Die EN ISO 11161 in der Praxis – Stand 2026 -

Beschreibung der Anwendung der Norm auf Integrierte Fertigungssysteme (IMS) mit Beispielen für Neuanlagen mit CE-Kennzeichnung und Bestandsanlagen ohne CE-Kennzeichnung bei Retrofit-Projekten – 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

1. Die Sicherheitsnorm EN ISO 11161:2010 - Sicherheit von Maschinen – Integrierte Fertigungssysteme (IMS– Integrated Manufacturing System) 4
1.1 Kurze Einführung in die Norm und Erläuterung des Begriffs IMS: 4
1.2 Grundlegende Anforderungen der EN ISO 11161 4
1.2.1 Ziel der Norm 4
1.2.2 Anwendungsbereich der Norm 4
1.2.3 Konkretisierung der Normen zur Risikobeurteilung 5
1.3 Der Integrator als natürliche Person und Generalunternehmer 5
1.3.1 Abnahmekriterien für integrierte Fertigungssysteme und Roboteranlagen 5
1.3.2 Allgemeine grundlegende Vereinbarungen 5
1.3.3 Kriterien für die Abnahme 6
2.Die Bestimmung der Grenzen eines Integrierten Fertigungssystems (IMS) in der EN ISO 11161 7
2.1 Räumliche Grenzen (Ortsbezogene Grenzen) 7
2.2 Zeitliche Grenzen (Lebensdauer und Zyklen) 7
2.3 Grenzen der Verwendung (Bestimmungsgemäße Nutzung) 7
2.4 Schnittstellen und steuerungstechnische Grenzen 7
3. Das Konzept der Aufgabenbereiche (Task Zones) 8
4. Praktische Umsetzung des Zonenkonzepts 8
4.1 Festlegung physischer und sensorischer Grenzen 9
4.2 Steuerungstechnische Hierarchie (Sicherheitszonen) 9
4.3 Absicherung der Schnittstellen (Übergabebereiche) 9
5. Beispiel aus der Praxis: Verpackungsstraße 9
6. Das Not-Halt-System im IMS 10
6.1 Die Hierarchie der Not-Halt-Funktion 10
6.2 Kriterien für die Aufteilung in Not-Halt-Zonen 10
6.3 Steuerungstechnische Verknüpfung 10
7. Die Dokumentationspflichten des Integrators 11
7.1 Die übergreifende Risikobeurteilung (Gesamt-IMS) 11
7.2 Der Sicherheits-Schnittstellenplan (Interface Specification) 11
7.3 Die Betriebsanleitung für das Gesamtsystem 11
7.4 Konformitätserklärung und CE-Kennzeichnung 12
8. Part 1: Das Verfahren zum Wiederanlauf (Reset / Re-Start) 12
8.1 Die Quittierung (Reset) der Sicherheitsfunktion 12
8.2 Der eigentliche Wiederanlauf (Start / Re-Start) 12
9. Part 2: Vertiefung der Schnittstellen-Validierung 13

