Umsetzung der EN ISO 11161:2010 in der Praxis

- Aufgaben des System Integrators -

Beispiel:

Errichtung einer Roboter-Transferanlage zur Pressenautomation unter Einbeziehung der ab 2027 geltenden EU-Maschinenverordnung (MVO)



Christoph Spreuer

AUTOR: CHRISTOPH SPREUER | DIPL:- VERFAHRENS- UND SICHERHEITSINGENIEUR |
Emser Straße 19 | Wiesbaden | Tel. (0611) 59 99 33 | E-Mail: info@spreuer.com | Page: www.spreuer.com

Inhaltsverzeichnis

Vorwort 4
1 Mustervertrag 4
1.1 Struktur des Vertrages 4
1.2 Wichtige Praxishinweise für den Abschluss 5
2. Beispiel für einen Vertragsentwurf für eine Roboter-Transferanlage 5
2.1 ANLAGENBAU- UND INTEGRATIONSVERTRAG 5
2.2 Vertragsklauseln: Wiederkehrende Software-Updates 6
2.2.1 ZUSATZVEREINBARUNG: SOFTWARE-UPDATES UND CYBERSECURITY 6
3 Beispiel - Erstellung eines übergeordneten Sicherheitskonzeptes 8
3.1 Der Ablauf in der Praxis (Methodik) 8
3.1.1 Praxis-Beispiel: Schnittstellen-Risikobeurteilung 8
3.1.2 System-Beschreibung der Schnittstelle 8
3.2 Schnittstellen-Bereich: Der Werkzeugraum der Presse (Eingriffszone) 9
3.3 Was der Integrator zusätzlich dokumentieren muss 9
3.3.1 Praxiserprobte E/A-Liste für die Roboter-Transferanlage: 10
3.3.2 Sicherheitsgerichtete Signale (Failsafe-Signale, PLd / PLe) 10
3.3.3 Betriebsmäßige Signale (Standard-Ablaufsteuerung) 11
3.3.4 Wichtiger Hinweis für die Programmierung (Interlock) 11
4 Logisches Ablaufdiagramm für einen kompletten Zyklus 12
4.1 Logischer Zyklus: Pressenautomation (Vom Einlegen bis zum Hub) 12
4.1.1 Detaillierte Schritt-für-Schritt-Beschreibung 12
4.2 Was passiert bei einer Störung? (Sicherheitsgerichtetes Verhalten) 14
5 Erweitertes Sicherheitskonzept zur Integration der Cybersecurity 14
5.1 Einfluss der EU-Maschinenverordnung auf die Arbeit des Integrators 14
5.1.1 MVO vs. BMAS-Interpretationspapier „Komplexe Anlagen“ 14
5.1.2 Was sich durch die MVO ändert: 14
5.2 Was bedeutet die Einbeziehung der „digitalen Verknüpfung“ genau? 15
5.2.1 Software ist ein eigenständiges Sicherheitsbauteil [1, 2] 15
5.2.2 Schutz vor Korrumpierung und Manipulation (Annex III, 1.1.9 & 1.2.1) [1] 15
5.2.3 Wesentliche Veränderung durch Software-Updates [1] 15
5.3 Zusammenfassung für Ihre Risikoanalyse 16
5.4 Erweiterung der Schnittstellen-Risikobeurteilung um Cyber-Risiken 16
5.5 Was Integratoren nun zusätzlich dokumentieren müssen 18

6 Schaltplandarstellung der Signale 18
6.1 Schaltungstechnische Umsetzung und die Darstellung der Signale im Schaltplan (E-Plan) für Ihre integrierte Roboter-Transferanlage. 18
6.2 Prinzipschaltbild: Einbindung der Sicherheits-SPS (F-CPU) 19
6.3 Schaltplan-Auszug: Zweikanalige Querschlusserkennung 20
6.4 Schaltungstechnische Integration der Cybersecurity (MVO 2023/1230) 21
6.5 Standard-E/A (Kollisionsschutz) im Schaltplan 21
6.6 Wie diese Signale im E-Plan dokumentiert werden sollten 22
6.6.1 Konkretes SPS-Code-Beispiel für die logische Verknüpfung der Signale 22
6.6.2 Fehlersicherer Code (F-Programm in FUP) 22
6.6.3 Betriebsmäßiger Code (Standard-Programm in SCL) 23
7. Besonderheiten dieser Software-Architektur nach EN ISO 11161: 25
8 VALIDIERUNGS-CHECKLISTE: SOFTWARE & DIGITALE VERKNÜPFUNG 26
9 BETREIBER-ANWEISUNGEN: DIGITALE SICHERHEIT & CYBERSECURITY 29

Vorwort

Die internationale Norm EN ISO 11161:2010 für Integrierte Fertigungssysteme, legt einen Integrator als natürliche Person fest. Nachfolgend wird zunächst die Struktur eines Vertrages des Integrators (Hersteller einer Roboteranlage) mit einem Auftraggeber für die Errichtung eines Integrierten Fertigungssystems beschrieben.

1 Mustervertrag

Ein Vertrag mit einem Integrator (als natürlicher Person nach **EN ISO 11161:2010**) unterscheidet sich von klassischen Lieferverträgen vor allem dadurch, dass

- **die Gesamtverantwortung für die sicherheitstechnische Verknüpfung**

und

- **die rechtliche Herstellerverantwortung (inklusive CE-Kennzeichnung des Gesamtsystems)**

explizit einer Person zugewiesen werden.

1.1 Struktur des Vertrages

Der Vertrag gliedert sich in folgende wesentliche Kernbereiche:

- **Präambel & Status**: Definition des Integrators als verantwortlicher Gesamt-Hersteller für das Integrierte Fertigungssystem (IMS) im Sinne der EN ISO 11161.
- **§ 1 & § 2 Leistungsumfang & Sicherheitskonzept**: Zuweisung der Pflicht zur Durchführung der Schnittstellen-Risikobeurteilung nach EN ISO 12100 / EN ISO 11161, Verknüpfung der Sicherheitsfunktionen (z. B. Not-Halt) und Ausstellung der CE-Konformitätserklärung.
- **§ 3 Mitwirkungspflichten des Auftraggebers**: Wichtig bei der Integration, da der Auftraggeber oft Einzelmaschinen, Einbauerklärungen oder Dokumentationen beistellen muss.
- **§ 4 bis § 6 Wirtschaftliche & Organisatorische Abwicklung**: Meilensteinbasierter Zahlungsplan, Projekttermine sowie Kriterien für die formelle Systemabnahme nach erfolgreichem Testlauf (SAT).
- **§ 7 & § 8 Haftung & Versicherungsschutz**: Absicherung der Parteien sowie Verpflichtung des Integrators zur Aufrechterhaltung einer ausreichenden Betriebshaftpflichtversicherung.

1.2 Wichtige Praxishinweise für den Abschluss

- **Schnittstellen klar definieren**: Da der Integrator für das *Gesamtsystem* haftet, muss im Lastenheft exakt stehen, wo die Verantwortung fremder Zulieferer aufhört und die des Integrators beginnt.
- **Dokumentenprüfung sichern**: Verpflichten Sie den Auftraggeber vertraglich dazu, vollständige und normgerechte Dokumente für beigestellte Maschinen zu liefern, da der Integrator sonst die CE-Erklärung für die Gesamtanlage rechtlich nicht finalisieren kann.

2. Beispiel für einen Vertragsentwurf für eine Roboter-Transferanlage

2.1 ANLAGENBAU- UND INTEGRATIONSVERTRAG

Für die Errichtung einer Roboter-Transferanlage zur Pressenautomation

Zwischen

[Name des Auftraggebers]
– nachfolgend „Auftraggeber“ genannt –

und

[Name des Integrators, natürliche Person]
– nachfolgend „Integrator“ genannt –
(Verantwortlicher Integrator im Sinne der EN ISO 11161:2010)

Präambel

Der Auftraggeber beabsichtigt, in seinem Werk am Standort [Ort] eine automatisierte Roboter-Transferanlage zur Verkettung von Umformpressen (Pressenautomation) in der Metallverarbeitung zu errichten. Die Anlage qualifiziert sich als Integriertes Fertigungssystem (IMS) nach EN ISO 11161:2010. Der Integrator übernimmt als natürliche Person die Gesamtverantwortung für die sicherheitstechnische Verknüpfung der Einzelkomponenten sowie die Funktion als rechtlicher Hersteller des Gesamtsystems.

§ 1 Vertragsgegenstand und Leistungsumfang

1. Der Integrator verpflichtet sich zur Planung, softwareseitigen und steuerungstechnischen Integration, Montageleitung, Inbetriebnahme und CE-Zertifizierung einer Roboter-Transferanlage zur Handhabung von Blechbauteilen zwischen den Pressenstufen [Bezeichnung/Nummer der Pressen].
2. Zum Leistungsumfang gehören insbesondere:
    - Einbindung von [Anzahl] 6-Achs-Industrierobotern inklusive der Greifer Systeme.
    - Integration der Sensorik zur Teile- und Lageerkennung sowie der Schnittstellen zur vorhandenen Pressensteuerung.

- Erstellung des übergeordneten Sicherheitskonzepts (Schnittstellen-Risikobeurteilung) nach EN ISO 11161 und EN ISO 12100.
- Zusammenführung der Sicherheitskreise (Zwei-Hand-Bedienungen, Lichtgitter, Schutztüren, Not-Halt-Ketten) zu einem validierten Gesamtsystem.

