Cobot Safety

Der Cyber Resilience Act (CRA)

Auswirkungen auf den Bereich Automation und Maschinenbau

Eine umfassende Analyse der neuen EU-Verordnung und ihrer Bedeutung für die industrielle Wertschöpfungskette

M.Sc. Andreas Schunkert

15. November 1974 in Neuwied (Rhein)

Cobot Safety

Nicht verheiratet, einen Sohn (13)
Fußball und Tauchen

- Lehre als Energieelektroniker
- Meister Elektrotechnik
- Bachelor und Masterstudium allgemeine Elektrotechnik
  an der Hochschule Koblenz

Cobot Safety
Automatisieren – Aber sicher

aalberts

UNITED ROBOTICS GROUP
the CobiotX company

masa
Milestone to your success.

UNIVERSAL ROBOTS

- 6,5 Jahre Technische Leitung WE bei Universal Robots
- 1,5 Jahre Director Service bei United Robotics Group
- Gründer und Inhaber der Firma Cobot Safety
- Mitglied im Arbeitskreis DIN NA 060-38-01-01 AK „Sicherheit Industrierobotik“
- Mitglied im internationalen Normungsgremium ISO TC 299 WG3 (Safety in industrial robotics)
- Mitglied im internationalen Normungsgremium ISO TC 299 WG2 (Safety in service robotics)
- Mitglied im internationalen Normungsgremium ISO TC 299 WG8 (Collaboratrive Robotics)
- Autor des Buchs „Kollaborative Roboterapplikationen – von der Idee bis zur Integration“ erschienen beim HANSER-Verlag

Agenda

Grundlagen des Cyber Resilience Acts

Rechtlicher Rahmen, Produktkategorien und Zeitplan

Auswirkungen auf Betreiber

Pflichten, Herausforderungen und strategische Überlegungen

Auswirkungen auf Maschinenbauer

Neue Anforderungen, Integration von Safety & Security

Auswirkungen auf Komponentenhersteller

Technische Anforderungen, Produktentwicklung, Bedienbarkeit

Fazit und Handlungsempfehlungen

Strategische Vorbereitung auf den CRA

Cobot Safety

Der Cyber Resilience Act: Paradigmenwechsel in der EU

Mit dem Cyber Resilience Act (CRA) etabliert die Europäische Union erstmals **verbindliche Cybersicherheitsanforderungen** für Produkte mit digitalen Elementen über deren gesamten Lebenszyklus hinweg.

Besonders betroffen sind Branchen mit hohem Automatisierungsgrad und digitalisierten Infrastrukturen wie der Maschinenbau und die Prozessindustrie.

Der CRA schafft ein **einheitliches Cybersicherheitsniveau** im EU-Binnenmarkt und regelt:

- Hardware und Software mit digitaler Funktionalität
- Produkte, die Daten verarbeiten oder sich mit anderen Systemen vernetzen

Cobot Safety

Produktkategorisierung nach dem CRA

Standard-Kategorie

Beispiele: Konsumgüter mit digitalen Elementen, Standard-Industrie-Hardware

Wichtige Produkte – Klasse 1

Beispiele: Betriebssysteme, Switche, Netzschnittstellen, Mikrocontroller, Mikroprozessoren

Wichtige Produkte – Klasse 2

Beispiele: Firewalls, Angriffserkennungssysteme, Mikrocontroller, Mikroprozessoren mit erhöhten Sicherheitsanforderungen

Kritische Produkte mit digitalen Elementen

Beispiele: Hardwaregeräte mit Sicherheitsboxen, kritische Abhängigkeiten, Essential Entities (NIS2), Komponenten mit potentiellen Störungen kritischer Lieferketten

Je höher die Kategorie, desto umfangreicher die Sicherheitsanforderungen und Nachweispflichten.

Zeitplan zur Umsetzung des CRA

Cobot Safety

Dezember 2024

Inkrafttreten des Cyber Resilience Acts

Beginn der Vorbereitungsphase für Unternehmen

1

2

September 2026

Meldepflicht für Schwachstellen tritt in Kraft

Aktiv ausgenutzte Sicherheitslücken müssen gemeldet werden

3

Dezember 2027

Alle CRA-Anforderungen müssen vollständig erfüllt sein

Nur noch CRA-konforme Produkte dürfen neu in Verkehr gebracht werden

Die IEC 62443-Reihe bildet die technische Normengrundlage für die Konformitätsbewertung (Produktentwicklungsprozess, Security Requirements, Schwachstellenmanagement).