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

9.1 Das Kernproblem an der Schnittstelle 13
9.2 Validierung der funktionalen Logik (Sicherheits-Kreuzvergleich) 13
9.3 Validierung der Gesamtsicherheitsabstandes (Nachlaufmessung) 13
9.4 Protokollierung der Validierung 14
10. Part 1: Beispiel für ein Validierungs-Testprotokoll 14
10.1 Systemkonfiguration & Softwarestände 14
10.2 Durchführung der funktionalen und Fehlersimulations-Tests 15
10.3 Messtechnische Überprüfung (Nachlaufmessung nach EN ISO 13855) 15
11. Part 2: Retrofit von Bestandsmaschinen ohne moderne Netzwerkschnittstelle 16
11.1 Bestandsaufnahme und Wesentliche Veränderung prüfen 16
11.2 Technische Umsetzung der Kopplung (Hardware-Retrofit) 16
11.3 Das Problem der Bremswege und Nachlaufzeiten 17
12. Part 1: Schaltbeispiel für die analoge Not-Halt-Einbindung 17
12.1 Prinzip Skizze der Schaltung 18
12.2 Funktionsweise der Schaltung 18
13. Part 2: Organisatorische Maßnahmen (Schulung der Bediener) 19
13.1 Kennzeichnung und visuelle Führung (Das größte Risiko minimieren) 19
13.2 Spezifische Schulungsinhalte für gemischte Anlagen 19
13.3 Organisatorische Absicherung bei Wartung (LOTO - Lockout/Tagout) 19
14. Praxisbeispiel: Betriebsanweisung (SOP) für den Fehlerfall 20
14.1 Standardarbeitsanweisung (SOP) – Sicherheits-Schnittstellenfehler 20
14.2 Situationsbeschreibung (Wann gilt diese SOP?) 20
14.3 Sofortmaßnahmen für den Anlagenbediener 20
14.4 Maßnahmen für das Instandhaltungspersonal (Elektro-Fachkraft) 21
14.5 Kontrollierter Wiederanlauf nach Fehlerbehebung 22
15. Simulation von Fehlerzuständen im Rahmen der wiederkehrenden Prüfungen (UVV / jährliche Sicherheitsprüfung 22
15.1 Simulation von Hardware-Fehlern (Fehlereinspeisung) 22
15.2 Simulation von hängenden/verschweißten Schützen (EDM-Test) 23
15.3 Prüfung der zeitlichen Bedingungen (Nachlauf- und Divergenzzeiten) 23
15.4 Wichtige Dokumentationspflicht für den Betreiber 24
15.5 Rechtliche Konsequenzen für den Betreiber, wenn eine solche jährliche Prüfung Mängel an der IMS-Schnittstelle aufdeckt. 24
15.6 Zivil- und strafrechtliche Konsequenzen im Falle eines Unfalls 25
16. Das korrekte Vorgehen für den Betreiber bei Mängeln 25
17. Die rechtssichere Pflichtenübertragung (Delegation) 26
17.1 Part 1: Die rechtssichere Pflichtenübertragung (Delegation) 26
17.2 Form und Inhalt der Übertragung 26

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

17.3 Die Auswahlpflicht (Sorgfältige Auswahl) 26
17.4 Die Ausstattungspflicht (Ressourcen und Befugnisse) 26
17.5 Die Überwachungspflicht (Kontrollpflicht des Unternehmers) 27
17.6 Part 2: Rechtssichere Formulierung einer Mängelliste im Prüfbuch 27
17.7 Struktur und Beispiel einer rechtssicheren Mängelliste 28
17.8 Part 1: Textvorlage für die Pflichtenübertragung (Muster) 29
17.9 Part 2: Kriterien für die Einstufung „Gefahr im Verzug“ 30

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

1. Die Sicherheitsnorm EN ISO 11161:2010 - Sicherheit von Maschinen – Integrierte Fertigungssysteme (IMS– Integrated Manufacturing System)

1.1 Kurze Einführung in die Norm und Erläuterung des Begriffs IMS:

Die Maschinenrichtlinie definiert in ihrem Anwendungsbereich neben Einzelmaschinen auch eine «Gesamtheit von Maschinen, die so angeordnet und betätigt werden, damit sie als Gesamtheit funktionieren», sogenannte Maschinenanlagen.

Ein sog. Integriertes Fertigungssystem (IMS – Integrated Manufacturing System) kann in Bezug auf Größe und Komplexität, Produktionstiefe, Integrationsgrad sehr variieren.
Es können vor Ort IT-Systeme und Maschinenanlagen vorhanden sein, die einzubeziehen sind.

1.2 Grundlegende Anforderungen der EN ISO 11161

Seit Januar 2008 ist die Norm EN ISO 11161:2010 - Sicherheit von Maschinen – Integrierte Fertigungssysteme – Grundlegende Anforderungen, im Amtsblatt gelistet. Die Norm enthält sicherheitstechnische Festlegungen für Anlagen.

1.2.1 Ziel der Norm

Integrierte Fertigungssysteme (IMS) können in Bezug auf Größe und Komplexität sehr variieren. Es können unterschiedliche Technologien in sich vereinigt sein, die ein breit gefächertes Fachwissen erfordern. Statt einer bloßen Kombination seiner verschiedenen Bestandteile, sollte ein IMS vielmehr, als eine gänzlich neue und andersartige Maschine betrachtet werden. Der Integrator (= natürliche Person, die ein IMS konstruiert oder zur Verfügung stellt) benötigt die Zusammenarbeit von Fachleuten, die jeder für sich betrachtet über ein Teilwissen der Gesamtheit verfügt. 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.

