Cyberresilienz-Verordnung als Teil des CE-Konformitätsprozesses in der Praxis

Vergleich zwischen einer automatisierten Roboteranlage zum Transfer von Bauteilen vor einer Metallpresse und einer Roboteranlage, für Materialtransport in der Lebensmittelherstellung (Pizzaherstellung). – Stand 2026 -

Autor: Dipl. -Ing. Christoph Spreuer

DIPL. -ING. C. SPREUER | Emser Straße 19 | 65195 Wiesbaden | Tel. (0611) 59 99 33 | E-Mail: info@spreuer.com | Page: www.spreuer.com

Inhalt

Wie muss die Cyberresilienz-Verordnung Teil als des CE-Konformitätsprozesses in der Praxis umgesetzt werden? 3
Vorwort 3
1. Die wichtigsten Kernpunkte der CRA im Überblick 3
1.1 Zeitplan und wichtige Fristen 4
1.2 Klarheit für Open Source 4
2. Roboteranlagen als integrierte Fertigungssysteme (Integrated Manufacturing Systems - IMS) 4
3. Die Umsetzung der CRA in der Praxis 5
3.1 Produkt klassifizieren 5
3.2 Risikoanalyse & "Security by Design" 5
3.3 Technische Dokumentation & SBOM erstellen 5
3.4 Konformitätsbewertung durchführen 5
3.5 EU-Konformitätserklärung unterschreiben & CE-Zeichen anbringen 5
3.6 Pflichten nach dem Verkauf (Lebenszyklus) 6
4. Ermittlung der Klasse für eine Roboteranlage in der Metallverarbeitung vor einer Presse 6
4.1 Teil 1 - Die CRA-Klassifizierung der Roboteranlage 6
4.2 Teil 2 - Die Software-Stückliste (SBOM) für die Anlage 7
4.3 Praxis-Beispiel für den Aufbau einer SBOM (JSON-Format) 8
4.4 Wie wird das im CE-Prozess angewendet? 8
4.5 Software-Tools zur automatischen Erstellung der SBOM 8
4.6 Drei Kategorien von Software-Tools 9
4.6.1 Kategorie 1: Spezialisierte Tools für Industrie & OT (Am einfachsten für SPS) 9
4.6.2 Kategorie 2: Open-Source-Tools (Über die Code-Ebene) 9
4.6.3 Kategorie 3: Plattformen zur SBOM-Verwaltung und Überwachung 9
4.7 Der Praxis-Workflow für Ihre Roboteranlage 10
4.8 Wie werden Komponenten mit unklarem CRA-Status rechtlich und technisch in der EU-Konformitätserklärung abgesichert? 10
4.8.1 Rechtliche Absicherung in der EU-Konformitätserklärung 10
A. Die Due-Diligence-Erklärung (Sorgfaltspflicht) 10
B. Einbindung über den "Modularen Ansatz" (Grenzen der Verantwortung) 11
4.8.2 Technische Absicherung im CE-Prozess (Wie Sie das Risiko minimieren) 11
4.8.3 Praxis-Formulierung für Ihre Technische Dokumentation 11
4.9 Vorschlag für eine Vertragsklausel / Haftungsübernahme für Zulieferer von Komponenten 12
4.9.1 Option 1: Klausel für den Einkauf neuer Komponenten 12
4.9.2 Option 2: "Übergangs-Klausel" für Komponenten mit unklarem Status 13
4.9.3 Anwendungshinweise für die Praxis: 13

DIPL. -ING. C. SPREUER | Emser Straße 19 | 65195 Wiesbaden | Tel. (0611) 59 99 33 | E-Mail: info@spreuer.com | Page: www.spreuer.com

4.10 Die 24-Stunden-Meldepflicht....14
4.10.1 Phase 1: Der 3-stufige Zeitplan für die Meldung....14
4.10.2 Phase 2: Wann tickt die Uhr? (Die Praxis-Definition)....14
4.11 Praxis-Leitfaden für Ihren Notfallplan (Incident Response)....14
4.12 Wichtig für Ihre Kunden:....15
4.13 Checkliste für die 24-Stunden-Frühwarnung (BSI / ENISA)....16
Teil 1: Checkliste für die 24-Stunden-Frühwarnung (BSI / ENISA)....16
Teil 2: Die Bußgelder bei Verstößen gegen den CRA....17
5. Dokumenten-Muster für die technische Dokumentation....18
5.1 Definition der genauen Netzwerk-Zonen (Zonierung nach IEC 62443) für die Roboterzelle....20
5.1.1 Teil 1: Netzwerk-Zonierung für die Roboterzelle (nach IEC 62443-3-3)....20
5.1.2 Teil 2: Detail-Sicherheitskonzept für das HMI-Bedienpanel....21
5.1.3 Einbindung in die CE-Dokumentation....22
6. Praxisorientierte Inbetriebnahme-Checkliste für die IT-Sicherheit....22
6.1 Was passiert nach der Inbetriebnahme?....24
7. Vergleich mit einer Roboteranlage anstatt zum Materialtransport in der Lebensmittelherstellung 24
7.1 Direkter Vergleich und die Anpassung für eine Pizza-Transportanlage....24
7.2 Die CRA-Klassifizierung:....24
7.3 Das angepasste IT-Sicherheitskonzept (Die Unterschiede in der Praxis)....24
7.4 Summary: Was müssen Sie für die Pizza-Anlage neu schreiben?....25
7.5 Teil 1: Das konkrete Praxis-Beispiel (Das Szenario)....26
7.6 Teil 2: Dokumentation der OPC-UA-Übertragung in der Risikoanalyse....27
7.7 Der Vorteil dieser Dokumentation im CE-Prozess:....28

DIPL. -ING. C. SPREUER | Emser Straße 19 | 65195 Wiesbaden | Tel. (0611) 59 99 33 | E-Mail: info@spreuer.com | Page: www.spreuer.com

Wie muss die Cyberresilienz-Verordnung als Teil des CE-Konformitätsprozesses in der Praxis umgesetzt werden?

Fallbeispiel: Vergleich zwischen einer automatisierten Roboteranlage zum Transfer von Bauteilen vor einer Metallpresse und einer

Roboteranlage, für Materialtransport in der Lebensmittelherstellung (Pizzaherstellung).

Vorwort

Industrieanlagen werden immer smarter, aber dadurch auch ein Ziel für Cyberangriffe. Deshalb erfordert zukunftssichere Automatisierung Cybersicherheit auf allen Ebenen.
Die **Cyberresilienz-Verordnung** (offiziell **Verordnung (EU) 2024/2847**, oft als Cyber Resilience Act (CRA) bezeichnet) ist ein EU-Gesetz, das einheitliche Mindestanforderungen an die Cybersicherheit digitaler Produkte vorschreibt. Das Gesetz soll sicherstellen, dass **vernetzte Hardware und Software über ihren gesamten Lebenszyklus hinweg gegen Cyberangriffe geschützt sind** und Schwachstellen durch Updates geschlossen werden.
Die Verordnung ist im Dezember 2024 in Kraft getreten. Die Umsetzung erfolgt gestaffelt und wird ab **Dezember 2027 für alle betroffenen Produkte vollständig verbindlich**.

Die **CRA** wird direkt in den bestehenden **CE-Konformitätsprozess** für Produkte mit digitalen Elementen integriert. Es gibt kein separates „Cyber-Logo“. Das normale CE-Kennzeichen sagt in Zukunft einfach aus, dass auch die IT-Sicherheit stimmt.
Da Cybersicherheit nicht statisch ist, endet der Prozess im Gegensatz zur klassischen Produktsicherheit (wie z.B. bei der CE-Maschinenrichtlinie) nicht mit dem Verkauf. Er läuft über den gesamten Lebenszyklus des Produkts weiter.

Wie sieht nun die Umsetzung der CRA in der Praxis für industrielle Anlagen aus?

Zunächst soll das für eine automatisierte Roboteranlage zum Transfer von Bauteilen vor einer Metallpresse gezeigt werden.

Im Anschluss erfolgt der Vergleich mit einer Roboteranlage die zum Materialtransport in der Lebensmittelherstellung z.B. Pizzaherstellung genutzt wird.

1. Die wichtigsten Kernpunkte der CRA im Überblick

- **Betroffene Produkte:** Alle Produkte mit „digitalen Elementen“, die direkt oder indirekt mit einem Netzwerk oder anderen Geräten verbunden sind. Dazu gehören Betriebssysteme, IoT-Geräte, Software und Industriesteuerungen.
- **Security by Design:** Sicherheit muss von Anfang an eingeplant werden. Unsichere Standardpasswörter sind verboten und unnötige Dienste müssen ab Werk deaktiviert sein.
- **CE-Kennzeichnung:** Nur Produkte, welche die Cybersicherheitsanforderungen erfüllen, erhalten das CE-Kennzeichen und dürfen im EU-Binnenmarkt verkauft werden.

DIPL. -ING. C. SPREUER | Emser Straße 19 | 65195 Wiesbaden | Tel. (0611) 59 99 33 | E-Mail: info@spreuer.com | Page: www.spreuer.com

- **Software-Stückliste (SBOM):** Hersteller müssen genau dokumentieren und transparent machen, welche Software-Bausteine und Bibliotheken in ihren Produkten stecken.
- **Marktüberwachung:** In Deutschland übernimmt das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Rolle des „digitalen TÜVs“ und kontrolliert die Einhaltung. Bei Verstößen drohen Verkaufsverbote und hohe Geldstrafen.