Cobot Safety

Fünf Säulen des CRA für Industrieprodukte

Security by Design

Sicherheit als integraler Bestandteil der Produktentwicklung

Konformitätsnachweise

Dokumentation und Bewertung der Cybersicherheit

Schwachstellenmanagement

Meldung und Behebung von Sicherheitslücken

Lifecycle-Support

Mindestens 5 Jahre Sicherheitsupdates

Transparenz

Offene Kommunikation zu Sicherheitsmaßnahmen

Auswirkungen auf Betreiber

Neue Pflichten und Herausforderungen

Betreiber industrieller Anlagen (z.B. chemische Industrie, Versorger) müssen:

- Ab Dezember 2027 ausschließlich CRA-konforme Produkte für Neuinstallationen einsetzen
- Aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle an Behörden und betroffene Nutzer melden
- Umfangreiche Dokumentation über eingesetzte Produkte führen (technische Dokumentation, Zweckbestimmung, Risikobewertung, Normenbezug)
- Sicherstellen, dass CRA-konforme Produkte mindestens 5 Jahre unterstützt werden

Cobot Safety

Migration und Ersatzteile für Betreiber

Altanlagen

Alt-Komponenten dürfen weiter betrieben, aber nicht mehr neu in Verkehr gebracht werden

Bestandsschutz für bereits installierte Systeme

Regulatorische Entlastung

CRA verschiebt Verantwortung teilweise zu Lieferanten

Dennoch: Betreiber müssen CRA-Konformität nachweisen können

Ersatzteile

Müssen identisch spezifiziert sein, sonst CRA-konform

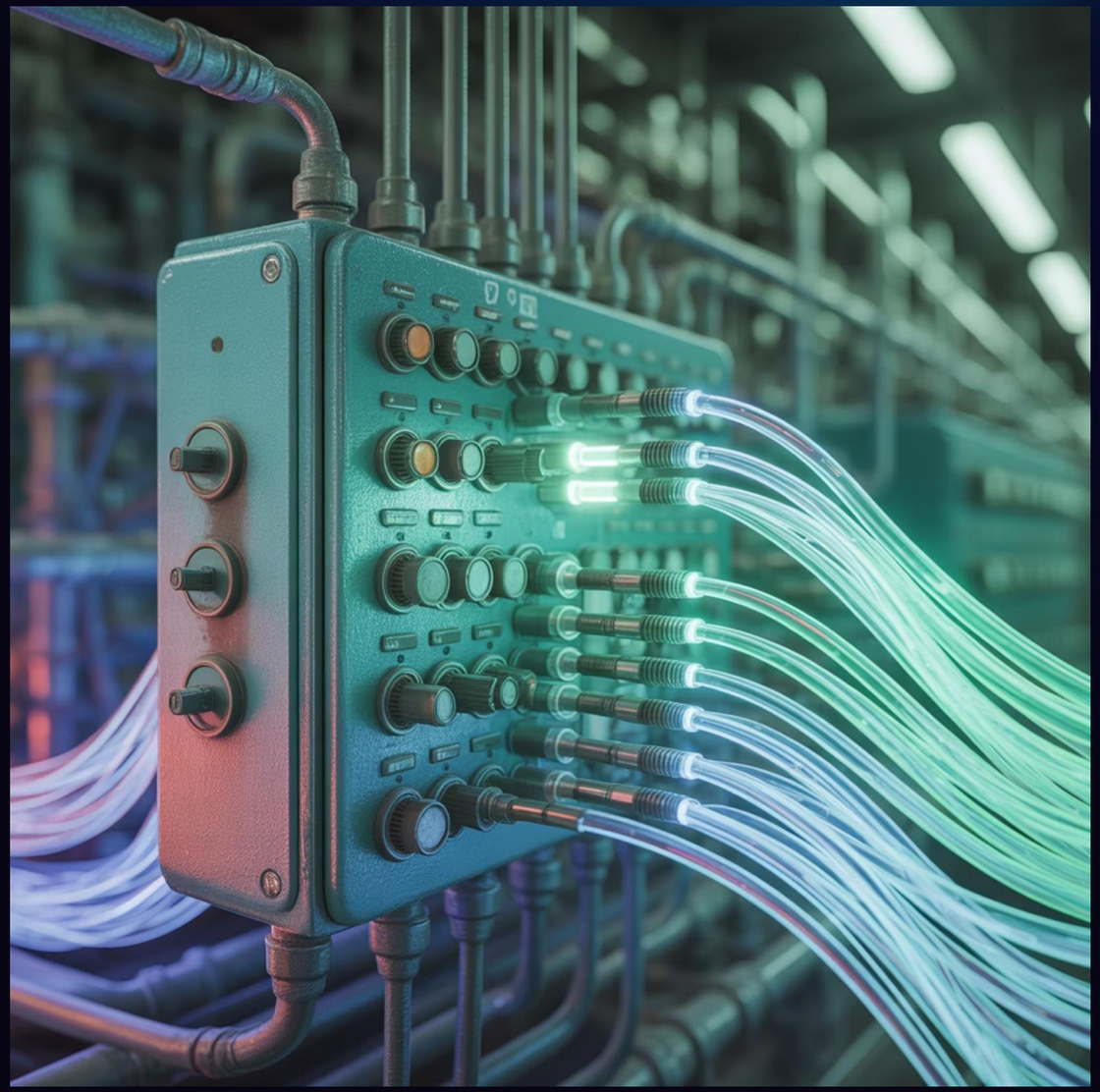
Verfügbarkeit von Ersatzteilen könnte zum kritischen Faktor werden