3. Die genauen technischen Spezifikationen ergeben sich aus dem Lastenheft des Auftraggebers (Anlage 1) und dem Pflichtenheft des Integrators (Anlage 2).

§ 2 Konformitätsbewertung und CE-Kennzeichnung

1. Der Integrator trägt die Verantwortung dafür, dass die Gesamtanlage den Anforderungen der Maschinenrichtlinie (bzw. der gültigen EU-Maschinenverordnung) entspricht.
2. Der Integrator führt das Konformitätsbewertungsverfahren durch, stellt die EG-Konformitätserklärung für das IMS aus und bringt das CE-Kennzeichen an der Anlage an.
3. Voraussetzung hierfür ist, dass der Auftraggeber für alle beigestellten Maschinen (z. B. Bestands-Pressen) gültige CE-Erklärungen oder Einbauerklärungen inkl. Montageanleitungen rechtzeitig bereitstellt.

§ 3 Abnahme und Funktionstest (SAT)

1. Nach der mechanischen und elektrischen Installation führt der Integrator einen Site Acceptance Test (SAT) im Werk des Auftraggebers durch.
2. Der SAT gilt als erfolgreich, wenn die Transferanlage die im Pflichtenheft definierten Taktzeiten und Qualitätskriterien im Automatikbetrieb über einen Zeitraum von [Anzahl] Stunden kontinuierlich und fehlerfrei erreicht.
3. Über die erfolgreiche Abnahme ist ein von beiden Parteien zu unterzeichnendes Protokoll zu erstellen. Mit der Unterzeichnung geht die Gefahr auf den Auftraggeber über.

2.2 Vertragsklauseln: Wiederkehrende Software-Updates

2.2.1 ZUSATZVEREINBARUNG: SOFTWARE-UPDATES UND CYBERSECURITY

als Anlage / Ergänzung zum Integrationsvertrag vom [Datum]

§ 1 Gegenstand der Software-Pflege

1. Der Integrator verpflichtet sich, die Steuerungs- und Robotersoftware der integrierten Transferanlage für eine Laufzeit von [Anzahl, z.B. 3] Jahren ab Abnahme auf dem aktuellen Stand der Technik zu halten.
2. Die Leistungen umfassen:
   - **Patches & Bugfixes:** Behebung von Softwarefehlern und Stabilitätsoptimierungen.

- **Sicherheits-Updates:** Schließen von neu bekannt gewordenen IT-Sicherheitslücken zur Gewährleistung der Netzsicherheit (Cybersecurity nach IEC 62443 / EN ISO 11161).
- **Kompatibilitäts-Updates:** Anpassungen an aktualisierte Firmware-Versionen der Roboter- und SPS-Hersteller, sofern diese für den sicheren Betrieb zwingend erforderlich sind.

§ 2 Durchführung von Updates und Stillstandszeiten

1. Der Integrator wird Updates vorab in einer Simulationsumgebung prüfen, um negative Auswirkungen auf den Produktionsprozess zu minimieren.
2. Die Einspielung von Updates vor Ort oder via Fernzugriff (Remote) erfolgt ausschließlich nach vorheriger schriftlicher Freigabe durch den Auftraggeber und außerhalb der regulären Produktionszeiten (z. B. an Wochenenden oder während geplanter Wartungsfenster).
3. Durch Updates verursachte geplante Stillstandszeiten sind mindestens [Anzahl, z.B. 14] Tage im Voraus anzukündigen.

§ 3 Gewährleistung und Validierung nach Updates

1. Der Integrator garantiert, dass durch das Einspielen von Updates die funktionalen Sicherheitsfunktionen (Safety) der Gesamtanlage gemäß EN ISO 11161 nicht beeinträchtigt werden.
2. Nach jedem wesentlichen Software-Update ist eine funktionale Teil-Validierung der Sicherheitskreise durchzuführen und zu protokollieren.
3. Führt ein Software-Update zu einer wesentlichen Veränderung der Anlage im rechtlichen Sinne, ist der Integrator verpflichtet, die Risikobeurteilung entsprechend zu aktualisieren.

§ 4 Vergütung

Die Vergütung für die wiederkehrenden Software-Updates erfolgt:

- [ ] Pauschal als jährliche Festgebühr in Höhe von [Betrag] EUR.
- [ ] Nach tatsächlichem Aufwand gemäß den Stundensätzen des Integrators nach Anlage [X].

Weitere Regelungen sollten **spezifische Gewährleistungsfristen** für die Metallbearbeitung (z.B. Verschleiß durch Zunder/Emulsion) enthalten und die **Bedingungen für den Fernzugriff** (Remote Access) genauer definieren.

3 Beispiel - Erstellung eines übergeordneten Sicherheitskonzeptes

Das übergeordnete Sicherheitskonzept und die **Schnittstellen-Risikobeurteilung** sind das Herzstück der Arbeit eines Integrators. Wenn Einzelmaschinen (z. B. eine Presse und ein Industrieroboter), die für sich genommen sicher sind, zu einem **Integrierten Fertigungssystem (IMS)** verkettet werden, entstehen an den Übergängen neue, oft lebensgefährliche Risiken [Anlage]. [1]

Die **EN ISO 11161** verlangt, dass der Integrator genau diese Wechselwirkungen untersucht, während die **EN ISO 12100** das methodische Werkzeug (Risikominderung in 3 Schritten) dafür liefert [Anlage]. [1, 2]

3.1 Der Ablauf in der Praxis (Methodik)

- **Grenzen des IMS festlegen:** Räumliche Grenzen (Schutzzäune) und zeitliche/funktionale Abläufe (Wann greift der Roboter in die Presse?).
- **Gefährdungsidentifikation an den Schnittstellen:** Was passiert beim Quertransport? Welche Signalfehler können auftreten?
- **Risikoabschätzung & Bewertung:** Wie schwer wäre eine Verletzung? Wie oft hält sich jemand dort auf?
- **Risikominderung (3-Stufen-Methode nach EN ISO 12100):**
  - *Stufe 1:* Konstruktive Sicherheit (z. B. Abstände so wählen, dass Quetschstellen gar nicht erst entstehen).
  - *Stufe 2:* Technische Schutzmaßnahmen (z. B. Lichtgitter, Verriegelungen) [Anlage].
  - *Stufe 3:* Benutzerinformationen (z. B. Warnhinweise, Schulungen). [1]

3.1.1 Praxis-Beispiel: Schnittstellen-Risikobeurteilung

Hier ist ein konkretes, tabellarisches Beispiel für eine Schnittstelle bei der oben genannten **Pressenautomation (Metallverarbeitung)**.

3.1.2 System-Beschreibung der Schnittstelle

- **Komponente A:** Exzenterpresse zum Stanzen von Blechteilen (Bestandsmaschine).
- **Komponente B:** 6-Achs-Transferroboter mit Magnetgreifer (Neuanlage).

3.2 Schnittstellen-Bereich: Der Werkzeugraum der Presse (Eingriffszone)

Schritt / Lebensphase	Identifizierte Gefahr (EN ISO 12100)	Ursache / Wechselwirkung (EN ISO 11161)	Risikobewertung (ohne Maßnahme)	Technische Schutzmaßnahme (PL nach EN ISO 13849-1)	Restrisiko & Info
Automatikbetrieb (Bestückung)	**Quetschen / Scheren** von Gliedmaßen im Werkzeugraum.	Roboter fährt in die Presse ein, während der Pressenstößel ungewollt nach unten fährt (Synchronisationsfehler).	**Hoch** (Lebensgefahr / schwere Amputation)	**Zweikanalige Verriegelung** der Steuerungen via Sicherheits-SPS (F-CPU). Der Roboter erhält die Freigabe zur Einfahrt nur, wenn die Presse sicher im Oberen Totpunkt (OT) steht und mechanisch/hydraulisch blockiert ist (**Performance Level d / PLd**).	**Akzeptabel.** Schulung des Wartungspersonals auf Schutzeinrichtungen zwingend erforderlich.
Einrichtbetrieb / Teachen	**Anfahren / Quetschen** des Bedieners durch den Roboter.	Bediener muss zum Teachen der Greifpunkte in den Gefahrenbereich der geöffneten Presse steigen.	**Hoch** (Unerwarteter Anlauf des Roboters)	**Zustimmtaster (3-Stellungs-Schalter)** am Roboter-Handbediengerät (Teach Pendant). Bewegung des Roboters ist nur mit reduzierter Geschwindigkeit (< 250 mm/s) und gehaltenem Taster möglich (**PLd**). Zudem wird der Hauptantrieb der Presse in diesem Modus sicher weggeschaltet (**PLe**).	**Akzeptabel.** Verbot des Aufenthalts von Dritten im Schutzzaun während des Teach-Vorgangs.
Störungsbeseitigung (Zunder)	**Verschütten / herabfallende Teile**.	Blechteil löst sich vorzeitig vom Magnetgreifer des Roboters (z. B. durch starken Zunder oder Ölfilm) und trifft Bediener bei der manuellen Reinigung.	**Mittel** (Schnittverletzungen, Prellungen)	**Teileverlust-Sensorik:** Der Roboter überwacht den Luftdruck/Unterdruck bzw. die magnetische Sättigung. Bei Signalverlust schaltet die Anlage sofort auf "Not-Halt" und stoppt alle Bewegungen (**PLc**).	**Gering.** Bediener muss beim Betreten der Anlage schnittfeste PSA (Handschuhe, Sicherheitsschuhe) tragen.