1.1 Zeitplan und wichtige Fristen

Die Pflichten greifen nicht alle auf einmal, sondern stufenweise: [1]

10. Dezember 2024: Die Verordnung ist offiziell in Kraft getreten.

11. September 2026 Erste Meldepflichten starten: Hersteller müssen aktiv ausgenutzte Schwachstellen und schwere Sicherheitsvorfälle innerhalb von 24 Stunden melden.

11. Dezember 2027 Vollständige Anwendung: Alle neuen Produkte müssen die technischen Vorgaben des CRA erfüllen, um auf dem Markt bereitgestellt zu werden.

1.2 Klarheit für Open Source

Die EU-Kommission hat im Sommer 2026 einen Leitfaden veröffentlicht, der wichtige Ausnahmen für die Open-Source-Community klarstellt. Reine Entwickler, die lediglich Code beisteuern oder Fehler beheben, haften in der Regel nicht. Erst Organisationen oder Stiftungen („Open-Source-Stewards“), die ein Projekt steuern, die Infrastruktur betreiben oder Software-Releases offiziell herausgeben, tragen je nach Intensität ihrer Einbindung Verantwortung und Meldepflichten

2. Roboteranlagen als integrierte Fertigungssysteme (Integrated Manufacturing Systems - IMS)

Roboteranlagen in der hier beschriebenen Form sind per Definition **integrierte Fertigungssysteme (Integrated Manufacturing Systems - IMS).** IMS sind ein Verbund aus zwei oder mehr miteinander verknüpften Maschinen und Anlagen, die zusammenarbeiten, um spezifische Aufgaben wie die Herstellung von Einzelteilen oder Baugruppen zu automatisieren.
Die Sicherheitsnorm EN ISO 11161; 2008 - Sicherheit von Maschinen – Integrierte Fertigungssysteme – beschreibt Grundlegende Anforderungen für IMS.
IMS können in Bezug auf Größe und Komplexität sehr variieren. Statt einer bloßen Kombination seiner verschiedenen Bestandteile, sollte ein integriertes Fertigungssystem vielmehr als eine gänzlich neue und andersartige Maschine betrachtet werden.
Ist permanentes manuelles Eingreifen in Teile des IMS erforderlich, z. B. für Inspektion, Instandhaltung und Einrichten, kann es unzweckmäßig oder unnötig sein, das gesamte IMS anzuhalten. Die in der Norm enthaltenen Anforderungen regeln die Sicherheit jener Personen, welche diese Aufgaben ausführen.

3. Die Umsetzung der CRA in der Praxis

Die Umsetzung der CRA in der Praxis erfolgt in **6 konkreten Schritten**:

3.1 Produkt klassifizieren

Zuerst müssen Sie prüfen, in welche Risiko-Klasse Ihr Produkt fällt. Davon hängt ab, wie streng geprüft wird:

- **Standard-Produkte (ca. 90 %):** Unkritische Hard- und Software (z.B. Smart-Home-Geräte, Spiele, einfache Software).
- **Wichtige Produkte (Klasse I & II):** Produkte mit höherem Risiko (z.B. Passwortmanager, Router, Betriebssysteme).
- **Kritische Produkte:** Hochrisiko-Bereiche (z.B. bestimmte industrielle Steuerungen).

3.2 Risikoanalyse & "Security by Design"

Schon bei der Entwicklung müssen Sie Cybersicherheit einplanen (Security by Design und by Default).

- **Risikoanalyse:** Sie müssen alle digitalen Schnittstellen erfassen und Bedrohungen aufschreiben.
- **Vorgaben umsetzen:** Keine Standard-Passwörter erlauben. Daten verschlüsseln. Unnötige Funktionen ab Werk abschalten.

3.3 Technische Dokumentation & SBOM erstellen

Sie müssen eine digitale "Akte" für das Produkt anlegen und für Behörden bereithalten:

- **Software-Stückliste (SBOM):** Eine genaue Liste aller verwendeten Software-Komponenten, Bibliotheken und Open-Source-Teile.
- **Architektur:** Beschreibung, wie das Produkt digital aufgebaut ist und wie Updates funktionieren.

3.4 Konformitätsbewertung durchführen

Hier wird offiziell bewiesen, dass das Produkt sicher ist:

- **Bei Standard-Produkten:** Der Hersteller darf die Prüfung selbst machen (Interne Kontrolle / Modul A). Sie brauchen keine externe Prüfstelle.
- **Bei wichtigen/kritischen Produkten:** Hier ist oft eine Prüfung durch eine unabhängige Organisation ("Notified Body" wie TÜV, DEKRA etc.) zwingend nötig.

3.5 EU-Konformitätserklärung unterschreiben & CE-Zeichen anbringen

- Sie schreiben eine **EU-Konformitätserklärung**. Darin listen Sie den CRA und genutzte technische Normen auf.
- Erst danach bringen Sie das **CE-Zeichen** auf dem Produkt, der Verpackung oder der Anleitung an.

3.6 Pflichten nach dem Verkauf (Lebenszyklus)

Das ist die größte Neuerung in der Praxis. Nach dem Verkaufsstart gelten harte Pflichten:

- **Update-Pflicht:** Sie müssen in der Regel mindestens 5 Jahre lang (oder für die erwartete Lebensdauer) kostenlose Sicherheitsupdates bereitstellen.
- **Schwachstellen-Management:** Wenn eine Sicherheitslücke entdeckt wird, müssen Sie diese aktiv bearbeiten und Kunden informieren.
- **Meldepflicht:** Aktiv ausgenutzte Schwachstellen oder schwere Cyber-Vorfälle müssen **binnen 24 Stunden** an die Behörden (z.B. ENISA / BSI) gemeldet werden.

4. Ermittlung der Klasse für eine Roboteranlage in der Metallverarbeitung vor einer Presse

4.1 Teil 1 - Die CRA-Klassifizierung der Roboteranlage

In der Praxis müssen Sie zwischen der **Gesamtanlage** und den **eingekauften Komponenten** unterscheiden:

Die Gesamtanlage (Das integrierte System)
Eine verkettete Roboteranlage, die Signale mit einer Presse austauscht, fällt unter die Kategorie **Industrial Automation Control Systems (IACS)** (Industrielle Automatisierungs- und Steuerungssysteme).

- **Einstufung:** Diese Systeme werden im CRA in die **Klasse I (Wichtige Produkte / "Important Class I")** eingeordnet.
- **Konsequenz für den CE-Prozess:** Sie können die Konformität nicht mehr durch eine reine, formlose Selbsterklärung bescheinigen, es sei denn, Sie nutzen eine voll harmonisierte Norm (wie die künftigen CRA-Erweiterungen der Industrienorm **IEC 62443**). Gibt es keine harmonisierte Norm oder weichen Sie davon ab, müssen Sie eine benannte Stelle (*Notified Body*) für ein Audit einbinden.

Die Einzelkomponenten (Zulieferteile)
Als Integrator der Anlage verbauen Sie Komponenten, die oft selbst in eine noch höhere Risikoklasse fallen:

- **Klasse II (Highly Important / Critical):** Wenn Sie in der Anlage zentrale Firewalls, Router für den Fernwartungszugang (VPN-Gateways) oder industrielle Steuerungen (SPS) mit direktem Netzwerkknoten verbauen, fallen diese Einzelkomponenten unter Klasse II. [1, 2]
- *Praxis-Tipp:* Verlangen Sie von Ihren Zulieferern (Roboterhersteller, SPS-Hersteller) zwingend deren eigene CRA-Konformitätserklärung, da Sie deren Komponenten in Ihr System integrieren.

DIPL. -ING. C. SPREUER | Emser Straße 19 | 65195 Wiesbaden | Tel. (0611) 59 99 33 | E-Mail: info@spreuer.com | Page: www.spreuer.com

4.2 Teil 2 - Die Software-Stückliste (SBOM) für die Anlage

Die **Software Bill of Materials (SBOM)** ist wie die Zutatenliste auf einer Lebensmittelverpackung – nur für Software. Da Ihre Roboteranlage aus Hardware, Firmware und Steuerungssoftware besteht, müssen Sie genau dokumentieren, was digital darin steckt.

Was muss in der Praxis in die SBOM hinein?

Sie müssen für die Steuerungssoftware der Anlage (z. B. das SPS-Programm oder die Roboterbahnsteuerung) folgende Schichten erfassen:

- **Hersteller-Informationen:** Name des Software-Entwicklers (Ihr Unternehmen oder der Zulieferer).
- **Komponenten-Name:** Exakte Bezeichnung der Software-Module (z. B. Robot_Grabber_Logic_V2).
- **Versionsnummer:** Die genaue Build- oder Revisionsnummer.
- **Einzigartige IDs:** Eindeutige Kennungen wie CPE (*Common Platform Enumeration*) oder PURL (*Package URL*), um Sicherheitslücken später automatisch abgleichen zu können.
- **Abhängigkeiten (Dependencies):** Verwendete Bibliotheken. Wenn Ihre Robotersteuerung beispielsweise ein Open-Source-Protokoll zur Datenübertragung (wie z. B. eine *Node-OPC-UA*-Bibliothek) nutzt, muss dieses exakt aufgeführt werden.
- **Lizenz-Informationen:** Unter welchen Rechten die Software läuft (z. B. proprietär oder MIT-Lizenz).

