aktualisierung
- Kontrolliertes und vorhersehbares Kommunikationsverhalten
- Durchgängige Systemintegrität

CRA – VON COMPLIANCE-ANFORDERUNGEN ZU TECHNISCHEN VORTEILEN

Der Cyber Resilience Act (CRA) macht Cybersecurity zur Voraussetzung für den Marktzugang in der EU. Über die reine Einhaltung von Vorgaben hinaus bietet er Chancen für besser strukturierte Systeme, geringere Integrationsrisiken, niedrigere Lebenszykluskosten sowie höhere Zuverlässigkeit und mehr Vertrauen. Der CRA erfordert ein Umdenken: die Einhaltung von Vorschriften entwickelt sich von einer einmaligen Aufgabe hin zu einer kontinuierlichen Systemverantwortung.



CRA VON ANFANG AN MITDENKEN

Frühe Designentscheidungen sind entscheidend für den langfristigen Erfolg. Durch die Auswahl der richtigen Komponenten zu Beginn lassen sich kostspielige Neuentwicklungen vermeiden, die Integrationskomplexität minimieren und die langfristige Konformität sicherstellen.

IHR BALLUFF VORTEIL

- Geringere technische Komplexität
- Schnellere und sichere Integration
- Geringere Lebenszyklus- und Wartungskosten
- Zuverlässige Einhaltung der CRA-Anforderungen
- Ein Partner für sichere, zukunftssichere Automatisierung

WORAUF SIE ACHTEN SOLLTEN

- Strukturierte Firmware-Update-Fähigkeit
- Kontrollierte Kommunikation zwischen den Komponenten
- Definiertes Systemverhalten und klare Systemarchitektur

SO UNTERSTÜTZT BALLUFF IHRE SYSTEME

Balluff bietet die technische Grundlage, die Prozesse und die Expertise, um Cybersecurity in Ihre Systeme zu integrieren.



IN DAS PRODUKT INTEGRIERTE LEBENSZYKLUSFÄHIGKEIT

Die Produkte von Balluff sind für einen langfristigen, zuverlässigen Betrieb ausgelegt.

- **Einfach abrufbare Updates** über die Balluff Update-Plattform
- **Geringerer Serviceaufwand:** Update-Management auf Systemebene
- Durch die **architektonische Stabilität** wird das Verhalten bereits in der Entwurfsphase festgelegt



KOORDINierter UMGANG MIT SICHERHEITSLÜCKEN

Sicherheitsherausforderungen enden nicht mit der Produkteinführung. Balluff gewährleistet einen strukturierten und zuverlässigen Umgang mit Sicherheitslücken.

- **Spezielles PSIRT** (Product Security Incident Response Team)
- **Zusammenarbeit** mit anerkannten Institutionen (CERT@VDE)
- **Festgelegte** Eskalations- und Kommunikationsprozesse



TRANSPARENZ UND PRAKTISCHE LEITLINIEN

Wir setzen gesetzliche Anforderungen in verwertbare technische Informationen um.

- **Klarer Integrationskontext:** Definierter Einsatzzweck und Systemgrenzen
- **Praktische Dokumentation:** Anwendbare Informationen abgestimmt auf reale Anwendungsfälle



SICHERE ENTWICKLUNG, AUF DIE SIE SICH VERLASSEN KÖNNEN

Cybersecurity ist fest in unseren Prozessen verankert und wird von Anfang an in die Produktentwicklung integriert.

- Sicherer Produktentwicklungszyklus (SPDLC) im Einklang mit **IEC 62443-4-1**
- Informationssicherheit auf der Grundlage von **IEC 27001**

www.balluff.com