3.3 Was der Integrator zusätzlich dokumentieren muss

Wenn dieses Sicherheitskonzept für die Anlage erstellt wird, muss der Integrator ein **Validierungsprotokoll** anfertigen.

Darin wird nachgewiesen, dass die Sicherheitsketten auch real funktionieren:

- *Testfall:* Sie ziehen im Automatikbetrieb den Stecker der Positionsüberwachung der Presse.

- *Erwartetes Ergebnis:* Der Roboter muss sofort stoppen und darf die Einfahrfreigabe nicht erhalten.
- *Ergebnis:* Bestanden / Nicht bestanden (mit Unterschrift des Integrators).

Für eine sichere und funktionierende Pressenautomation müssen die Signale zwischen der Presse und dem Roboter in **sicherheitsgerichtete Signale** (Failsafe, für den Personenschutz nach EN ISO 13849-1) und **betriebsmäßige Signale** (für den reinen Ablauf) unterteilt werden.
Da der Integrator die Gesamtverantwortung trägt, werden diese Signale idealerweise über einen sicheren Bus (z. B. PROFIsafe oder CIP Safety) oder über eine zweikanalige, potenzialfreie Hardware-Verkabelung zwischen den Sicherheits-SPSen ausgetauscht.

3.3.1 Praxiserprobte E/A-Liste für die Roboter-Transferanlage:

3.3.2 Sicherheitsgerichtete Signale (Failsafe-Signale, PLd / PLe)

Diese Signale dienen ausschließlich dem Schutz von Mensch und Maschine. Fällt eines dieser Signale weg (0-Signal), müssen die Antriebe sofort stoppen oder blockiert werden. [1]

Signalname	Richtung	Typ	Beschreibung / Sicherheitsfunktion
F-Not-Halt Presse an Roboter	Presse → Roboter	digital (2-kanalig)	Not-Halt-Taster der Presse wurde gedrückt. Roboter muss sofort in *Sicheren Stopp* gehen.
F-Not-Halt Roboter an Presse	Roboter → Presse	digital (2-kanalig)	Not-Halt-Taster des Roboters (am Teach Pendant) wurde gedrückt. Presse muss sofort stoppen.
F-Presse in OT sicher	Presse → Roboter	digital (2-kanalig)	Bestätigt, dass der Pressenstößel sicher im Oberen Totpunkt (OT) steht und mechanisch/hydraulisch gegen Absacken gesichert ist. Einzige Bedingung, bei der der Roboter einfahren darf.
F-Roboter in Home sicher	Roboter → Presse	digital (2-kanalig)	Bestätigt, dass sich der Roboter außerhalb des Werkzeugraums der Presse in einer sicheren Parkposition befindet. Nur dann darf die Presse einen Hub starten.
F-Schutzzaun / Lichtgitter OK	IMS → beide	digital (2-kanalig)	Der übergeordnete Schutzkreis des Fertigungssystems ist geschlossen. Bei Unterbrechung stoppen beide Maschinen.

3.3.3 Betriebsmäßige Signale (Standard-Ablaufsteuerung)

Diese Signale regeln den automatischen Produktionsprozess im fehlerfreien Zustand. Sie verhindern Werkzeugschäden (Kollisionsschutz), dienen aber nicht dem direkten Personenschutz.

Signale von der Presse → zum Roboter

Signalname	Datentyp	Beschreibung
Presse im Automatikmodus	BOOL	Presse steht auf Automatik und ist startbereit.
Werkzeug geöffnet	BOOL	Mechanische Rückmeldung, dass das Pressenwerkzeug weit genug offen ist (Zusatzinfo zu "Presse in OT").
Teil fertig / Auswerfer oben	BOOL	Das Blechteil wurde gepresst und durch den Auswerfer für den Roboter zur Entnahme freigegeben.
Anforderung Roboter-Einfahrt	BOOL	Die Presse wartet aktiv auf die Beladung oder Entnahme durch den Roboter.

Signale vom Roboter → zur Presse

Signalname	Datentyp	Beschreibung
Roboter im Automatikmodus	BOOL	Robotersteuerung steht auf Automatik und ist fehlerfrei.
Roboter fährt ein	BOOL	Vorwarnsignal. Der Roboter verlässt seine Warteposition und bewegt sich in den Werkzeugraum.
Teil eingelegt (Beladung fertig)	BOOL	Der Roboter hat das Rohteil im Werkzeug abgelegt und die Magnete/Greifer gelöst.
Startfreigabe Presse (Hub-Start)	BOOL	Der Roboter hat den Werkzeugraum verlassen, das Teil erfolgreich entnommen/eingelegt und gibt den nächsten Pressenhub frei.

Signale für die Greifer- und Prozessüberwachung (Zunder/Öl)

Signalname	Richtung	Datentyp	Beschreibung
Vakuum / Magnetkreis 1 OK	Greifer → Roboter	BOOL	Bauteil wird sicher vom Magnet-/Vakuumgreifer gehalten (Teileverlustüberwachung).
Teil im Greifer vorhanden	Greifer → Roboter	BOOL	Optische oder induktive Abfrage direkt am Greifer, ob das Blech physisch anliegt.
Doppelblech-Erkennung	Sensor → Roboter	BOOL	Verhindert, dass zwei verklebte Bleche (durch Ziehöl) gleichzeitig in die Presse eingelegt werden (Schutz vor Werkzeugbruch).

3.3.4 Wichtiger Hinweis für die Programmierung (Interlock)

Der Integrator muss Sie im SPS-Programm eine sogenannte **Verriegelung (Interlock)** programmieren.

Das bedeutet:
Das Signal Startfreigabe Presse darf vom Roboter *nur dann* auf 1 gesetzt werden, wenn das Signal F-Roboter in Home sicher ebenfalls 1 ist. Sobald der Roboter auch nur 1 mm aus der Home-Position Richtung Presse herausfährt, muss die Startfreigabe sofort hardwareseitig weggenommen werden.

4 Logisches Ablaufdiagramm für einen kompletten Zyklus

Nachfolgend wird gezeigt, wie eine Ablaufbeschreibung aussehen könnte, für ein logisches Ablaufdiagramm des kompletten Zyklus der Pressenautomation

– vom Einlegen des Blechs bis zum Pressenhub –

Der Ablauf kombiniert die logischen Prozessschritte mit der im vorherigen Schritt definierten Signalabfolge.

4.1 Logischer Zyklus: Pressenautomation (Vom Einlegen bis zum Hub)

Mermaid graph TD
A[Start: Roboter holt Rohteil] --> B[Warten auf Freigabe der Presse]
B --> C{Presse in OT & Sicher?}
C -- Nein --> B
C -- Ja: F-Presse in OT sicher = 1 --> D[Roboter fährt in Werkzeugraum ein]
D --> E[Teil einlegen & Greifer lösen]
E --> F[Roboter verlässt Werkzeugraum]
F --> G{Roboter in sicherer Position?}
G -- Nein --> F
G -- Ja: F-Roboter in Home sicher = 1 --> H[Roboter gibt Hub frei]
H --> I[Presse führt Hub aus]
I --> J[Presse fährt zurück in OT]
J --> A

Verwende Code mit Vorsicht.

4.1.1 Detaillierte Schritt-für-Schritt-Beschreibung

Der Zyklus startet im Automatikbetrieb, wenn beide Systeme fehlerfrei hochgefahren sind und der Schutzzaun geschlossen ist (F-Schutzzaun / Lichtgitter OK = 1).

Schritt 1: Materialaufnahme und Bereitstellung

- **Aktion:** Der Transferroboter nimmt ein neues Blechteil vom Stapelplatz auf.
- **Signalprüfung:** Die Sensoren Teil im Greifer vorhanden = 1 und Vakuum / Magnetkreis 1 OK = 1 müssen aktiv sein. Die Doppelblech-Erkennung muss 0 (kein Doppelblech) melden.
- **Status:** Der Roboter fährt mit dem Rohteil in die Warteposition direkt vor dem Schutzzaun/Werkzeugraum der Presse.

Schritt 2: Einfahrfreigabe und Synchronisation

- **Aktion:** Der Roboter wartet auf das sichere Signal der Presse, dass das Werkzeug komplett geöffnet ist.
- **Signalwechsel:** Die Presse meldet Presse im Automatikmodus = 1, Werkzeug geöffnet = 1 und schaltet das sichere Signal F-Presse in OT sicher = 1.
- **Logik:** Erst wenn F-Presse in OT sicher auf 1 steht, schaltet die Robotersteuerung intern die Achsbewegung für den Werkzeugraum frei.

Schritt 3: Einlegen des Blechteils

- **Aktion:** Der Roboter fährt in den Werkzeugraum ein.
- **Signalwechsel:** Der Roboter setzt das Betriebssignal Roboter fährt ein = 1. Das sichere Signal F-Roboter in Home sicher fällt sofort auf 0.
- **Prozess:** Der Roboter positioniert das Blech exakt im Unterwerkzeug der Presse, schaltet die Magnete/Vakuumdüsen ab und setzt das Signal Teil eingelegt (Beladung fertig) = 1.