4.3 Praxis-Beispiel für den Aufbau einer SBOM (JSON-Format)

In der Industrie haben sich automatisierte Standardformate wie **CycloneDX** oder **SPDX** durchgesetzt. Ein vereinfachter Ausschnitt für Ihre Transferanlage sieht in der Praxis so aus:

json

```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.5",
  "component": {
    "name": "Roboter-Transfer-System-Presse",
    "version": "1.0.4",
    "type": "firmware",
    "components": [
      {
        "publisher": "Roboter-Hersteller XYZ",
        "name": "Core-Robot-OS",
        "version": "8.32.1",
        "purl": "pkg:generic/robotxyz/core-os@8.32.1"
      },
      {
        "publisher": "Inhouse-Engineering",
        "name": "Presse-Interlocking-Modul",
        "version": "1.2.0",
        "description": "Sicherheitsverriegelung und Transferfreigabe zur Presse"
      },
      {
        "publisher": "Open Source Community",
        "name": "libmodbus",
        "version": "3.1.10",
        "licenses": [ { "license": { "id": "LGPL-2.1-or-later" } } ]
      }
    ]
  }
}
```

Verwende Code mit Vorsicht.

4.4 Wie wird das im CE-Prozess angewendet?

- **Automatische Überwachung:** Diese SBOM-Datei verbleibt in Ihrer technischen Dokumentation.
- **Lebenszyklus-Prüfung:** Wenn das Bundesamt für Sicherheit in der Informationstechnik (BSI) oder die ENISA eine neue kritische Schwachstelle (z. B. in der gezeigten Bibliothek libmodbus) meldet, müssen Sie mittels Ihrer SBOM sofort prüfen können: *"Ist meine Roboteranlage an der Presse betroffen?"* Wenn ja, tickt die 24-Stunden-Uhr für die Meldepflicht und Sie müssen ein Sicherheitsupdate bereitstellen.

4.5 Software-Tools zur automatischen Erstellung der SBOM

Mit welchen Software-Tools kann eine solche SBOM für Ihre SPS- oder Roboterprogramme am einfachsten automatisch erzeugt werden, unabhängig von konkreten Zuliefer-Komponenten, deren CRA-Status unklar ist?

Bei Automatisierungsanlagen (SPS und Robotik) steht man in der Praxis vor einer Hürde:

Klassische IT-Tools scannen vollautomatisch Paketmanager (wie npm oder pip), doch die Steuerungs- und Engineering-Software der Industrie (z. B. Siemens TIA Portal, Beckhoff TwinCAT oder CODESYS) nutzt proprietäre Binärdaten und IEC 61131-3-Code.

Um eine SBOM automatisch zu erstellen – **unabhängig** davon, ob Zulieferer-Komponenten ihren CRA-Status schon geklärt haben oder nicht –, nutzt man in der Praxis primär **SCA-Tools (Software Composition Analysis)** und spezialisierte **Industrial-OT-Plattformen**.

4.6 Drei Kategorien von Software-Tools

Die Erzeugung lässt sich in drei Kategorien von Software-Tools unterteilen:

4.6.1 Kategorie 1: Spezialisierte Tools für Industrie & OT (Am einfachsten für SPS)

Diese Tools wurden speziell für die Automatisierungstechnik entwickelt. Sie verstehen SPS-Architekturen und können aus den Projektdateien der Hersteller automatisch Stücklisten extrahieren, ohne dass Sie Quellcode manuell abtippen müssen.

- **ONEKEY:** Eine führende Plattform im Bereich Product Cybersecurity. Sie ist darauf spezialisiert, die Firmware von Steuerungen (SPS, Edge-Gateways, Industrie-Router) im Binärformat zu analysieren (*Binary Analysis*). Sie laden einfach das Firmware-Image oder das kompilierte Projekt hoch, und das Tool extrahiert vollautomatisch eine CRA-konforme SBOM (in den Formaten CycloneDX oder SPDX).
- **PLC-Sicherheits-Scanner (z. B. von Rhebo oder Claroty):** Diese Tools analysieren primär den Netzwerkverkehr der Roboterzelle an der Presse. Sie erkennen vollautomatisch, welche Steuerungen, Firmware-Stände und Kommunikations-Bibliotheken aktiv im Netz sind, und generieren daraus die Asset-Stückliste.

4.6.2 Kategorie 2: Open-Source-Tools (Über die Code-Ebene)

Wenn Ihre SPS-Programme oder Roboter-Skripte strukturierte Textdateien (z. B. *Structured Text / ST*, Python-Skripte für Roboter oder C++ Module) nutzen, greifen klassische, mächtige Open-Source-Generatoren.

- **Syft (by Anchore):** Das weltweit populärste Open-Source-Tool zur SBOM-Generierung. Es durchsucht Dateisysteme extrem schnell. Wenn Sie z. B. PC-basierte Steuerungen (wie Beckhoff TwinCAT) oder Open-Source-Komponenten im System nutzen, listet **Syft** alle Abhängigkeiten in Sekunden als JSON oder CycloneDX auf.
- **cdxgen (OWASP CycloneDX Generator):** Das offizielle Tool der OWASP-Organisation. Es ist ein "Allesfresser" und hervorragend geeignet, wenn Ihre Robotersteuerung oder HMI-Bedienpanels auf Linux/Windows-Basis aufbauen. Es scannt die Verzeichnisse und erzeugt vollautomatisch die nötige Struktur.

4.6.3 Kategorie 3: Plattformen zur SBOM-Verwaltung und Überwachung

Ein Tool erzeugt die SBOM nur einmal. Da der CRA aber verlangt, dass Sie Schwachstellen über Jahre hinweg *aktiv überwachen* müssen, benötigen Sie eine Verwaltungssoftware.

- **OWASP Dependency-Track:** Dieses kostenfreie, plattformunabhängige Tool ist der Industriestandard für das Management. Sie füttern es mit der SBOM Ihrer Roboteranlage (z. B. erzeugt durch *Syft*). **Dependency-Track** gleicht die Stückliste rund um die Uhr

DIPL. -ING. C. SPREUER | Emser Straße 19 | 65195 Wiesbaden | Tel. (0611) 59 99 33 | E-Mail: info@spreuer.com | Page: www.spreuer.com

automatisch mit weltweiten Schwachstellen-Datenbanken (NVD) ab. Gibt es morgen eine Sicherheitslücke in einer von Ihnen genutzten Modbus- oder OPC-UA-Bibliothek, schlägt das System sofort Alarm.

4.7 Der Praxis-Workflow für Ihre Roboteranlage

Da der CRA-Status Ihrer Zulieferer unklar ist, gehen Sie am besten so vor:

- **Exportieren:** Nutzen Sie die Export-Funktionen Ihrer Engineering-Software (z. B. die XML- oder Projekt-Exporte im TIA Portal oder CODESYS), um die Software- und Hardware-Struktur der Anlage als Datei zu sichern.
- **Generieren:** Lassen Sie ein Tool wie **ONEKEY** oder **Syft** über diese Export-Ordner laufen, um die Basis-SBOM im **CycloneDX-Format** zu erzeugen. Komponenten ohne klaren CRA-Status tauchen hier einfach mit ihrem aktuellen Versionsstand als "Zulieferer-Software" auf.
- **Überwachen:** Importieren Sie die Datei in **Dependency-Track**, um die Anlage für die geforderten 5 Jahre im Monitoring zu haben.

4.8 Wie werden Komponenten mit unklarem CRA-Status rechtlich und technisch in der EU-Konformitätserklärung abgesichert?

Wenn Sie als Integrator die Roboteranlage (das Gesamtsystem) in den Verkehr bringen, tragen **Sie rechtlich die Gesamtverantwortung** für die CE-Konformität.
Der **Cyber Resilience Act (CRA)** regelt die Integration von Drittkomponenten (Zulieferteile oder Open Source) sehr strikt:

Sie dürfen Komponenten mit unklarem oder fehlendem CRA-Status nicht einfach "durchwinken".

Wenn Sie die Anlage bis zur vollständigen CRA-Pflicht ab **Dezember 2027** verkaufen, müssen Sie diese unklaren Komponenten über Ihre eigene technische Dokumentation und Risikoanalyse rechtlich und technisch absichern.

4.8.1 Rechtliche Absicherung in der EU-Konformitätserklärung

In der Konformitätserklärung (DoC) für Ihre Gesamtanlage unterschreiben Sie, dass das System die grundlegenden Sicherheitsanforderungen des CRA erfüllt. Komponenten mit unklarem Status sichern Sie rechtlich über zwei Hebel ab:

A. Die Due-Diligence-Erklärung (Sorgfaltspflicht)

Sie müssen in Ihrer technischen Dokumentation nachweisen, dass Sie Ihre **Sorgfaltspflicht (Due Diligence)** erfüllt haben. Das bedeutet: Sie müssen den Zulieferer nachweislich schriftlich kontaktiert, den Status abgefragt und die Antwort dokumentiert haben. Reagiert der Zulieferer

nicht, geht das Risiko voll auf Sie über – Sie müssen die Komponente dann behandeln wie eine eigene Eigenentwicklung.

B. Einbindung über den "Modularen Ansatz" (Grenzen der Verantwortung)

In der Konformitätserklärung listen Sie alle harmonisierten Normen (z. B. Teile der **IEC 62443**) auf, die Sie für das Gesamtsystem angewendet haben.