Strategische Entscheidung

Migration vor oder nach 2028?

Frühzeitige Planung der Anlagenmodernisierung empfohlen

Herausforderungen für Betreiber: Bestandsanlagen



Strategische Dilemmata

- Weiterbetrieb von Altanlagen wird komplexer (Ersatzteilversorgung)
- Modernisierung erfordert CRA-konforme Komponenten
- Mischbetrieb zwischen alten und neuen Systemen schafft Sicherheitsherausforderungen

Empfehlungen

- Bestandsaufnahme kritischer Systeme und deren Lifecycle-Status
- Modernisierungsplan mit CRA-Zeitplan abstimmen
- Investitionen in Sicherheitszonen und Netzwerksegmentierung

Cobot Safety

Auswirkungen auf Maschinenbauer

Neue Anforderungen durch CRA und Maschinenverordnung (MVO)

CRA-Konformität

Maschinen mit digitalen Komponenten müssen CRA-Anforderungen erfüllen

Sichere Software

Software wird integraler Teil der sicherheitsrelevanten Maschinenkomponenten

Digitale Dokumentation

Konformitätserklärungen und Dokumentation dürfen digital erfolgen

Schutz gegen Korrumpierung

MVO definiert Schutz gegen Manipulationen als verbindliches Ziel

Maschinenbauer müssen ihre Entwicklungsprozesse anpassen und Cybersecurity als integralen Bestandteil der Produktentwicklung etablieren.

Integration von Safety & Security im Maschinenbau

Herausforderungen

- Konflikt zwischen Sicherheitsanforderungen (Safety) und Cybersecurity
- Unterschiedliche Fachdisziplinen und Normenlandschaften
- Erhöhte Komplexität bei Risikoanalysen

Lösungsansätze

- Integrierte Risikoanalysen für Safety und Security
- Zonensegmentierung nach IEC 62443
- Maßgeschneiderte Sicherheitskonzepte für spezifische Anwendungsfälle
- Sichere Fernwartungslösungen mit Mehrfaktor-Authentifizierung

Cobot Safety

Lieferkettenverantwortung nach NIS2 und CRA

Betreiber

Verpflichten Maschinenbauer vertraglich zur CRA-Konformität

Müssen Cybersecurity-Risiken in der Lieferkette managen

Regulatorische Aufsicht

Überprüft Einhaltung der Anforderungen

Sanktioniert Verstöße in der gesamten Kette

Maschinenbauer

Verantworten Konformität der Gesamtmaschine

Benötigen konforme Komponenten von Zulieferern

Komponentenhersteller

Müssen CRA-konforme Produkte liefern

Stehen am Anfang der Sicherheitskette

Der CRA schafft eine durchgängige Verantwortungskette für Cybersecurity über alle Wertschöpfungsstufen hinweg.

