Fachartikel

Cyber Resilience Act: Neue Anforderungen an alle Gerätehersteller in der Fabrik- und Prozessautomatisierung

April 2025

Mit dem Cyber Resilience Act (CRA) hat die Europäische Union einen wegweisenden Schritt zur Verbesserung der Cybersicherheit im digitalen Binnenmarkt beschlossen. Im Gegensatz zu bestehenden Normen, die häufig den Schutz der Herstellerinteressen fokussieren, setzt der CRA den Schutz der Anwender in den Mittelpunkt. Er verpflichtet Hersteller, Sicherheitsmaßnahmen zu implementieren und Updates bereitzustellen, um potenzielle Risiken für Nutzer zu minimieren.

Ab Ende 2027 dürfen digitale Komponenten nur noch dann in Verkehr gebracht werden, wenn sie die grundlegenden **Sicherheitsanforderungen des CRA** erfüllen. Neben der Erhöhung der Widerstandsfähigkeit digitaler Systeme gegenüber Cyberbedrohungen soll die Verordnung auch dazu beitragen, bestehende Sicherheitslücken in den Geräten zu erkennen und zu schließen.

Diese Regelung betrifft daher auch Geräte der Fabrik- und Prozessautomation, darunter Sensoren, Aktoren, Steuerungen und Kommunikationstechnologien – insbesondere solche mit digitalen Schnittstellen. Ab Ende 2027 dürfen Komponenten mit **Embedded Software** nur noch dann auf den Markt gebracht werden, wenn sie die spezifischen Vorgaben des CRA erfüllen.

Die MESCO-Experten beraten Sie technologie- und herstellerneutral und unterstützen Sie dabei, Ihre Entwicklungsprojekte effizient und konform mit den neuen regulatorischen Vorgaben umzusetzen.

Cyber Resilience Act fordert erhöhte Sicherheitsstandards für Digitale Geräte

Unternehmen der Fabrik- und Prozessautomatisierungsbranche stehen vor der Herausforderung, ihre Produkte an die neuen gesetzlichen Anforderungen des Cyber Resilience Act anzupassen. Die Einhaltung dieser Vorschriften ist zwingend erforderlich, um weiterhin eine **CE-Kennzeichnung** auf ihren Produkten anbringen und diese in der EU vertreiben zu können. Allerdings behalten Produkte, die vor 2027 in Verkehr gebracht werden, ihre CE-Kennzeichnung auch über diesen Stichtag hinaus, wenn sie nicht wesentlich verändert wurden. Ein Software-Update oder ein Austausch einer Software-Komponente könnte aber bereits eine wesentliche Veränderung darstellen und erfordern, dass alle Anforderungen des CRA einzuhalten sind.

Sicherheitsmaßnahmen sind nicht nur auf das Feldgerät beschränkt, sondern müssen insbesondere auch die Schnittstellen, wie zum Beispiel **Feldbusse**, betrachten. Da andere **Feldgeräte** als Einfallstor in einen Feldbus genutzt werden könnten, haben sich die Feldbusorganisationen schon eingehend mit dem Thema **Security in Echtzeitnetzwerken**, insbesondere solche auf Ethernet-Basis oder Funknetzwerke befasst.

Industrielle Feldbusse und der Cyber Resilience Act

Die **Feldbus-Organisationen haben bereits erste Sicherheitskonzepte entwickelt**: So gibt es beispielsweise Maßnahmen, die darauf abzielen, den Zugriff auf ein System oder eine Infrastruktur vor unbefugter Manipulation zu schützen.

Die **PROFIBUS Nutzerorganisation PI** stellt zum Beispiel mit der **Sicherheitsklasse 1 bei PROFINET** sicher, dass Geräte korrekt von der Steuerung angesprochen werden.

Dies wird unter anderem durch die Deaktivierung der einfachen Geräteadressmanipulation sowie die Signierung der GSDML-Dateien erreicht. Allerdings trägt diese Maßnahme nur bedingt dazu bei, externe Bedrohungen abzuwehren. Wird insbesondere ein Gerät zum Beispiel über eine **IOT-Schnittstelle** durch einen Angreifer übernommen, so sind diese Maßnahmen weitgehend wirkungslos.