Sie schreiben **nicht** hinein: *"Die Komponente X von Hersteller Y ist sicher."*

- Sie schreiben hinein: *"Das Gesamtsystem (inklusive der Schnittstellen zu Drittkomponenten) wurde gemäß den Anforderungen des CRA geprüft."*
  Damit verschieben Sie den Fokus von der *Zulieferer-Compliance* auf die *System-Integrität*.

4.8.2 Technische Absicherung im CE-Prozess (Wie Sie das Risiko minimieren)

Da Sie für die Sicherheit der unklaren Komponente haften, müssen Sie das technische Risiko durch eigene Maßnahmen auf Systemebene isolieren (sogenannte **Kompensierende Maßnahmen**):

- **Netzwerk-Isolierung (Zonierung):** Packen Sie die unklare Komponente in ein eigenes, stark abgesichertes Netzwerksegment (VLAN) innerhalb der Roboterzelle. Beschränken Sie den Datenverkehr zur Presse oder zum Firmennetzwerk über eine Firewall auf das absolute Minimum.
- **Eigene Schwachstellen-Scans (Black-Box-Testing):** Da Sie keine Hersteller-SBOM oder Sicherheitsgarantien haben, müssen Sie die Komponente selbst technisch prüfen. Nutzen Sie Tools wie *ONEKEY* für eine automatisierte Binäranalyse der Firmware. Findet das Tool kritische Lücken, müssen Sie den Zugang zu dieser Komponente sperren oder patchen.
- **Übernahme des Schwachstellen-Managements:** In Ihrer SBOM taucht die unklare Komponente mit Name und Version auf. Sie müssen diese ab jetzt in Ihrem eigenen Tool (z. B. *Dependency-Track*) überwachen. Wenn eine kritische Sicherheitslücke (CVE) für diese Zulieferkomponente gemeldet wird, müssen Sie reagieren – entweder indem Sie beim Hersteller Druck machen oder die Anlage durch eine Firewall-Regel schützen.

4.8.3 Praxis-Formulierung für Ihre Technische Dokumentation

In der offiziellen **EU-Konformitätserklärung** wird die unklare Komponente in der Regel nicht namentlich als "Risiko" erwähnt, um das CE-Zeichen nicht zu gefährden. Stattdessen verweisen Sie in der **zugehörigen technischen Dokumentation** (die Sie für Behörden bereithalten müssen) auf Ihr Sicherheitskonzept:

Beispiel-Eintrag für die Risikoanalyse:

"Für die Steuerungskomponente [Name] liegt zum Zeitpunkt des Inverkehrbringens keine separate CRA-Konformitätserklärung des Zulieferers vor. Das daraus resultierende Risiko von unentdeckten Softwareschachstellen wurde durch folgende kompensierende Maßnahmen auf Systemebene auf ein akzeptables Minimum reduziert: 1. Vollständige Kapselung in der Netzwerk-

Zone 'Roboter-Intern'. 2. Deaktivierung aller ungenutzten physischen und logischen Schnittstellen. 3. Einbindung der Komponente in das kontinuierliche Schwachstellen-Monitoring des Integrators."

Wichtiger Hinweis zur Frist:
Falls eine Komponente vor dem Stichtag im **Dezember 2027** unverändert eingekauft wurde, greift für diese oft noch eine Übergangsregelung (Bestandsschutz), solange sie von Ihnen nicht substanziell verändert wird. Sobald Sie die Gesamtanlage aber nach Dezember 2027 neu in den Verkehr bringen, müssen Sie als Integrator dafür geradestehen, dass das Gesamtsystem CRA-konform ist.

4.9 Vorschlag für eine Vertragsklausel / Haftungsübernahme für Zulieferer von Komponenten

Für eine rechtliche Absicherung im Einkauf sollten diese Klauseln direkt in die **Einkaufsbedingungen**, in der **Qualitätsmanagement-Vereinbarung (QMV)** oder im **Lastenheft** für die Zulieferkomponenten verankert werden.
Da Hersteller des Gesamtsystems ab dem offiziellen CRA-Stichtag im **Dezember 2027** voll für die Cybersicherheit der Roboteranlage haften, muss das Haftungs- und Arbeitsrisiko vertraglich an die Zulieferer weitergegeben werden.

Hier sind zwei rechtliche Vorlagen, die für Verträge genutzt werden können:

4.9.1 Option 1: Klausel für den Einkauf neuer Komponenten

(Nutzen Sie diese Variante, wenn Sie neue Komponenten für die Roboteranlage einkaufen und die volle CRA-Unterstützung erzwingen wollen.)

§ X Einhaltung des EU Cyber Resilience Acts (CRA) und IT-Sicherheit

1. Der Lieferant garantiert, dass alle gelieferten Produkte mit digitalen Elementen (Hardware, Software, Firmware) den Anforderungen der Verordnung (EU) 2024/2847 (Cyber Resilience Act – CRA) in der jeweils gültigen Fassung entsprechen. Der Lieferant stellt dem Besteller unaufgefordert eine gültige EU-Konformitätserklärung sowie die erforderlichen Sicherheitsinformationen und Betriebsanleitungen in digitaler Form zur Verfügung.
2. Der Lieferant ist verpflichtet, dem Besteller spätestens bei Lieferung eine maschinenlesbare Software-Stückliste (Software Bill of Materials – SBOM) in einem gängigen Standardformat (vorzugsweise CycloneDX oder SPDX) für alle im Produkt enthaltenen Softwarekomponenten (einschließlich Open-Source-Software) bereitzustellen.
3. Der Lieferant verpflichtet sich, über den gesamten erwarteten Lebenszyklus des Produkts, mindestens jedoch für einen Zeitraum von 5 Jahren ab Lieferung, kostenfreie Sicherheitsupdates zur Behebung von Schwachstellen zur Verfügung zu stellen.
4. Der Lieferant wird dem Besteller aktiv ausgenutzte Schwachstellen oder Sicherheitsvorfälle, die das gelieferte Produkt betreffen, unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Bekanntwerden, schriftlich oder in Textform melden.
5. Verstößt der Lieferant gegen die Pflichten aus dieser Vereinbarung oder führt ein Mangel der IT-Sicherheit des gelieferten Produkts zu einer Verzögerung oder Verweigerung der CE-Zertifizierung des Gesamtsystems des Bestellers, stellt der Lieferant den Besteller von allen daraus resultierenden Schäden, behördlichen Bußgeldern und Kosten der Rechtsverteidigung frei.

4.9.2 Option 2: "Übergangs-Klausel" für Komponenten mit unklarem Status

(Nutzen Sie diese Variante, wenn der Zulieferer aktuell noch keine CRA-Erklärung liefern kann, Sie ihn aber für den Übergang zu Zuarbeit und Schadensersatz verpflichten wollen.)

§ X Mitwirkungspflichten zur Cybersicherheit und CRA-Compliance

1. Soweit für den Liefergegenstand zum Zeitpunkt der Lieferung noch keine offizielle EU-Konformitätserklärung nach dem Cyber Resilience Act (CRA) vorliegt, verpflichtet sich der Lieferant, den Besteller bei dessen eigener Risikoanalyse und Konformitätsbewertung des Gesamtsystems bestmöglich zu unterstützen.
2. Der Lieferant wird dem Besteller auf Verlangen alle hierfür erforderlichen technischen Details offenlegen. Dies umfasst insbesondere Auskünfte über verwendete Drittsoftware/Open-Source-Bibliotheken, bekannte Schwachstellen sowie Dokumentationen über implementierte Sicherheitsfunktionen (z.B. Verschlüsselung, Zugriffskontrollen).
3. Der Lieferant sichert zu, dass das Produkt keine bekannten kritischen Schwachstellen (z.B. gemäß CVSS-Score v3 > 7.0) aufweist, für die kein offizieller Patch zur Verfügung steht. Er wird den Besteller unverzüglich informieren, sobald ihm Sicherheitsrisiken im Liefergegenstand bekannt werden.
4. Der Lieferant stellt sicher, dass im Falle einer behördlichen Überprüfung des Gesamtsystems durch die Marktüberwachungsbehörden alle notwendigen technischen Nachweise bezüglich des Liefergegenstandes innerhalb von 5 Werktagen nachgeliefert werden. Der Lieferant haftet für alle Schäden und Verzögerungen, die dem Besteller durch eine verspätete oder unvollständige Zuarbeit entstehen.

4.9.3 Anwendungshinweise für die Praxis:

- **Wichtig bei Fristen:** Da der CRA im Herbst 2024 final verabschiedet wurde und die Pflichten für Hersteller nach der 36-monatigen Übergangsphase im **Oktober/November 2027** (bzw. Dezember 2027 je nach exakter Amtsblatt-Veröffentlichung) voll greifen, sollten Sie Option 1 ab sofort zum Standard für alle neuen Rahmenverträge machen.
- **Haftungsgrenzen prüfen:** Zulieferer versuchen oft, ihre Gesamthaftung auf den Warenwert der gelieferten Komponente (z.B. eine SPS für 2.000 €) zu begrenzen. Da ein Cyber-Vorfall oder ein Verkaufsstopp Ihrer gesamten Roboterpresse aber Schäden im sechs- oder siebenstelligen Bereich verursachen kann, sollten Sie die CRA-Haftung in Ihren Verträgen explizit von der normalen Haftungsbegrenzung ausnehmen.