Schritt 4: Rückzug in die sichere Parkposition

- **Aktion:** Der Roboter zieht den Greifarm zügig aus dem Gefahrenbereich der Presse zurück in seine Ausgangsposition (Home-Position).
- **Signalwechsel:** Das Signal Roboter fährt ein wechselt wieder auf 0.
- **Sicherheitsverriegelung:** Erst wenn der Roboter die mechanische Trennebene komplett verlassen hat, schaltet das zweikanalige Failsafe-Signal F-Roboter in Home sicher = 1.

Schritt 5: Hub-Auslöser und Pressvorgang

- **Aktion:** Die Presse erhält den Startbefehl für den nächsten Stanz- oder Umformvorgang.
- **Signalwechsel:** Der Roboter setzt das Betriebssignal Startfreigabe Presse (Hub-Start) = 1.
- **Logik (Interlock):** Die Presse startet den Hub nur, weil das übergeordnete Sicherheitskonzept prüft, ob zeitgleich F-Roboter in Home sicher = 1 und Startfreigabe Presse = 1 aktiv sind. Während des gesamten Hubs blockiert der Roboter jede eigene Bewegung in Richtung Presse.

Schritt 6: Zyklusende und Folgezyklus

- **Aktion:** Die Presse führt den Hub aus, formt das Blech um und fährt den Stößel wieder nach oben.
- **Signalwechsel:** Während des Hubs fallen die Pressensignale Werkzeug geöffnet und F-Presse in OT sicher auf 0. Nach Erreichen des oberen Totpunkts schalten sie wieder auf 1, das Signal Teil fertig / Auswerfer oben wird aktiv, und der Zyklus beginnt für den nächsten Roboterschritt (Entnahme/Folgebeladung) von vorn.

4.2 Was passiert bei einer Störung? (Sicherheitsgerichtetes Verhalten)

Der Integrator muss das System so programmieren, dass bei jeder Abweichung vom obigen Ablauf der **Sichere Zustand** eingenommen wird:

- **Teileverlust im Werkzeugraum:** Verliert der Roboter beim Einfahren das Blech vorzeitig (Vakuum / Magnetkreis 1 OK fällt auf 0), stoppt der Roboter sofort (Sicherer Stopp). Die Presse bleibt im OT gesperrt, da die Startfreigabe Presse nicht erteilt wird.
- **Not-Halt während des Hubs:** Wird während des Pressenhubs der Not-Halt des Roboters gedrückt, öffnet das Signal F-Not-Halt Roboter an Presse. Die Pressensteuerung wirft sofort die hydraulische Kupplungs-Brems-Kombination ab, um den Pressenstößel mitten in der Abwärtsbewegung zu stoppen.

5 Erweitertes Sicherheitskonzept zur Integration der Cybersecurity

Das erweiterte Sicherheitskonzept, integriert die Anforderungen der **neuen EU-Maschinenverordnung (MVO 2023/1230)** im Bereich der digitalen Verknüpfung und Cybersecurity (in Anlehnung an die Normenreihe **IEC 62443**).

5.1 Einfluss der EU-Maschinenverordnung auf die Arbeit des Integrators

Die Einführung der **neuen EU-Maschinenverordnung (MVO 2023/1230)**, die ab dem **20. Januar 2027** die alte Maschinenrichtlinie (2006/42/EG) ablöst, verändert die Arbeit des Integrators grundlegend. [1, 2]
Besonders im Vergleich zum alten **BMAS-Interpretationspapier „Gesamtheit von Maschinen“** und hinsichtlich der **digitalen Verknüpfung** ergeben sich weitreichende rechtliche und methodische Neuerungen. [1, 2]

5.1.1 MVO vs. BMAS-Interpretationspapier „Komplexe Anlagen“

Das bisherige BMAS-Interpretationspapier „Gesamtheit von Maschinen“ war eine rein *nationale deutsche Auslegungshilfe*. Es regelte über ein Flussdiagramm, wann verkettete Einzelmaschinen eine rechtlich neue Gesamtanlage bilden (produktionstechnischer und sicherheitstechnischer Zusammenhang). [1, 2, 3, 4]

5.1.2 Was sich durch die MVO ändert:

- **Vom Leitfaden zum Gesetz:** Die Kriterien für eine „Gesamtheit von Maschinen“ (Anlagenverkettung) sind nun **europaweit einheitlich und rechtlich bindend** direkt im Text der MVO verankert. Grauzonen und nationale Unterschiede fallen weg. [1, 2, 3, 4]
- **Rechtssicherheit bei „Wesentlicher Veränderung“:** Das in Deutschland bewährte Prinzip der „wesentlichen Veränderung“ (wann führt ein Umbau oder

eine Erweiterung dazu, dass man rechtlich als neuer Hersteller gilt) wurde ebenfalls direkt in die MVO (Artikel 18) hochgestuft. [1, 2]

- **Der Integrator haftet schärfer:** Wenn Sie bestehende Pressen mit neuen Robotern verketten, prüft die MVO strenger, ob Sie durch den Eingriff in die Sicherheitssteuerung eine „wesentliche Veränderung“ herbeiführen. Ist das der Fall, werden Sie *kraft Gesetz* zum Hersteller der gesamten Anlage und müssen das Konformitätsbewertungsverfahren komplett neu durchführen. [1, 2]

5.2 Was bedeutet die Einbeziehung der „digitalen Verknüpfung“ genau?

Früher bezog sich die Schnittstellen-Risikobeurteilung nach **EN ISO 11161** primär auf mechanische Wechselwirkungen (z. B. Roboter quetscht Hand in der Presse) und die funktionale Sicherheit (z. B. Performance Level von Lichtgittern). [1]

Die neue MVO erweitert den Sicherheitsbegriff radikal um die **digitale Komponente**: **Cybersecurity wird zum integralen Bestandteil der Maschinensicherheit**. [1, 2]

Für Sie als Integrator bedeutet das konkret:

5.2.1 Software ist ein eigenständiges Sicherheitsbauteil [1, 2]

Software, die Sicherheitsfunktionen ausführt (z. B. Ihr Verriegelungsprogramm zwischen Presse und Roboter), gilt nun offiziell als **Sicherheitsbauteil** im Sinne der MVO. Sie muss eine eigene Dokumentation besitzen und im Rahmen der CE-Kennzeichnung separat bewertet werden. [1, 2]

5.2.2 Schutz vor Korrumpierung und Manipulation (Annex III, 1.1.9 & 1.2.1) [1]

Die MVO fordert explizit, dass die Steuerungssysteme gegen **böswillige Manipulation von außen oder innen** (Cyberangriffe, unbefugten Zugriff) geschützt sein müssen. [1, 2]

- **Das Szenario:** Ein Hacker greift über den Fernwartungszugang des Roboters an und manipuliert das Signal `F-Presse in OT sicher` im Software-Code. Der Roboter fährt ein, während die Presse schließt. [1, 2, 3]
- **Die Integratoren-Pflicht:** Der Integrator muss in der Risikobeurteilung nach EN ISO 12100 nachweisen, dass die digitale Verknüpfung (Bus-Systeme, Netzwerke, OT-Gateways*) so abgesichert ist, dass ein digitaler Fehler oder Angriff **niemals zu einem physisch unsicheren Zustand** führen kann. [1, 2]

* Ein OT-Gateway (Operational Technology Gateway) ist eine Hard- und Software-Schnittstelle. Sie verbindet Maschinen und Steuerungen aus der Produktion (OT) mit IT-Systemen oder der Cloud, übersetzt Protokolle und sichert den Datenfluss.

5.2.3 Wesentliche Veränderung durch Software-Updates [1]

Wenn im Rahmen des Update-Vertrags die Software des Roboters oder der Sicherheits-SPS verändert wird, muss genau geprüft werden, ob dies eine „digitale wesentliche Veränderung“ darstellt. Sobald ein Update neue funktionale Risiken

erzeugt oder Logiken ändert, erlischt die alte CE-Kennzeichnung und der Integrator haftet erneut. [1, 2, 3]

5.3 Zusammenfassung für Ihre Risikoanalyse

Bereich	Alte Welt (Richtlinie / BMAS)	Neue Welt (MVO ab 2027)
Schnittstellen-Fokus	Mechanisch, elektrisch, funktional.	Mechanisch, elektrisch, funktional **+ digital (Cybersecurity)**.
Risikobeurteilung	Fokus auf physische Gefahren.	Bedrohungsanalyse für Software & Datenintegrität zwingend erforderlich.
Updates	Reine Wartungsmaßnahme.	Potenzielle „wesentliche Veränderung“ mit neuer CE-Pflicht.

5.4 Erweiterung der Schnittstellen-Risikobeurteilung um Cyber-Risiken

Der Integrator muss ab 2027 nachweisen, dass die digitale Kopplung zwischen Presse, Roboter und dem Netzwerk des Auftraggebers gegen Verfälschung und unbefugte Eingriffe geschützt ist.