Auswirkungen auf Komponentenhersteller

Cobot Safety

Technische Anforderungen

Komponentenhersteller (z.B. Anbieter von Steuerungen, Netzwerktechnik, Software) stehen vor besonders umfangreichen Anforderungen:

- **Security by Design:** Cybersecurity muss von Beginn der Entwicklung an integriert werden
- **Security by Default:** Keine Standardpasswörter, sichere Voreinstellungen ab Werk
- **Schwachstellenmanagement:** Systematische Prozesse zur Erkennung und Behebung von Sicherheitslücken
- **Meldepflichten:** Aktiv ausgenutzte Schwachstellen müssen innerhalb von 24 Stunden gemeldet werden
- **Entwicklung nach IEC 62443:** Insbesondere Teil 4-1 (Produktentwicklungsprozess) und 4-2 (technische Anforderungen)

Cobot Safety

Produktentwicklung nach CRA-Anforderungen

15-30%

Erhöhter Entwicklungsaufwand

Zusätzliche Sicherheitsanforderungen und Tests verlängern die Entwicklungszyklen und erhöhen die Kosten

100%

Konformitätsbewertung

Größere Änderungen an bestehenden Produkten erfordern eine neue vollständige Konformitätsbewertung

5+ Jahre

Lifecycle-Unterstützung

Hersteller müssen Sicherheitsupdates für mindestens 5 Jahre nach Markteinführung bereitstellen

Die erhöhten Anforderungen werden voraussichtlich zu einer Marktkonsolidierung führen, da kleinere Hersteller Schwierigkeiten haben könnten, die komplexen Anforderungen zu erfüllen.

Cobot Safety

Bedienbarkeit und Nutzerfreundlichkeit

Herausforderungen

Sicherheitsanforderungen und Bedienbarkeit müssen in Balance gehalten werden:

- Umsetzung sicherer Identitäts- und Zugriffskonzepte (z.B. Zwei-Faktor-Authentifizierung)
- Nutzerfreundliches Passwort-Management in industriellen Umgebungen
- Verschlüsselte Kommunikation ohne Beeinträchtigung der Echtzeitfähigkeit
- Sichere Fernwartung unter Berücksichtigung betrieblicher Anforderungen

Empfehlung: Orientierung an Standards wie NAMUR NE201 für benutzerfreundliche Security-Implementierungen

Cobot Safety

Konformitätsbewertung nach dem CRA

Selbstbewertung

Für Standardprodukte ausreichend

Eigenverantwortliche Prüfung und Dokumentation

Umfangreiche Konformitätsbewertung

Für wichtige Produkte der Klasse 1

Umfassendere Dokumentation und Nachweise

Prüfung durch Dritte

Für wichtige Produkte der Klasse 2

Externe Zertifizierung erforderlich

Strenge Zertifizierung

Für kritische Produkte

Umfassende externe Prüfungen und Dokumentation

Der Umfang der Konformitätsbewertung richtet sich nach der Produktkategorie und den damit verbundenen Risiken.

Fallbeispiel: Steuerungssystem nach CRA CRA

Vor CRA

Standardpasswörter, unverschlüsselte Kommunikation, keine systematische Schwachstellenbehebung

Nach CRA

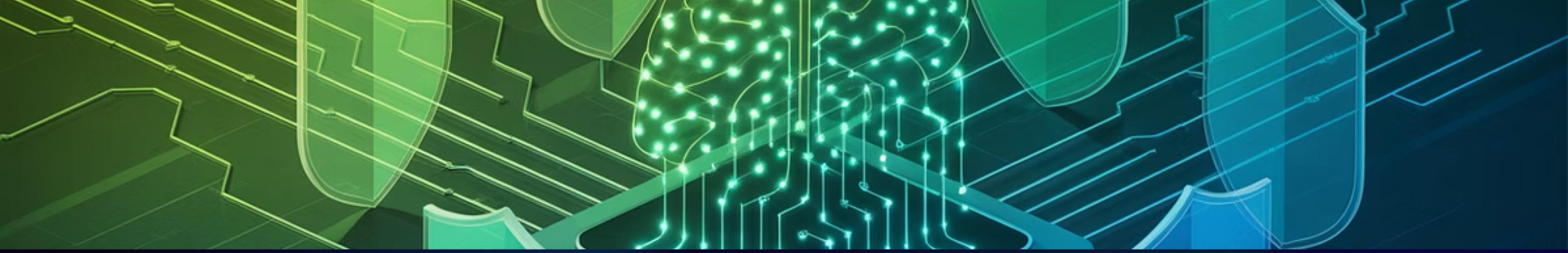
Sichere Standardkonfiguration, Mehrfaktor-Authentifizierung, verschlüsselte Kommunikation, regelmäßige Sicherheitsupdates