Die 24-Stunden-Meldepflicht gehört zu den schärfsten Regeln des Cyber Resilience Acts (CRA). Wenn an Ihrer Roboteranlage an der Presse eine Sicherheitslücke ausgenutzt wird (z. B. durch Ransomware oder unbefugten Fernzugriff), müssen Sie extrem schnell handeln.
Hier ist der genaue Ablauf in der Praxis, aufgeteilt in zwei Phasen:

DIPL. -ING. C. SPREUER | Emser Straße 19 | 65195 Wiesbaden | Tel. (0611) 59 99 33 | E-Mail: info@spreuer.com | Page: www.spreuer.com

4.10 Die 24-Stunden-Meldepflicht

4.10.1 Phase 1: Der 3-stufige Zeitplan für die Meldung

Sie müssen den Vorfall an zwei Stellen melden: an die europäische Cybersicherheitsbehörde **ENISA** (über ein zentrales EU-Portal) und an Ihre nationale Marktüberwachungsbehörde (in Deutschland das **BSI**).

Zeitfenster	Art der Meldung	Was muss gemeldet werden?
Innerhalb von 24 Stunden	**Frühwarnung** *(Early Warning)*	* Dass ein Vorfall vorliegt. * Ob der Verdacht auf Sabotage oder Erpressung besteht. * Erste grobe Einschätzung der Auswirkungen.
Innerhalb von 72 Stunden	**Vorfallsmeldung** *(Incident Notification)*	* Detaillierte Infos zum Vorfall. * Aktualisierte Risikobewertung. * Erste technische Details (Indikatoren für eine Kompromittierung / IoCs).
Innerhalb von 1 Monat	**Abschlussbericht** *(Final Report)*	* Genaue Ursachenanalyse (Root Cause). * Eingeleitete Gegenmaßnahmen (Patches, Firewall-Regeln). * Langfristige Auswirkungen auf die Anlage.

4.10.2 Phase 2: Wann tickt die Uhr? (Die Praxis-Definition)

Die 24-Stunden-Frist beginnt in dem Moment, in dem Ihr Unternehmen **Kenntnis** von dem Vorfall erlangt (*"becomes aware"*).

4.10.3 Wann gilt ein Vorfall als meldepflichtig?

Nicht jeder harmlose Software-Fehler muss gemeldet werden. Es müssen zwei Bedingungen erfüllt sein:

1. **Aktiv ausgenutzt:** Die Sicherheitslücke wird tatsächlich von Angreifern angegriffen (z. B. Schadsoftware versucht, Schadcode auf die SPS der Roboteranlage aufzuspielen).
2. **Schwere Auswirkung:** Der Angriff führt zu einem Sicherheitsrisiko. Bei Ihrer Anlage an der Presse bedeutet das konkret: Der Angriff führt zu einem Produktionsstillstand, hebelt Sicherheitsverriegelungen aus oder ermöglicht unbefugten Fernzugriff von außen.

4.11 Praxis-Leitfaden für Ihren Notfallplan (Incident Response)

Da 24 Stunden extrem kurz sind, können Sie diese Meldung nicht erst am Tag des Angriffs vorbereiten. Sie benötigen ein festes Ablaufschema in Ihrem Unternehmen:

[Schritt 1: Erkennung]
Anlage meldet Fehler oder IT-Abteilung bemerkt ungewöhnlichen Datenverkehr zur Presse.



[Schritt 2: Technische Bewertung]
Prüfung durch IT-Sicherheit: Wird eine Schwachstelle aktiv ausgenutzt? (Dauer: max. 2-4 Std.)



[Schritt 3: 24h-Frühwarnung]
Meldung über das ENISA/BSI-Portal abgeben. (Auch wenn noch nicht alle Details feststehen!)



[Schritt 4: Eindämmung]
Anlage isolieren (Netzwerkstecker ziehen), um weiteren Schaden zu verhindern.



[Schritt 5: Zulieferer einbinden]
Den Roboter-/SPS-Hersteller über die Vertragsklausel zwingen, sofort einen Patch bereitzustellen.

4.12 Wichtig für Ihre Kunden:

Der CRA verpflichtet Sie auch, die **Betreiber der Anlage** (Ihre Kunden, die die Presse und den Roboter nutzen) unverzüglich über den Vorfall und über mögliche Schutzmaßnahmen zu informieren. Sie dürfen den Vorfall also nicht verheimlichen, um Ihren Ruf zu schützen.

DIPL. -ING. C. SPREUER | Emser Straße 19 | 65195 Wiesbaden | Tel. (0611) 59 99 33 | E-Mail: info@spreuer.com | Page: www.spreuer.com

4.13 Checkliste für die 24-Stunden-Frühwarnung (BSI / ENISA)

Teil 1: Checkliste für die 24-Stunden-Frühwarnung (BSI / ENISA)

Bei der ersten Meldung müssen Sie noch **keine** tiefgehende IT-Forensik vorlegen. Die Behörden wollen primär wissen, dass etwas passiert ist, um im Zweifel andere Unternehmen vor derselben Angriffswelle zu warnen.

Folgende Kernpunkte müssen Sie bereithalten:

- **Identität des Herstellers:** Name des Unternehmens, Kontaktdaten des zuständigen Sicherheitsansprechpartners (CISO / IT-Leiter).
- **Betroffenes Produkt:** Exakte Bezeichnung der Roboteranlage (Modell, Seriennummernbereich, Software-Version laut Ihrer SBOM).
- **Zeitpunkt der Feststellung:** Wann genau wurde der Angriff bemerkt? (Datum und Uhrzeit).
- **Art des Vorfalls:** Kurze Beschreibung (z. B. *"Unbefugter Zugriff auf die SPS-Steuerung über die Fernwartungsschnittstelle"* oder *"Ransomware-Verschlüsselung des Steuerungsrechners"*).
- **Erste Schadenseinschätzung:** Hat der Vorfall Auswirkungen auf die funktionale Sicherheit (z. B. Gefahr für Leib und Leben an der Presse) oder "nur" auf die Verfügbarkeit der Anlage (Produktionsstillstand)?
- **Grenzüberschreitende Relevanz:** Steht die Anlage bei einem Kunden im EU-Ausland oder sind Anlagen in mehreren EU-Ländern betroffen?

Praxis-Tipp: Richten Sie im Unternehmen eine Standard-E-Mail-Vorlage oder ein Webformular-Konto beim **BSI** (bzw. dem zentralen EU-Meldepunkt der ENISA) ein, damit Sie diese Daten im Ernstfall nur noch einfügen müssen.

Teil 2: Die Bußgelder bei Verstößen gegen den CRA

Der Cyber Resilience Act droht bei Missachtung der Regeln mit extrem empfindlichen Strafen. Die Bußgelder sind prozentual am weltweiten Jahresumsatz orientiert – ähnlich wie bei der DSGVO. Sie sind in drei Stufen unterteilt:

Verstoß	Maximales Bußgeld
Verstoß gegen die wesentlichen Sicherheitsanforderungen (z.B. Sie verkaufen die Anlage trotz bekannter, kritischer Sicherheitslücken oder ohne Risikoanalyse).	Bis zu **15.000.000 €** oder **2,5 %** des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres (je nachdem, welcher Betrag *höher* ist).
Verstoß gegen die Melde- und Update-Pflichten (Hierunter fällt das **Verschweigen oder die verspätete Meldung** eines Vorfalls innerhalb der 24-Stunden-Frist).	Bis zu **10.000.000 €** oder **2,0 %** des weltweiten Jahresumsatzes (je nachdem, welcher Betrag *höher* ist).
Falsche, unvollständige oder irreführende Angaben gegenüber den Marktüberwachungsbehörden (z. B. eine manipulierte SBOM oder gefälschte Testberichte).	Bis zu **5.000.000 €** oder **1,0 %** des weltweiten Jahresumsatzes (je nachdem, welcher Betrag *höher* ist).

Wer verhängt die Strafen in Deutschland?
In Deutschland überwachen die Marktüberwachungsbehörden der Bundesländer in enger Zusammenarbeit mit dem **BSI** die Einhaltung des CRA. Die Behörden haben zudem das Recht, das **CE-Kennzeichen zu entziehen** und einen **Verkaufsstopp** oder einen **Rückruf** für Ihre Roboteranlagen anzuordnen, falls diese als gravierendes Sicherheitsrisiko für die Industrie eingestuft werden.

DIPL. -ING. C. SPREUER | Emser Straße 19 | 65195 Wiesbaden | Tel. (0611) 59 99 33 | E-Mail: info@spreuer.com | Page: www.spreuer.com

5. Dokumenten-Muster für die technische Dokumentation

Hier ist ein kurzes, praxisorientiertes Dokumenten-Muster für die IT-Risikoanalyse Ihrer Roboteranlage. Dieses Muster orientiert sich an den gängigen Standards der industriellen Cybersicherheit (**IEC 62443**) und erfüllt die Anforderungen, die der Cyber Resilience Act (CRA) für die technische Dokumentation vorschreibt.