Schnittstellen-Risikobeurteilung mit Cyber-Risiken

Schritt / Systembereich	Identifizierte digitale Gefahr (MVO Annex III)	Ursache / Wechselwirkung (Digitale Verknüpfung)	Risikobewertung (ohne Schutzmaßnahme)	Technische / Organisatorische Schutzmaßnahme	Restrisiko & Info
Fernwartung & Software-Updates	**Böswillige Manipulation** von Parametern oder Steuerungslogik.	Unbefugter Zugriff über das Firmennetzwerk (IT) auf das Produktionsnetzwerk (OT) des Fertigungssystems.	**Kritisch** (Gefahr der Deaktivierung von Sicherheitskreisen)	**Zonen-Trennung (IEC 62443):** Physische Trennung von IT und OT über eine zertifizierte **Firewall**. Fernzugriff erfolgt ausschließlich über ein **verschlüsseltes VPN** mit **Zwei-Faktor-Authentifizierung (2FA)**. Einwahl ist nur nach manueller, physischer Schlüsselschalter-Freigabe vor Ort an der Anlage möglich.	**Akzeptabel.** Der Auftraggeber muss restriktive Benutzerrechte (RBAC) in seiner IT-Infrastruktur pflegen.
Netzwerk-Kommunikation	**Sicherheits-Ausfall** durch manipulierten Datenverkehr (z.B. DoS-Angriff).	Der Kommunikationsbus (z. B. PROFINET) wird mit Datenpaketen geflutet, wodurch sichere Signale verzögert werden oder ausfallen.	**Hoch** (Ungewollter Anlauf oder blockierter Not-Halt)	**Black-Channel-Prinzip (PROFIsafe):** Die sicherheitsgerichteten Datenpakete erhalten eine fortlaufende Zähler-ID, eine Zeitstempel-Überwachung und eine CRC-Prüfsumme. Bei jeder Unregelmäßigkeit oder Verzögerung im Netzwerk schaltet das System sofort in den **Sicheren Zustand (Not-Halt / PLd)**.	**Gering.** Manipulierte Pakete führen zum sofortigen Produktionsstopp, niemals zur Gefährdung.
Lokales HMI / Software-Integrität	**Unbeabsichtigte / unbefugte Änderung** der Software.	Ein Einrichter ändert unbemerkt kritische Geschwindigkeitsgrenzen oder Sicherheitszeiten am Bedienpanel (HMI).	**Mittel** (Mechanischer Werkzeugbruch oder Personenschaden)	**Manipulationsschutz nach MVO:** Die Sicherheitskonfiguration ist durch ein separates Passwort geschützt. Jede Änderung erzeugt einen Eintrag in einem **revisionssicheren Logbuch (Audit Trail)** in der Sicherheits-SPS. Die Firmware des Roboters akzeptiert nur digital signierte Updates.	**Akzeptabel.** Regelmäßige Überprüfung der Logfiles durch den Sicherheitsverantwortlichen.

5.5 Was Integratoren nun zusätzlich dokumentieren müssen

Um die Konformität nach der neuen MVO für das Integrierte Fertigungssystem zu erklären, reicht eine rein mechanische Dokumentation nicht mehr aus. Sie müssen folgende Nachweise zur technischen Akte (Technical File) hinzufügen:

1. **Software-Lebenszyklus-Dokumentation:** Eine Beschreibung, wie die Sicherheitssoftware entwickelt, getestet und vor unbefugten Änderungen geschützt wurde.
2. **Nachweis der Integrität (Prüfsummen):** Nach der Inbetriebnahme und Validierung der Anlage müssen Sie die eindeutigen **Prüfsummen (Checksummen)** des Sicherheits-SPS-Programms und der Roboter-Sicherheitskonfiguration im Abnahmeprotokoll dokumentieren. Jede spätere Abweichung von dieser Prüfsumme gilt als Modifikation und erfordert eine Überprüfung der CE-Konformität.
3. **Schnittstellen-Architekturplan:** Ein Netzwerkplan, der genau zeigt, welche Datenflüsse zwischen der Presse (Bestandsanlage), dem Roboter und externen Systemen (MES/ERP/Fernwartung) existieren und wo sich die Sicherheitsgrenzen (Firewalls/Gateways) befinden.

---

6 Schaltplandarstellung der Signale

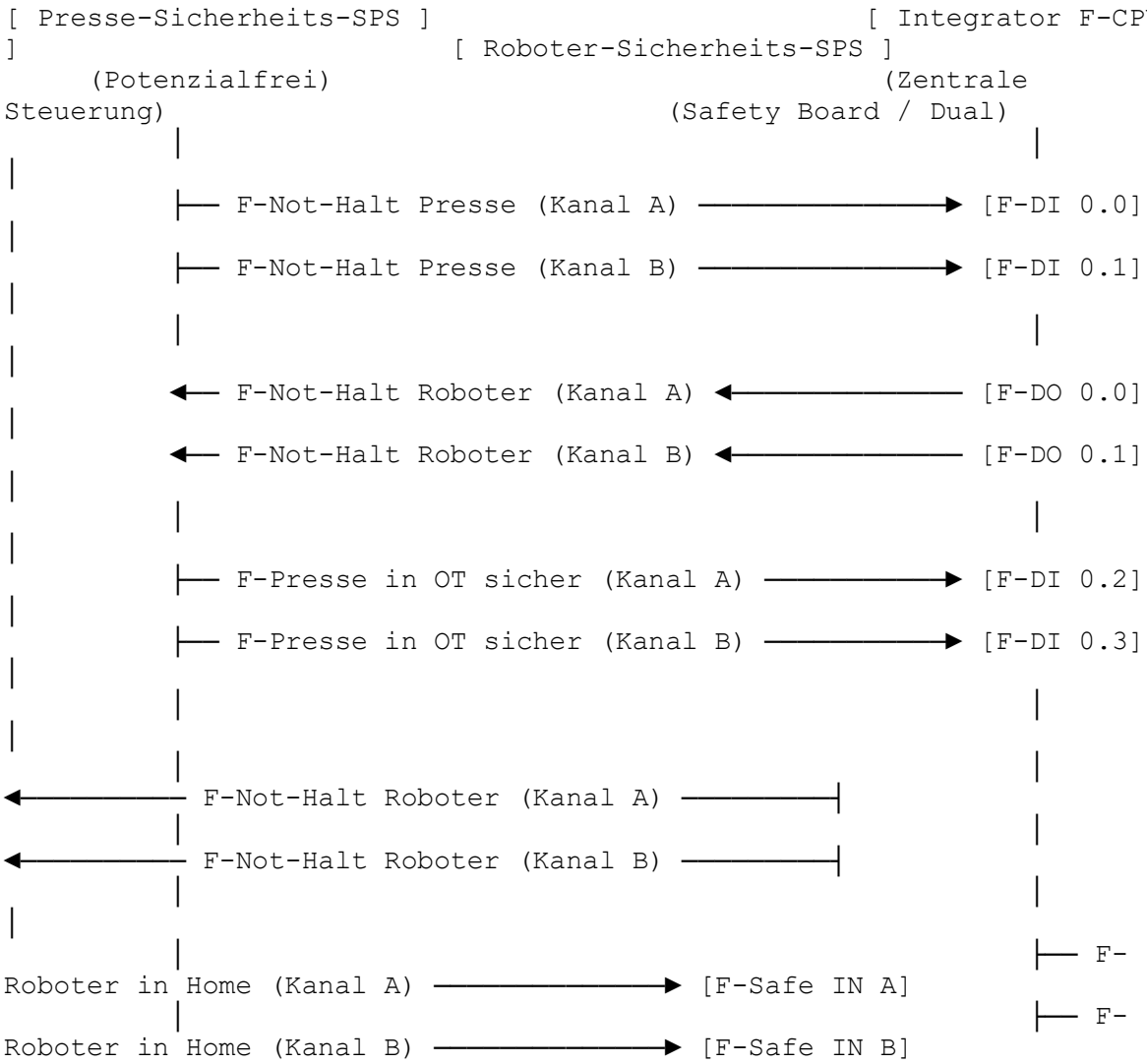
Wie müssen die sicherheitsgerichteten und betriebsmäßigen Signale (inklusive der neuen Cybersecurity-Komponenten wie dem Schlüsselschalter für Fernwartung) in einem **Schaltplan (E-Plan)** funktional dargestellt werden?

6.1 Schaltungstechnische Umsetzung und die Darstellung der Signale im Schaltplan (E-Plan) für Ihre integrierte Roboter-Transferanlage.

Da die Anlage als **Integriertes Fertigungssystem (IMS)** nach EN ISO 11161 projektiert wurde, müssen die sicherheitsgerichteten Signale (Failsafe) zwingend **zweikanalig** und mit **Querschlusserkennung** ausgeführt werden, um den geforderten Performance Level (PLd/PLe) zu erreichen.