Dokumentation

Umfassende Risikoanalyse, Konformitätsnachweise, Nutzerhinweise zur sicheren Verwendung

Lifecycle-Management

Garantierte Sicherheitsupdates für 5 Jahre, definierter Prozess für Schwachstellenmeldungen



Chancen durch den CRA

Für Betreiber

- Verbesserte Sicherheit der eingesetzten Produkte
- Transparentere Risikobeurteilung
- Teilweise Entlastung von Sicherheitsverantwortung
- Mehr Rechtssicherheit beim Einsatz von Produkten

Für Maschinenbauer

- Differenzierungsmöglichkeit durch starke Sicherheitskonzepte
- Harmonisierte Anforderungen im EU-Binnenmarkt
- Klarere Verantwortungsabgrenzung

Für Komponentenhersteller

- Wettbewerbsvorteil für frühe Adopter
- Klare Orientierung durch Normenlandschaft
- Möglichkeit zur Produktdifferenzierung
- Höhere Margen für sichere Produkte

Für die Industrie insgesamt

- Stärkere Resilienz gegen Cyberangriffe
- Reduzierung der Ausfallrisiken
- Verringerung von Haftungsrisiken
- Vertrauensbildung bei Kunden und Behörden

Handlungsempfehlungen für die Vorbereitung auf den CRA

Cobot Safety

Bestandsaufnahme

Identifizieren Sie betroffene Produkte und Komponenten in Ihrem Portfolio oder Ihrer Anlage

Klassifizieren Sie diese nach den CRA-Kategorien

Gap-Analyse

Bewerten Sie den aktuellen Sicherheitsstand im Vergleich zu den CRA-Anforderungen

Identifizieren Sie Schwachstellen und Handlungsbedarf

Maßnahmenplanung

Erstellen Sie einen priorisierten Umsetzungsplan unter Berücksichtigung des CRA-Zeitplans

Planen Sie Budget und Ressourcen für die Umsetzung ein

Qualifikation

Schulen Sie Mitarbeiter zu den neuen Anforderungen und notwendigen Prozessen

Bauen Sie interdisziplinäre Teams aus OT- und IT-Sicherheitsexperten auf

Zusammenarbeit

Intensivieren Sie den Dialog mit Kunden und Lieferanten entlang der Wertschöpfungskette

Klären Sie Verantwortlichkeiten und Schnittstellen frühzeitig

Strategische Planung

Integrieren Sie CRA-Anforderungen in Ihre Produktentwicklungs- und Investitionsstrategien

Nutzen Sie die Chance zur Differenzierung im Markt

Cobot Safety

Fazit: Der CRA als Paradigmenwechsel

Der Cyber Resilience Act stellt die gesamte Wertschöpfungskette im Bereich Automation und Maschinenbau vor tiefgreifende Herausforderungen.

Gleichzeitig bietet er die Chance, Cybersecurity endlich strukturiert und regulatorisch fundiert in die industrielle Entwicklung und den Betrieb zu integrieren.

Entscheidend wird die frühzeitige Zusammenarbeit zwischen Betreibern, Maschinenbauern und Komponentenherstellern sein, um Kompatibilität, Konformität und Wirtschaftlichkeit in Einklang zu bringen.

Die Einführung des CRA markiert einen Paradigmenwechsel in der Produktverantwortung innerhalb digital vernetzter Industrieumgebungen.

Unternehmen, die frühzeitig handeln, können aus den neuen Anforderungen einen Wettbewerbsvorteil generieren.

Cobot Safety

Vielen Dank für Ihre Aufmerksamkeit