Produkt/System: Integrierte Roboter-Transferanlage (Presse-Zuführung)
Modell/Typ: TR-Robot-Press-Link v1.0
Hersteller: [Ihr Unternehmensname]
Datum der Erstellung: 27. August 2026
Verantwortlicher: [Name/Rolle, z. B. IT-Sicherheitsbeauftragter OT]

---

1. Systembeschreibung & Netzwerktopologie (Asset-Identifikation)
Die Anlage besteht aus einer 6-Achs-Robotersteuerung (Zulieferer XYZ), einer zentralen Anlagen-SPS (Siemens S7-1500) zur Verriegelung mit der Presse sowie einem integrierten VPN-Router für die Fernwartung. Die Kommunikation erfolgt intern über PROFINET und Modbus/TCP.

---

2. Risikomatrix (Bewertungsmethode)

Das Risiko berechnet sich aus: **Eintrittswahrscheinlichkeit (1-5) × Auswirkung bei Eintritt (1-5)** = **Risikowert (1-25)**.
*Ab einem Risikowert von **10** (Medium/High) sind technische oder organisatorische Gegenmaßnahmen zwingend erforderlich.*

---

3. Spezifische Bedrohungsanalyse & Maßnahmenkatalog

Bedrohung 1: Unbefugter Zugriff über die Fernwartungsschnittstelle

- **Beschreibung:** Ein Angreifer kompromittiert den Fernwartungszugang und manipuliert die Roboter-Bahndaten oder die Pressen-Verriegelung.
- **Anfängliches Risiko:** Wahrscheinlichkeit (4) × Auswirkung (5) = **20 (Kritisch)**
- **Kompensierende Maßnahmen (Umsetzung):**
    1. *Technisch:* Einsatz von Zwei-Faktor-Authentifizierung (2FA) für jeden Fernzugriff.
    2. *Technisch:* Hardware-Schlüsselschalter an der Anlage („Fernwartung EIN/AUS“), damit der Kunde den Zugriff physisch freigeben muss.
- **Restrisiko nach Maßnahmen:** Wahrscheinlichkeit (1) × Auswirkung (5) = **5 (Akzeptabel)**

Bedrohung 2: Einschleppen von Schadsoftware (Ransomware) via USB-Schnittstelle

- **Beschreibung:** Ein Servicetechniker steckt einen infizierten USB-Stick an das HMI-Bedienpanel an. Die SPS wird verschlüsselt, es kommt zum Produktionsstillstand.
- **Anfängliches Risiko:** Wahrscheinlichkeit (3) × Auswirkung (4) = **12 (Medium)**
- **Kompensierende Maßnahmen (Umsetzung):**
    1. *Technisch:* Physische Deaktivierung oder Sperrung aller ungenutzten USB-Ports im BIOS/Betriebssystem des HMI-Panels.
    2. *Organisatorisch:* Schulung und Verpflichtung des Servicepersonals, nur geprüfte, firmeneigene Laptops/Sticks zu verwenden.
- **Restrisiko nach Maßnahmen:** Wahrscheinlichkeit (1) × Auswirkung (4) = **4 (Akzeptabel)**

Bedrohung 3: Ausnutzung einer bekannten Schwachstelle in einer Zulieferkomponente (z. B. OPC-UA-Bibliothek)

- **Beschreibung:** Eine im Roboter-OS integrierte Kommunikationsbibliothek weist eine kritische Sicherheitslücke auf, für die der Zulieferer (noch) keinen Patch bereitstellt.
- **Anfängliches Risiko:** Wahrscheinlichkeit (4) × Auswirkung (3) = **12 (Medium)**
- **Kompensierende Maßnahmen (Umsetzung):**
    1. *Technisch (Zonierung):* Die Robotersteuerung wird in ein eigenes VLAN („Zone Roboter-Intern“) gepackt. Die Firewall erlaubt nur zwingend nötige Protokolle zur Presse-SPS.
    2. *Organisatorisch:* Aufnahme der Komponente in das automatisierte Schwachstellen-Monitoring (*Dependency-Track*) mittels der Anlagen-SBOM.
- **Restrisiko nach Maßnahmen:** Wahrscheinlichkeit (2) × Auswirkung (3) = **6 (Akzeptabel)**

---

4. Kontinuierliches Schwachstellen-Management & Freigabe

Hiermit wird bestätigt, dass alle identifizierten Risiken durch die oben genannten Maßnahmen auf ein akzeptables Minimum reduziert wurden. Die Software-Stückliste (SBOM) wurde am [Datum] generiert und in das Überwachungssystem eingepflegt.

Freigegeben durch:
Unterschrift Geschäftsführung / IT-Sicherheitsleitung

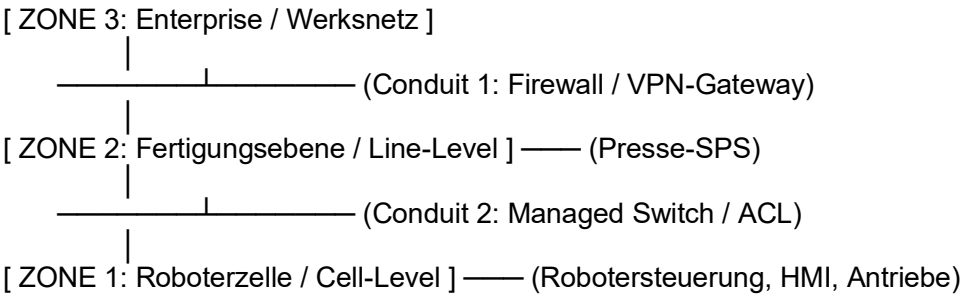
Dieses Dokument verbleibt in Ihren internen CE-Unterlagen. Sie müssen es nicht proaktiv an Kunden herausgeben, aber es dient als **wichtigster Schutzschild bei einer Überprüfung durch das BSI oder die Marktüberwachung**, um zu beweisen, dass Sie die Cybersicherheit Ihrer Anlage professionell analysiert haben.

5.1 Definition der genauen Netzwerk-Zonen (Zonierung nach IEC 62443) für die Roboterzelle

Hier ist die detaillierte Dokumentation für die technische Akte, aufgeteilt in die Netzwerk-Zonierung nach der Industrienorm **IEC 62443** und das konkrete Sicherheitskonzept für das **HMI-Bedienpanel**.

5.1.1 Teil 1: Netzwerk-Zonierung für die Roboterzelle (nach IEC 62443-3-3)

Nach IEC 62443 wird ein industrielles Netzwerk in logische **Zonen** (Bereiche mit gleichen Sicherheitsanforderungen) unterteilt. Die Verbindungen zwischen den Zonen heißen **Conduits** (Leitungen/Kanäle), an denen Firewalls oder Filter sitzen.
Für Ihre Roboterzelle an der Presse definieren wir **drei Zonen**:



1. Zone 1: Cell-Level (Die gesperrte Roboterzelle)

- **Beschreibung:** Das innerste Netzwerk direkt an der Hardware. Hier kommunizieren die Geräte, die für den reinen Ablauf des Transfers zuständig sind.
- **Enthaltene Assets:** Robotersteuerung, HMI-Bedienpanel, E/A-Module, Antriebsregler.
- **Schutzbedarf (Security Level):** SL 2 bis SL 3 (Schutz gegen gezielte Manipulation).
- **Regel:** Geräte in dieser Zone dürfen **keinen** direkten Zugriff auf das Internet oder das übergeordnete Werksnetzwerk haben.

2. Zone 2: Line-Level (Die Fertigungslinie)

- **Beschreibung:** Die Zone, in der die Roboterzelle mit der Presse gekoppelt ist.
- **Enthaltene Assets:** Presse-SPS, übergeordnetes Linien-HMI, Leitrechner (SCADA).
- **Schutzbedarf:** SL 2.
- **Kommunikation:** Über PROFINET oder standardisierte E/A-Signale zur Freigabe des Transfers.

3. Zone 3: Enterprise-Level (Das Werksnetzwerk)

- **Beschreibung:** Das Office- oder Produktionsnetzwerk des Kunden (MES/ERP-Anbindung). Hier herrscht das größte Risiko für IT-Vorfälle (z. B. Office-Viren).

Die Conduits (Übergänge) und Filterregeln

- **Conduit 1 (Werksnetz ➔ Fertigungsebene):** Ein industrieller VPN-Router (z. B. Siemens Scalance oder mGuard) trennt das Werksnetz. Fernwartung ist standardmäßig **deaktiviert** und wird nur per Schlüsselschalter an der Anlage für IP-Adresse X temporär freigeschaltet.
- **Conduit 2 (Fertigungsebene ➔ Roboterzelle):** Ein *Managed Switch* blockiert alle Protokolle außer den zwingend notwendigen Daten für die Presse (z. B. nur Port 502 für Modbus oder dedizierte PROFINET-Pakete). HTTP, FTP oder unverschlüsseltes Telnet zur Robotersteuerung werden an diesem Übergang komplett blockiert.

5.1.2 Teil 2: Detail-Sicherheitskonzept für das HMI-Bedienpanel

Das HMI (Human Machine Interface) ist die größte physische und digitale Angriffsfläche direkt an der Maschine. Ein Angriffsvektor wäre ein unbefugter Mitarbeiter oder ein infizierter USB-Stick.