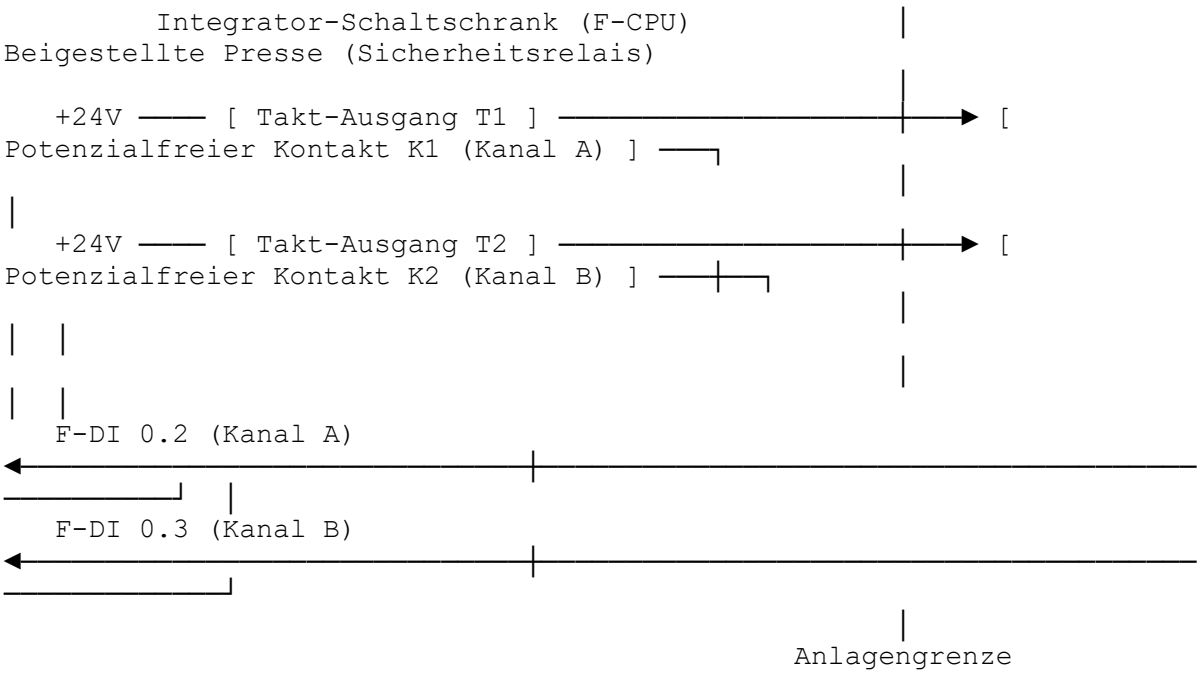
6.2 Prinzipschaltbild: Einbindung der Sicherheits-SPS (F-CPU)

In modernen Anlagen werden die Signale der Presse und des Roboters über eine zentrale Sicherheits-SPS (z. B. Siemens SIMATIC S7-F-CPU oder PILZ PNOZmulti) miteinander verriegelt. Die folgende Darstellung zeigt das Verdrahtungsprinzip für die digitalen Failsafe-Eingänge (F-DI) und -Ausgänge (F-DO).



6.3 Schaltplan-Auszug: Zweikanalige Querschlusserkennung

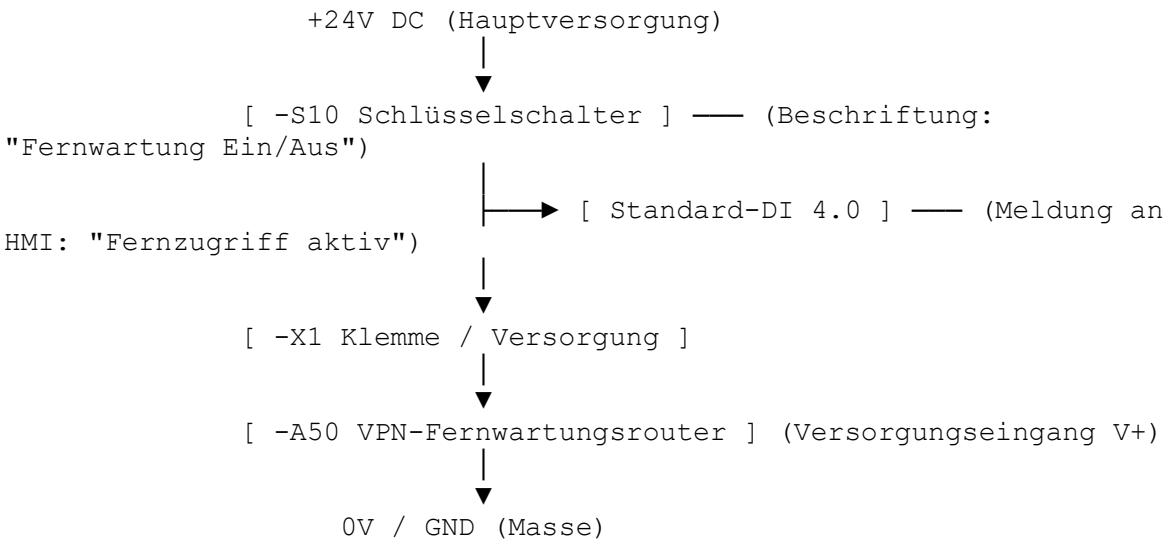
Um einen Kurzschluss zwischen den beiden Kanälen (A und B) oder gegen die Versorgungsspannung (24V) sofort zu erkennen, nutzt die F-CPU **Taktsignale** (Takt A und Takt B).
Hier ist das schaltungstechnische Prinzip für das Signal **„F-Presse in OT sicher“** (Rückmeldung der Presse an den Integrator-Schaltschrank):



- **Logik im E-Plan:** Die F-CPU prüft permanent, ob das Signal an `F-DI 0.2` exakt dem Pulsmuster von `T1` entspricht. Kreuzen sich die Kabel (Querschluss), erkennt die SPS das falsche Taktsignal und schaltet die Anlage sofort ab.

6.4 Schaltungstechnische Integration der Cybersecurity (MVO 2023/1230)

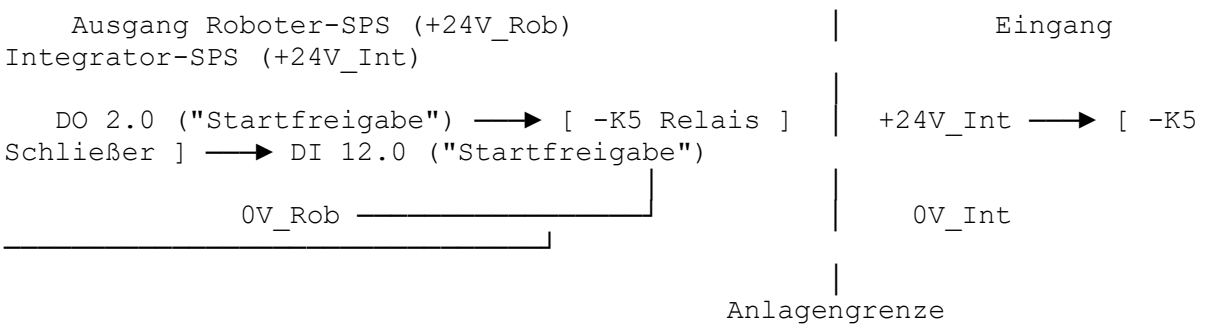
Um die neuen Anforderungen der Maschinenverordnung an den manipulationssicheren Fernzugriff hardwareseitig umzusetzen, wird ein **physischer Schlüsselschalter** am Bedienpult der Anlage installiert. Erst dieser Schalter schaltet die Versorgungsspannung für den Fernwartungs-Router (z. B. Ewon, Tosibox) frei.



- **Schaltplan-Vorteil:** Solange der Schlüssel abgezogen ist, ist der Router komplett stromlos. Ein digitaler Angriff über das Internet auf das Integrierte Fertigungssystem ist physikalisch unmöglich.

6.5 Standard-E/A (Kollisionsschutz) im Schaltplan

Die betriebsmäßigen Signale (z. B. `Startfreigabe Presse` oder `Qualitätskontrolle / Gutteil`) werden über Standard-E/A-Baugruppen (nicht fehlersicher) verdrahtet. Da die Presse und der Roboter oft separate Stromkreise nutzen, müssen diese Signale über **Koppelrelais** potenzialgetrennt werden:



6.6 Wie diese Signale im E-Plan dokumentiert werden sollten

- **Ortskürzel verwenden:** Kennzeichnen Sie die Betriebsmittel nach ihrer Zugehörigkeit (z. B. `=PRS1+SCH1-K5` für das Koppelrelais im Schaltschrank der Presse 1).
- **Sicherheitsstromkreise farblich abheben:** Im Schaltplan werden die Adern für Failsafe-Signale traditionell in **Gelb** oder **Rot** gezeichnet, während Standard-24V-Signale in **Dunkelblau** dargestellt werden.

6.6.1 Konkretes SPS-Code-Beispiel für die logische Verknüpfung der Signale

Der Code ist zweigeteilt:
Zuerst wird der **fehlersichere Teil** (Failsafe für den Personenschutz) in FUP (Funktionsplan) dargestellt, danach folgt die **betriebsmäßige Ablauflogik** in SCL (Structured Control Language) inklusive der neuen MVO-Cybersecurity-Überwachung.

6.6.2 Fehlersicherer Code (F-Programm in FUP)

Dieser Baustein läuft in der Sicherheits-SPS (F-CPU). Er berechnet die absolut sichere Einfahrfreigabe für den Roboter. Er ist so aufgebaut, dass beim Ausfall eines Signals (0-Signal) sofort der sichere Zustand eingenommen wird.

Netzwerk 1: Berechnung der sicheren Einfahrfreigabe für den Roboter

text

```
                                  +---------+
"F-Presse_in_OT_sicher" ----------|  &      |
"F-Schutzzaun_Lichtgitter_OK" ----|         |--------(
#F_Sichere_Einfahrfreigabe )
"F-Not-Halt_Kette_OK" ------------|         |
                                  +---------+
```

Verwende Code mit Vorsicht.

Netzwerk 2: Sicherer Not-Halt an die Presse (Auslösung durch Roboter)

text

```
                                  +---------+
"F-Not-Halt_Roboter_OK" ----------|  &      |
"F-Router_Cybersecurity_OK" ------|         |--------( "F-Not-
Halt_an_Presse" )
                                  +---------+
```

Verwende Code mit Vorsicht.