Soll die **Sicherheit bei PROFINET** weiter erhöht werden, sind folgende, zusätzliche Maßnahmen erforderlich:

- Integrität und Authentizität der Daten (Sicherheitsklasse 2): Diese Maßnahmen verhindern Manipulationen an Daten während der Übertragung und stellen sicher, dass Informationen nicht verfälscht oder unbemerkt verändert werden. Dies kann durch kryptografische Signaturen oder Prüfmechanismen erreicht werden.
- Vertraulichkeit der Daten (Sicherheitsklasse 3): Hierbei geht es um den Schutz sensibler Informationen vor unbefugtem Zugriff. Verschlüsselungstechnologien sorgen dafür, dass nur autorisierte Parteien Zugriff auf Prozessdaten haben. Dies dient insbesondere dem Know-how-Schutz in der Applikation.

Die Umsetzung dieser Sicherheitsanforderungen erfordert die Implementierung geeigneter Schutzmechanismen sowie umfassende Tests zur Validierung.

CRA-Anforderungen: MESCO-Experten unterstützen Sie bei der Umsetzung

Unsere Hardware- und Software-Experten begleiten Sie technologie- und herstellerneutral bei der Umsetzung der Anforderungen des Cyber Resilience Act – von der ersten Analyse, über Software- und Hardware-Anpassungen bis hin zur Unterstützung der Konformitäts-Erklärung für Ihre Produkte.

Unsere Leistungen umfassen:

- **Auswahl des geeigneten Konformitätsbewertungsverfahrens**: Im Regelfall erfolgt die Bewertung im Rahmen einer Selbsterklärung für nicht kritische Produkte
- **Durchführung von Risikobewertungen und Minimierung der Angriffsflächen** zur Reduzierung potenzieller Sicherheitsrisiken

- **Integration von Schutzmechanismen** einschließlich Maßnahmen für Datenintegrität, Vertraulichkeit und weitere relevante Sicherheitsaspekte
- **Beratung und Entwicklung von (cyber-)sicherer Feldbus-Kommunikation:** PROFINET, EtherCAT, IO-Link als auch von funktional-sicheren Protokollen wie PROFIsafe, FSoE, IO-Link Safety
- **Erstellung einer Software Bill of Materials (SBOM)** gemäß den technischen Richtlinien, um eine transparente Nachverfolgbarkeit von Software-Komponenten zu gewährleisten
- **Unterstützung bei der Identifikation und Behandlung von Schwachstellen**, basierend auf bewährten Sicherheitsstandards
- **Ausführliche Dokumentation nach den Vorgaben des CRA**, um die Einhaltung der regulatorischen Anforderungen sicherzustellen und die Konformitätserklärung zu unterstützen.

Ihr Entwicklungspartner. Seit 35 Jahren.

...und aus Ideen werden Erfolge!

MESCO Engineering ist Ihr Partner für innovative Elektronikentwicklung für Produkte im Bereich der Prozess- und Fabrikautomation. Unsere Kernkompetenz liegt in der Entwicklung von Hardware und Software.

Die Kombination der technischen Bereiche der industriellen Kommunikation, der Funktionalen Sicherheit und des Explosionsschutzes ist unsere Stärke. Seit 1990 bieten wir unseren Kunden weltweit aktuelles branchenübergreifendes Know-how, integrierte Lösungen und umfassenden Service. Hier steht eine ehrliche, transparente und partnerschaftliche Zusammenarbeit an erster Stelle.

Pressekontakt

Peter Bernhardt
Head of Sales & Marketing

Tel.: +49 7621 1575 441
peter.bernhardt@mesco-engineering.com

MESCO Engineering GmbH
Berner Weg 7
79539 Lörrach
Germany

Tel. +49 7621 1575 0
info@mesco-engineering.com