1. Physische Härtung & Schnittstellen-Schutz

- **USB-Ports:** Alle physischen USB-Schnittstellen am Gehäuse des HMI-Panels werden dauerhaft mechanisch blockiert (z. B. durch abschließbare USB-Sperren) oder im BIOS/Betriebssystem (Windows IoT / Linux) softwareseitig deaktiviert. *Ausnahme:* Ein interner Port für die Projektsicherung, der nur im verschlossenen Schaltschrank zugänglich ist.
- **Zugriff auf das Betriebssystem:** Die "Kiosk-Mode"-Funktion ist aktiv. Nach dem Hochfahren startet ausschließlich die Visualisierungs-Applikation. Tastaturkommandos (wie Alt+F4, Strg+Alt+Entf oder Windows-Taste) sind gesperrt, um den Zugriff auf den Desktop oder die Eingabeaufforderung zu verhindern.

2. Authentifizierung & Rollenkonzept (RBAC)

Es gibt keine anonyme Bedienung der Anlage. Die Anmeldung erfolgt über ein rollenbasiertes System (Role-Based Access Control) – entweder per Passworteingabe oder via RFID/RFID-Chip (z. B. EUCHNER EKS):

- **Rolle: Operator (Bediener):** Darf die Anlage starten, stoppen und Fehlermeldungen quittieren. Keine Änderung von Parametern oder Transferzeiten. (Kein Passwort oder RFID-Standardchip).
- **Rolle: Maintainer (Instandhalter):** Darf Schrittketten manuell steuern, Geschwindigkeiten anpassen und Achsen teachen. (Passwortpflicht, automatischer Logout nach 10 Minuten Inaktivität).
- **Rolle: Administrator (Integrator/Hersteller):** Vollzugriff auf Netzwerkeinstellungen, Firmware-Updates und Benutzerverwaltung. (Starkes, individuelles Einmal-Kennwort).

3. Software-Integrität & Update-Prozess

- **Verschlüsselung:** Gespeicherte Passwörter oder Rezeptdaten auf dem HMI werden verschlüsselt abgelegt. Die Kommunikation zwischen HMI und SPS erfolgt verschlüsselt (z. B. über OPC UA mit aktivierten Zertifikaten und SignAndEncrypt).
- **Sicheres Update:** Firmware- und Projektupdates für das HMI dürfen nur über eine kryptografisch signierte Datei eingespielt werden. Das HMI verweigert die Installation, wenn die Signatur des Herstellers fehlt.

5.1.3 Einbindung in die CE-Dokumentation

Sie fügen diese beiden Abschnitte als Anhänge zu Ihrer **Risikoanalyse** hinzu. Bei einer CRA-Prüfung beweisen Sie damit Folgendes:

1. Sie verhindern durch die **IEC 62443 Zonierung**, dass ein infizierter Office-PC die Roboterzelle lahmlegt.
2. Sie verhindern durch das **HMI-Konzept**, dass Schadsoftware per USB eingebracht wird oder Fehlbedienungen zu Unfällen an der Presse führen.

6. Praxisorientierte Inbetriebnahme-Checkliste für die IT-Sicherheit

Nachfolgend ist eine praxisorientierte **Inbetriebnahme-Checkliste für die IT-Sicherheit** dargestellt.
Mit dieser Liste können Ihre Techniker direkt an der Presse vor Ort dokumentieren, dass alle Anforderungen des Cyber Resilience Acts (CRA) und der IEC 62443 im realen System scharf geschaltet sind. Die ausgefüllte und unterschriebene Liste wandert als Nachweis in Ihre technische Projektakte.

Inbetriebnahme-Checkliste: IT-Sicherheit & Cyberresilienz

Anlagen-ID / Projektnummer: _____

Kunde / Standort: _____

Datum der Prüfung: 27. August 2026

Prüfender Techniker (Name): _____

---

1. Physische Sicherheit & Schnittstellen (HMI & Schaltschrank)

- **HMI-Kiosk-Modus aktiv:** Nach dem Einschalten startet nur die Visualisierung. Der Zugriff auf das Betriebssystem (Windows/Linux) über Tastenkombinationen ist unmöglich.
- **USB-Sperren geprüft:** Alle außenliegenden USB-Ports am HMI und am Schaltschrank sind physisch blockiert oder im BIOS nachweislich deaktiviert.
- **Schaltschrank-Zugriff:** Der Schaltschrank, in dem die SPS und der Haupt-Switch sitzen, ist verschlossen. Der Schlüssel wird nur an autorisiertes Personal übergeben.

2. Netzwerksicherheit & Segmentierung (IEC 62443 Zonierung)

- **Zonentrennung aktiv:** Der Roboter und die Presse-SPS befinden sich im zugewiesenen VLAN (Zone 1/2) und sind nicht direkt aus dem Kunden-Büro-Netzwerk (Zone 3) pingbar.
- **Ungenutzte Ports abgeschaltet:** Am Managed Switch in der Roboterzelle sind alle Ports, an denen kein Kabel steckt, softwareseitig deaktiviert (*Port Disabling*).
- **Protokoll-Filterung:** Die Firewall lässt ausschließlich die definierten Kommunikationsports (z.B. PROFINET, OPC UA) durch. Unverschlüsselte Dienste wie HTTP oder Telnet sind gesperrt.

3. Zugriffskontrolle & Passwörter (RBAC)

- **Keine Standard-Passwörter:** Alle herstellerseitigen Standard-Logins (z.B. admin / admin oder 1234) bei der Robotersteuerung, der SPS, dem HMI und dem Router wurden geändert.
- **RFID / Passwort-Rollen getestet:** Der Login für Bediener, Instandhalter und Administrator wurde erfolgreich mit den jeweiligen Berechtigungen getestet.
- **Automatischer Logout:** Das HMI loggt den Benutzer nach maximal 10 Minuten Inaktivität automatisch aus (Zurücksetzen auf Bediener-Ebene).

4. Fernwartung & Notfall-Prozedere

- **Schlüsselschalter-Funktion:** Der physische Schlüsselschalter an der Bedienfront trennt/verbindet die VPN-Verbindung des Fernwartungsrouters zuverlässig. Der VPN-Tunnel steht *nur*, wenn der Schlüssel gedreht ist.
- **Meldeweg-Test:** Dem Kunden wurde das Übergabe-Dokument mit der Kontaktadresse für Sicherheitsupdates und dem Prozess zur Meldung von Schwachstellen ausgehändigt.
- **Backup erstellt:** Ein vollständiges, sauberes Image des HMI-Panels und der SPS-Steuerung wurde im Zustand der Auslieferung erstellt und sicher auf dem Firmen-Server hinterlegt.

Bestätigung des Technikers:
Hiermit wird bestätigt, dass alle oben genannten Sicherheitsfunktionen erfolgreich getestet wurden und die Anlage im cyberresistenten Zustand an den Betreiber übergeben wurde.

Unterschrift Techniker: _____

6.1 Was passiert nach der Inbetriebnahme?

Mit der Checkliste ist der CE-Prozess für die *Auslieferung* abgeschlossen. Da der CRA jedoch ein **Lebenszyklus-Gesetz** ist, läuft ab jetzt im Hintergrund Ihr automatisiertes Schwachstellen-Monitoring (z. B. via *Dependency-Track*), um die Anlage über die nächsten Jahre hinweg abzusichern.

7. Vergleich mit einer Roboteranlage zum Materialtransport in der Lebensmittelherstellung

Was ändert sich an der Dokumentation, wenn die Roboteranlage anstatt mit einer Presse zur Metallverarbeitung zum Materialtransport in der Lebensmittelherstellung z.B. Pizza-Herstellung genutzt wird?

Der Wechsel von der Metallverarbeitung zur **Lebensmittelherstellung (z. B. Pizza-Produktion)** ändert zwar grundlegend die mechanischen Anforderungen (Hygienic Design, Edelstahl, Washdown), an der **grundlegenden IT-Sicherheitsarchitektur nach dem Cyber Resilience Act (CRA) ändert sich jedoch überraschend wenig**.

Allerdings verschieben sich im Detail die **Risikobewertungen**, die **Klassifizierung** und einige **technische Prioritäten** massiv.

7.1 Direkter Vergleich und die Anpassung für eine Pizza-Transportanlage

7.2 Die CRA-Klassifizierung:

Bleibt die Klasse I ?

Ja, aber mit anderer Begründung.

- Eine Roboteranlage zum Materialtransport (z. B. Teiglinge auflegen, Zutaten dosieren oder verpackte Pizzen palettieren) gilt auch hier als **Industrial Automation Control System (IACS)** und fällt damit in die **Klasse I (Wichtige Produkte)**.
- **Der Unterschied zur Presse:** Bei der Presse droht bei einem Hack sofort **physische Lebensgefahr** (Quetschen, Hebeln). Bei der Pizzaherstellung droht bei einem Hack primär **Sabotage der Lieferkette** (Produktionsstillstand in einer hochgradig zeitkritischen Frische-Produktion) oder **Verunreinigung** (z. B. durch bewusste Manipulation von Kühltemperaturen oder Backzeiten im gekoppelten Ofen).

7.3 Das angepasste IT-Sicherheitskonzept (Die Unterschiede in der Praxis)

Während bei der Metallpresse die mechanische Sicherheit (Interlocking) im Vordergrund stand, liegt der Fokus in der Lebensmittelindustrie auf **Prozessintegrität** und **Hygiene-Sicherheitsfunktionen**.