Hinweis zu Netzwerk 2: Sollte der Fernwartungsrouter trotz ausgeschaltetem Schlüsselschalter eine unbefugte Aktivität melden (`#F-Router_Cybersecurity_OK = 0`), wird die Presse sofort sicher gestoppt.

6.6.3 Betriebsmäßiger Code (Standard-Programm in SCL)

Dieser Baustein regelt den automatischen Ablauf, den Kollisionsschutz und die Qualitätskontrolle (Gut-/Ausschusshub). Er wertet zudem den Zustand des Cybersecurity-Schlüsselschalters aus.

scl

```
FUNCTION_BLOCK "FB_Pressenautomation_Zyklus"
{ S7_Optimized_Access := 'TRUE' }
VERSION : 0.1
VAR_INPUT
    // Physische Eingänge von der Anlage / Presse
    I_Presse_Automatik        : Bool;   // Presse steht auf Automatik
    I_Werkzeug_geoeffnet       : Bool;   // Mechanische Rückmeldung
Werkzeug offen
    I_Teil_verfuegbar          : Bool;   // Auswerfer oben / Blech
bereit
    I_Schluessel_Fernwartung   : Bool;   // Hardware-Schlüsselschalter
am HMI

    // Signale von der Qualitätskontrolle (Kamera / Sensorik)
    I_Kamera_GUT_Teil         : Bool;   // Optische Prüfung: Teil ist
maßhaltig
    I_Kamera_SCHLECHT_Teil    : Bool;   // Optische Prüfung: Ausschuss
(z.B. Riss)

    // Sicheres Signal aus dem F-Programm (wird intern übergeben)
    I_F_Sichere_Einfahrfreigabe : Bool;
END_VAR

VAR_OUTPUT
    // Ausgänge an den Roboter und die Presse
    O_Roboter_Einfahrbefehl   : Bool;   // Befehl an Roboter: In
Werkzeug einfahren
    O_Startfreigabe_Presse    : Bool;   // Signal an Presse für den
nächsten Hub
    O_Weiche_Ausschuss_aktiv  : Bool;   // Steuerung der Sortierweiche
    O_HMI_Fernwartung_Aktiv   : Bool;   // Anzeige auf dem Bedienpanel
END_VAR

VAR
    // Interne Schrittkette und Merker
    Stat_Schritt              : Int := 0; // 0=Reset, 10=Warten auf
Presse, 20=Einfahren, 30=Qualitätsprüfung
    Stat_Qualitaet_OK         : Bool;   // Zwischenspeicher Ergebnis
Qualitätsprüfung
END_VAR

BEGIN
    //
================================================================
    // CYBERSECURITY & MVO-ÜBERWACHUNG (IMMER AKTIV)
    //
================================================================
    // Der Zustand des Schlüsselschalters wird an das HMI gemeldet.
    // Ein unbefugtes Einschalten löst eine Warnmeldung aus.
    "O_HMI_Fernwartung_Aktiv" := #I_Schluessel_Fernwartung;
```

```
    //
================================================================
    // ABLAUFSTEUERUNG (INTERLOCK & PROZESS)
    //
================================================================
    CASE #Stat_Schritt OF

        0: // Initialisierung / Reset-Zustand
            #O_Roboter_Einfahrbefehl := FALSE;
            #O_Startfreigabe_Presse  := FALSE;
            #Stat_Qualitaet_OK       := FALSE;
            IF #I_Presse_Automatik THEN
                #Stat_Schritt := 10;
            END_IF;

        10: // Warten auf sichere Bedingungen der Presse
            // Nur wenn das F-Programm die Freigabe gibt UND die
Standard-Signale stimmen
            IF #I_F_Sichere_Einfahrfreigabe AND #I_Werkzeug_geoeffnet
AND #I_Teil_verfuegbar THEN
                #O_Roboter_Einfahrbefehl := TRUE; // Roboter darf Blech
holen/einlegen
                #Stat_Schritt := 20;
            END_IF;

        20: // Roboter arbeitet im Werkzeugraum
            // Warten bis der Roboter fertig gemeldet hat und den Raum
verlassen hat
            // (Das Signal "F-Roboter_in_Home_sicher" wird direkt in
der Pressen-Hardware verriegelt)
            IF "I_Roboter_wieder_in_Home" THEN
                #O_Roboter_Einfahrbefehl := FALSE;
                #Stat_Schritt := 30; // Wechsel zur Qualitätskontrolle
            END_IF;

        30: // Nachgelagerte Qualitätskontrolle (MVO-
Prozessoptimierung)
            IF #I_Kamera_GUT_Teil AND NOT #I_Kamera_SCHLECHT_Teil THEN
                #Stat_Qualitaet_OK := TRUE;
                #O_Weiche_Ausschuss_aktiv := FALSE; // Teil geht zur
Weiterverarbeitung
                #O_Startfreigabe_Presse := TRUE;    // Nächsten
Pressenhub freigeben
                #Stat_Schritt := 10;                // Zyklus von vorn

            ELSIF #I_Kamera_SCHLECHT_Teil THEN
                #Stat_Qualitaet_OK := FALSE;
                #O_Weiche_Ausschuss_aktiv := TRUE;  // Ausschussweiche
aktivieren
                #O_Startfreigabe_Presse := FALSE;   // Presse stoppen
wegen Serienfehler-Gefahr
                #Stat_Schritt := 0;                 // Anlage in
sicheren Halt/Reset zwingen
            END_IF;

    END_CASE;
END_BLOCK
```

Verwende Code mit Vorsicht.

7. Besonderheiten dieser Software-Architektur nach EN ISO 11161:

- **Zweistufige Verriegelung:** Selbst wenn im SCL-Code durch einen Programmierfehler `#O_Roboter_Einfahrbefehl` auf `TRUE` gesetzt wird, verhindert das F-Programm im Hintergrund jede physikalische Bewegung, falls das Lichtgitter unterbrochen oder die Presse nicht im OT ist.
- **Fehlersichere Datenbausteine (F-DB):** Die Variablen mit dem Präfix `F-` liegen in einem geschützten Speicherbereich der F-CPU. Dieser Bereich ist mit einer separaten F-Schnittstellen-Prüfsumme versehen, die bei der CE-Zertifizierung unveränderlich dokumentiert wird.

Die nachfolgende strukturierte Validierungs-Checkliste für die technische Dokumentation (Technical File) dieses Integrierten Fertigungssystems ist methodisch so aufgebaut, dass sie die Anforderungen der **neuen EU-Maschinenverordnung (MVO 2023/1230)** erfüllt.
Sie dient dem rechtssicheren Nachweis, dass sowohl die funktionale Sicherheit (EN ISO 11161 / EN ISO 13849-1) als auch die Cybersecurity-Maßnahmen im SPS-Code real geprüft wurden und fehlerfrei funktionieren.

---

8 VALIDIERUNGS-CHECKLISTE: SOFTWARE & DIGITALE VERKNÜPFUNG

Projekt: Roboter-Transferanlage Pressenautomation

Normenbasis: EN ISO 11161:2010, EN ISO 13849-1, EU-MVO 2023/1230

Verantwortlicher Integrator (Natürliche Person): [Name des Integrators]

1. Stammdaten & Software-Integrität (MVO-Konformität)

Vor dem eigentlichen Funktionstest müssen die Softwarestände unveränderlich eingefroren werden.

- **F-Gesamtprüfsumme (F-Signature):** Die eindeutige CRC-Prüfsumme des F-Programms der Sicherheits-SPS wurde ausgelesen und dokumentiert.
  Ist-Wert: `0x_____`
- **Roboter-Sicherheitsprüfsumme:** Die Prüfsumme der sicheren Achs- und Raumüberwachung des Roboters (z. B. SafeOperation / Dual Check Safety) wurde dokumentiert.
  Ist-Wert: `0x_____`
- **Firmware-Integrität:** Es wurde überprüft, dass alle eingesetzten Netzwerkkomponenten (SPS, Router, Managed Switches) auf dem aktuellen, vom Hersteller signierten Sicherheits-Patch-Stand sind.

2. Funktionale Validierung der Failsafe-Signale (FUP-Programm)

Ziel: Nachweis, dass Signalfehler immer in den sicheren Zustand (Stopp) führen.

Prüfpunkt / Testverfahren	Erwartetes Verhalten	Ergebnis (i.O. / n.i.O.)	Prüfer / Datum
Drahtbruch F-Not-Halt Presse: Abklemmen eines Kanals des Signals `F-Not-Halt Presse an Roboter` im laufenden Betrieb.	Der Roboter muss sofort in den *Sicheren Stopp* (STO) fallen. Die F-CPU muss einen Peripherie-Fehler (Querschluss/Drahtbruch) melden.	[ ]	_____
Plausibilität OT-Signal: Manuelles Erzwingen des Signals `F-Presse in OT sicher = 1`, während der Pressenstößel die OT-Position physisch verlässt.	Die F-CPU muss die Diskrepanzzeit-Verletzung erkennen, das Signal intern auf `0` setzen und die Einfahrfreigabe für den Roboter sperren.	[ ]	_____
Black-Channel-Unterbrechung: Physisches Ziehen des Netzwerkkabels (PROFINET) zwischen Presse und Integrator-SPS während der Roboter einfährt.	Das PROFIsafe-Protokoll muss den Timeout erkennen. Beide Anlagen müssen sofort einen Not-Stopp auslösen.	[ ]	_____

3. Validierung der Ablauflogik & Qualitätskontrolle (SCL-Programm)

Ziel: Nachweis, dass Prozessfehler und Schlechtteile nicht zu Gefährdungen führen.