A. Risikoanalyse: Neue Bedrohungsszenarien

In Ihrer technischen Dokumentation müssen Sie für die Lebensmittelbranche folgende spezifische Risiken bewerten:

- **Rezeptur-Sabotage:** Angreifer verändern über das HMI oder die SPS die Dosierung von Zutaten oder Allergenen.
- **Manipulation von Reinigungsprozessen (CIP - Cleaning in Place):** Wenn der Transportroboter mit Wasser/Chemie gereinigt werden muss, steuert die SPS oft die Reinigungszyklen. Ein Hack könnte dazu führen, dass Reinigungsmittel nicht richtig ausgespült werden (Vergiftungsgefahr).
- **Manipulierte Track & Trace-Daten:** In der Lebensmittelbranche ist die Rückverfolgbarkeit gesetzlich vorgeschrieben. Ein Cyberangriff, der die Chargennummern im System (MES/SPS) löscht oder verändert, macht die gesamte Tagesproduktion unverkäuflich.

B. Das HMI-Bedienpanel: Physische Härtung im "Washdown"-Bereich

Das HMI-Konzept von der Presse muss für die Lebensmittelindustrie mechanisch und digital angepasst werden:

- **Keine USB-Sperren aus Plastik:** Da die Anlage oft mit Hochdruckreinigern und aggressiven Desinfektionsmitteln gereinigt wird, müssen alle Ports hinter einer **Edelstahl-Abdeckung mit IP69K-Dichtung** liegen.
- **RFID statt Passwörter (Hygienischer Standard):** Passworteingaben über Touchscreens sind in der Lebensmittelproduktion mit Handschuhen oft unpraktisch. Hier setzt man fast ausschließlich auf **wasserfeste RFID-Schlüssel** (z. B. EUCHNER EKS im Hygienic Design). Die dokumentierte Rollenverteilung (Bediener vs. Reinigungspersonal vs. Techniker) bleibt exakt gleich streng wie bei der Presse.

C. Netzwerk-Zonierung (IEC 62443): Höhere Konnektivität

In modernen Lebensmittelbetrieben sind Roboteranlagen meist viel stärker vernetzt als in alten Presswerken:

- Die Roboterzelle muss Daten an das **MES (Manufacturing Execution System)** senden, um Rezepte (z. B. "Pizza Salami" vs. "Pizza Margherita") live zu empfangen.
- **Konsequenz für das Conduit (Übergang):** Der Datenkanal zwischen der Roboterzelle (Zone 1) und dem Werksnetz (Zone 3) muss über ein verschlüsseltes Protokoll wie **OPC UA mit TLS-Verschlüsselung** laufen. Einfache, unverschlüsselte Modbus-Verbindungen sind hier wegen des Manipulationsrisikos der Rezepturen nicht mehr CRA-konform.

7.4 Summary: Was müssen Sie für die Pizza-Anlage neu schreiben?

80 % der Dokumente (Vertragsklauseln für Zulieferer, die SBOM-Struktur mit CycloneDX und die 24-Stunden-Meldepflicht) eins zu eins von der Presse können übernommen werden.

Sie müssen lediglich **20 % in Ihrer technischen Dokumentation anpassen**:

1. In der **Risikoanalyse** tauschen Sie die Bedrohung "Mechanische Quetschung an der Presse" gegen "Manipulation von Rezepturen / Reinigungsprozessen / Chargendaten".
2. In der **Inbetriebnahme-Checkliste** ergänzen Sie die Prüfung der IP69K-Schnittstellenabdeckungen und den sicheren Datenempfang vom Rezeptur-Server des Kunden.

Damit ist die Cyberresilienz-Strategie flexibel genug, um sie auf jede beliebige Industrie-Anlage zu übertragen.

Nachfolgend ist ein konkretes Praxis-Szenario dargestellt für die Pizza-Anlage und die dazugehörige Dokumentation für Ihre IT-Risikoanalyse nach **IEC 62443** und **CRA**.

7.5 Teil 1: Das konkrete Praxis-Beispiel (Das Szenario)

Der Ablauf in der Produktion:

Ihre Roboteranlage transportiert Teiglinge auf ein Band und dosiert über ein gekoppeltes Ventil die Tomatensauce für die Pizzen. Das Werk produziert im Minutentakt abwechselnd *Pizza Margherita* und *Pizza Tonno* (Thunfisch).

Die digitale Schnittstelle:

Die Anlage ist über **OPC UA** mit dem übergeordneten Rezeptur-Server (MES) der Großbäckerei verbunden. Wenn eine Charge gewechselt wird, sendet der Server den Befehl:

- *„Rezept ID 42 (Margherita): Dosierung 50ml Sauce, Robotergeschwindigkeit 80 %“*.

Die Gefahr bei einem Hack:

Ein Angreifer dringt in das Werksnetzwerk ein. Er fängt die OPC-UA-Daten ab und manipuliert sie (*Man-in-the-Middle-Angriff*) oder sendet gefälschte Befehle an Ihre Anlagen-SPS. Er ändert das Rezept unbemerkt so, dass die Sauce komplett abgeschaltet wird oder falsche Allergen-Daten (z.B. Thunfisch-Rückstände auf einer vegetarischen Pizza) im System protokolliert werden. Dies führt zu einem massiven Schaden, Produktionsstopp oder Rückrufaktionen.

DIPL. -ING. C. SPREUER | Emser Straße 19 | 65195 Wiesbaden | Tel. (0611) 59 99 33 | E-Mail: info@spreuer.com | Page: www.spreuer.com

7.6 Teil 2: Dokumentation der OPC-UA-Übertragung in der Risikoanalyse

Dieses Textmodul fügen Sie direkt in die **Technische Dokumentation (IT-Risikobewertung)** Ihrer Lebensmittel-Anlage ein, um die Anforderungen des Cyber Resilience Acts zu erfüllen.
Ausschnitt aus der Risikoanalyse: Schnittstelle MES-Anbindung (OPC UA)

Schnittstellen-Beschreibung:

Eingehende Ethernet-Verbindung von Zone 3 (Werksnetz / MES) zu Zone 2 (Anlagen-SPS) via OPC UA zur automatischen Rezeptur- und Chargenübergabe.

Bedrohung: Manipulation von Rezepturdaten durch unbefugte OPC-UA-Zugriffe

- **Beschreibung:** Ein Angreifer im Werksnetzwerk sendet manipulierte Rezepturwerte (z. B. falsche Dosierungsdaten oder veränderte Geschwindigkeiten) an die SPS der Transportanlage, um Ausschuss zu erzeugen oder den Prozess zu sabotieren.
- **Anfängliches Risiko (Ohne Schutzmaßnahmen):**
  - *Eintrittswahrscheinlichkeit:* 4 (Hoch, da das Werksnetzwerk mit dem Internet/Office verbunden ist)
  - *Auswirkung:* 4 (Schwerer Schaden: Produktionsausfall, Chargen-Verunreinigung)
  - **Risikowert: 16 (Kritisch – Maßnahmen zwingend erforderlich)**
- **Kompensierende Maßnahmen (Technische Umsetzung an der Anlage):**

1. **Kryptografische Absicherung (Verschlüsselung):** Die OPC-UA-Kommunikation wird zwingend mit dem Profil Basic256Sha256 und dem Modus SignAndEncrypt verschlüsselt. Unverschlüsselte Verbindungen (None) werden von der SPS strikt abgewiesen.

2. **Zertifikatsbasierte Authentifizierung:** Der Zugriff auf den OPC-UA-Server der SPS ist nur mit einem gültigen, vom Betreiber signierten X.509-Sicherheitszertifikat möglich. Unbekannte Clients werden blockiert.

3. **Plausibilitätsprüfung in der SPS (Daten-Härtung):** Die empfangenen Rezepturdaten werden in der SPS-Logik vor der Freigabe auf physikalische Grenzwerte geprüft (z. B. *„Wenn Dosierung > 100ml oder < 10ml ➔ Fehlermeldung und Stopp“*). Ein Überfluten mit Extremwerten wird so verhindert.

4. **Netzwerk-Kapselung:** Der OPC-UA-Port (Standard: 4840) wird in der vorgeschalteten Firewall (Conduit) explizit nur für die IP-Adresse des spezifischen MES-Rezeptur-Servers freigegeben.

- **Restrisiko (Nach Umsetzung der Maßnahmen):**
  - *Eintrittswahrscheinlichkeit:* 1 (Sehr gering, da Angreifer Verschlüsselung und Zertifikate brechen müssten)
  - *Auswirkung:* 2 (Gering, da die SPS utopische Werte abfängt und kontrolliert stoppt)
  - **Risikowert: 2 (Akzeptabel / CRA-konform)**

7.7 Der Vorteil dieser Dokumentation im CE-Prozess:

Wenn Sie diese Analyse in Ihren Unterlagen haben, beweisen Sie der Marktüberwachung (BSI), dass Sie das Risiko der **digitalen Produktpiraterie und Sabotage** erkannt und durch moderne IT-Standards gelöst haben. Sie erfüllen damit die CRA-Forderung nach *"Sicherheit über den gesamten Lebenszyklus und Schutz vor unbefugter Datenmanipulation"*.

Wiesbaden, den 10.08.2026

C. Spreuer – Dipl. Ing. Verfahrenstechnik, Anlagen- und Arbeitssicherheit

DIPL. -ING. C. SPREUER | Emser Straße 19 | 65195 Wiesbaden | Tel. (0611) 59 99 33 | E-Mail: info@spreuer.com | Page: www.spreuer.com