Prüfpunkt / Testverfahren	Erwartetes Verhalten	Ergebnis (i.O. / n.i.O.)	Prüfer / Datum
Einfahr-Interlock (Code-Simulation): SCL-Schrittkette auf Schritt 20 setzen (`O_Roboter_Einfahrbefehl = TRUE`), während `I_F_Sichere_Einfahrfreigabe = FALSE` ist.	Der Roboter darf sich physisch nicht bewegen. Das F-Programm muss das Standard-Ablaufsignal hart überschreiben und blockieren.	[ ]	
Ausschussteil-Erkennung: Simulation des Kamerasignals `I_Kamera_SCHLECHT_Teil = 1` nach dem Pressenhub.	Die Ausschussweiche muss aktivieren (`O_Weiche_Ausschuss_aktiv = 1`). Die Anlage muss in Schritt 0 (Reset) wechseln und den Folgestart sperren.	[ ]	
Doppelblech-Reaktion: Sensor meldet ein Doppelblech beim Aufnehmen des Rohteils.	Der Roboter muss die Fahrt zur Presse stoppen, eine Fehlermeldung am HMI ausgeben und darf das Signal `Roboter fährt ein` nicht setzen.	[ ]	

---

4. Validierung der Cybersecurity-Maßnahmen (MVO Annex III)

Ziel: Nachweis des physischen und digitalen Schutzes gegen unbefugte Manipulation.

- **Schlüsselschalter-Test:** Wenn der Schlüsselschalter `-S10` auf „AUS“ steht, wurde messtechnisch überprüft, dass am VPN-Router keine Versorgungsspannung (0V) anliegt.
- **Verbindungs-Ausschuss:** Bei eingeschaltetem Router (`-S10` auf „EIN“) wurde versucht, ohne VPN-Zertifikat und ohne 2-Faktor-Authentifizierung auf die SPS zuzugreifen. Der Zugriff muss von der integrierten Firewall blockiert und im Audit Trail protokolliert werden.
- **HMI-Passwortschutz:** Es wurde verifiziert, dass die Eingabe von kritischen Parametern (z.B. Erhöhung der Robotergeschwindigkeit beim Teachen) nur nach Eingabe eines passwortgeschützten Benutzer-Levels (Level: Integrator) möglich ist.

Freigabeerklärung des Integrators

Hiermit wird bestätigt, dass alle oben aufgeführten Software-Funktionstests und Sicherheitsprüfungen erfolgreich durchgeführt wurden. Die Software entspricht in ihrer Logik und Absicherung dem aktuellen Stand der Technik sowie den Anforderungen der EU-Maschinenverordnung (MVO 2023/1230).

Ort, Datum: _____

Unterschrift des Integrators: _____

Mit dem Ausfüllen dieser Checkliste und dem Beifügen des SCL/FUP-Codes in Ihre technische Dokumentation wurde die Sorgfaltspflicht als Integrator nachgewiesen.

Die nachfolgend aufgeführten Betreiber-Anweisungen, sind vom Integrator der Betriebsanleitung der Roboter-Transferanlage beizufügen.

Nach der **neuen EU-Maschinenverordnung (MVO 2023/1230)** und der Norm **IEC 62443** ist der Hersteller/Integrator verpflichtet, dem Betreiber klare organisatorische und technische Vorgaben für den sicheren Betrieb des Integrierten Fertigungssystems (IMS) zu übergeben.

Damit sind von der rechtlichen Vertragsstruktur über die technische Risikobeurteilung, die Signal- und Code-Ebene bis hin zur Betreiber-Dokumentation alle wesentlichen Bausteine für das Projekt für den Integrator vorhanden.

---

9 BETREIBER-ANWEISUNGEN: DIGITALE SICHERHEIT & CYBERSECURITY

Anlage zur Betriebsanleitung gemäß EU-MVO 2023/1230 (Anhang III)
System: Roboter-Transferanlage zur Pressenautomation
Verantwortlicher Integrator (Natürliche Person): [Name des Integrators]

1. Organisatorisches Schlüsselmanagement für die Fernwartung

Der installierte Hardware-Schlüsselschalter (`-S10`) am Bedienpult stellt den primären physischen Schutz gegen unbefugte Fernzugriffe dar. Der Betreiber ist verpflichtet, diesen wie folgt zu verwalten:

- **Restriktive Schlüsselvergabe:** Der physische Schlüssel für den Schalter `-S10` darf ausschließlich an autorisiertes und geschultes Fachpersonal (z. B. den Leiter der Instandhaltung oder den IT-Sicherheitsbeauftragten des Werks) ausgegeben werden.
- **„Abgezogen"-Prinzip:** Im regulären Automatikbetrieb der Anlage muss der Schlüssel abgezogen und sicher verwahrt werden. Der VPN-Router hat im Produktionsalltag permanent stromlos zu sein.
- **Protokollierung bei Aktivierung:** Jede Aktivierung des Fernzugriffs durch Umlegen des Schlüsselschalters ist vom Instandhaltungspersonal schriftlich oder digital (z. B. im Schichtbuch) unter Angabe von Datum, Uhrzeit, Grund und Name des Technikers zu protokollieren.

---

2. Vorgaben für den Fernzugriff (Remote Access Policy)

Wenn der Integrator oder ein Drittanbieter via Fernwartung auf die Roboter-Transferanlage zugreift, müssen folgende IT-Sicherheitsregeln eingehalten werden:

- **Zwei-Faktor-Authentifizierung (2FA):** Der Zugriff über das Netzwerk darf niemals über einfache Passwörter erfolgen. Das vom Betreiber bereitgestellte Netz muss eine 2FA-Abfrage (z. B. via Authenticator-App oder SMS-Token) erzwingen.
- **Sichtkontakt-Pflicht bei Bewegung:** Es ist strengstens untersagt, Achsbewegungen des Roboters oder Hübe der Presse per Fernwartung auszuführen, wenn kein direkter Sichtkontakt zur Anlage besteht. Befindet sich der Programmierer remote an einem anderen Standort, muss eine qualifizierte Fachkraft vor Ort an der Anlage stehen, die den Gefahrenbereich überwacht und die Bewegung über einen Zustimmtaster oder den Not-Halt jederzeit abbrechen kann.
- **Sofortige Deaktivierung:** Nach Beendigung der Wartungsarbeiten ist der Schlüsselschalter unverzüglich wieder in Position „AUS" zu bringen und der Schlüssel abzuziehen.

---

3. Benutzerverwaltung und Passwort-Richtlinien am HMI

Um unbefugte Änderungen an der Ablaufsteuerung (SCL-Code) oder den Prozessparametern (z. B. Taktzeiten, Kameraschwellen der Qualitätskontrolle) zu verhindern, muss das lokale Bedienpanel (HMI) abgesichert werden:

- **Personalisierte Logins:** Das pauschale Login über Standard-Benutzer (z. B. „Bediener“ mit Passwort „1234“) ist für administrative Tätigkeiten unzulässig. Jeder Einrichter und Instandhalter muss ein eigenes Benutzerkonto erhalten.
- **Passwort-Komplexität:** Passwörter für die Level „Einrichter“ und „Instandhaltung“ müssen den IT-Richtlinien des Betreibers entsprechen (mindestens 8 Zeichen, Sonderzeichen, Zahlen).
- **Automatisches Logout (Time-Out):** Das HMI ist so konfiguriert, dass nach [z. B. 5 Minuten] Inaktivität ein automatisches Logout des aktuellen Benutzers erfolgt. Das Personal ist anzuweisen, diese Funktion nicht durch mechanische Hilfsmittel (z. B. Festklemmen von Tasten) zu umgehen.

---

4. Verhalten bei Cyber-Sicherheitsvorfällen (Incident Response)

Sollte der Betreiber den Verdacht haben, dass die digitale Verknüpfung der Anlage korrumpiert wurde (z. B. unkontrolliertes Verhalten des Roboters, unerwartete Fehlermeldungen der Sicherheits-SPS, unbefugte Netzwerkaktivität im Audit Trail), ist nach folgendem Notfallplan vorzugehen:

1. **Anlage stoppen:** Sofortige Betätigung des Not-Halt-Tasters, um das Fertigungssystem in den mechanisch und elektrisch sicheren Zustand zu versetzen.
2. **Netzwerktrennung:** Physikalisches Ziehen des Netzwerkkabels (Uplink zum Firmennetzwerk) am Schaltschrank, um eine weitere Ausbreitung des Angriffs oder Datenabfluss zu verhindern.
3. **Integrator informieren:** Benachrichtigung des verantwortlichen Integrators zur gemeinsamen Überprüfung der Software-Prüfsummen (Vergleich mit den Werten aus der Validierungs-Checkliste).

Bestätigung des Betreibers

Mit der Übernahme der Anlage und der technischen Dokumentation bestätigt der Betreiber, die oben genannten Anweisungen in seine internen Betriebsabläufe, Arbeitsanweisungen und Unterweisungen aufzunehmen.

Ort, Datum: _____
Unterschrift des Betreibers (Werksleitung / Sicherheitsbeauftragter):
_____