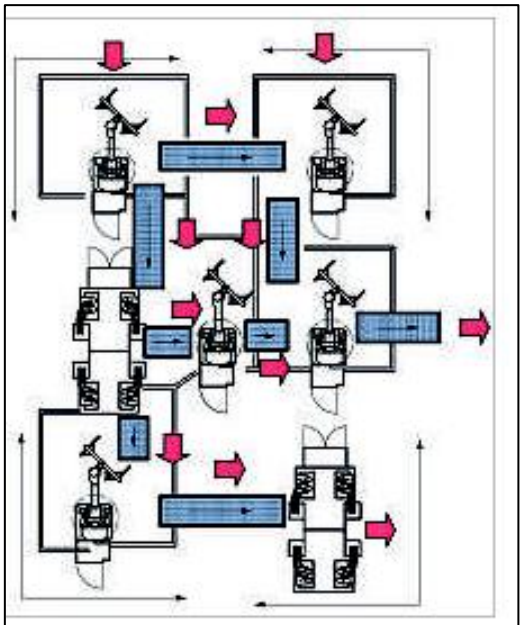
1.2.2 Anwendungsbereich der Norm

IMS enthalten zwei oder mehr miteinander verbundene Maschinen für spezielle Anwendungen, z.B. für die Herstellung von Einzelteilen oder Baugruppen.
Es gibt eine Abgrenzung zu anderen, für das Fertigungssystem anzuwendende Normen.
Die EN ISO 11161 verfolgt nicht die Absicht, Sicherheitsaspekte von einzelnen Maschinen und Ausrüstungen zu behandeln, die in den für diese Maschinen und Ausrüstungen relevanten Normen enthalten sein können.
Deshalb behandelt sie nur die Sicherheitsaspekte, die für die sicherheitsrelevante Verbindung der Maschinen und Bauteile wichtig sind. Werden Maschinen und Ausrüstungen eines IMS getrennt oder einzeln bedient, während die Schutzwirkung der Schutzeinrichtungen, die für den Produktionsbetrieb vorgesehen wurden, zeitweise überbrückt sind oder außer Kraft gesetzt wurden, gelten die für diese Maschinen und Ausrüstung relevanten Sicherheitsnormen.

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

1.2.3 Konkretisierung der Normen zur Risikobeurteilung

Der Prozess der Risikobeurteilung soll nach EN 11161 so durchgeführt werden, wie dies in den Normen EN 12100 beschrieben wird. Konkretisiert wird dies in der Norm EN 11161 allerdings dadurch, dass Beispiele für das Fest-legen der Grenzen des IMS gegeben werden. Besondere Bedeutung erhalten das Bestimmen der Funktionalität und der Arbeitsaufgaben sowie die Fest-legung der Zugangsmöglichkeiten zum IMS. Die Ident-ifizierung von Gefährdungen und die Vorgehensweise bei der Risikoeinschätzung folgt den Normen zur Risiko-beurteilung, aber auch zu diesen Arbeitsschritten gibt es in Checklistenform Anregungen, die die speziellen Gegebenheiten von integrierten Fertigungssystemen berücksichtigen.



Beispiel für integrierte Fertigungssysteme (Auszug aus EN ISO 11161), Bearbeitung und Verteilung der Teile im IMS.

Quelle: DGUV-Schriften-2026

1.3 Der Integrator als natürliche Person und Generalunternehmer

Die Norm legt einen **Integrator** fest.

Er wird definiert als

„natürliche Person, die ein integriertes Fertigungssystem konstruiert, zur Verfügung stellt, fertigen oder montieren lässt und für die Sicherheitsstrategie einschließlich der Schutzmaßnahmen, Steuerungsschnittstellen und Verbindungen des Steuerungssystems verantwortlich ist“.

Weiter wird angemerkt:

„ Jener kann Hersteller, Monteur, Ingenieurbüro oder der Benutzer selbst sein“. Er ist also ein Generalunternehmer.

1.3.1 Abnahmekriterien für integrierte Fertigungssysteme und Roboteranlagen

1.3.2 Allgemeine grundlegende Vereinbarungen

Die Software wird gemeinsam mit den Robotern und der gesamten technischen Anordnung beim Kunden angeliefert. Im Anschluss an die Anlieferung wird der Hersteller folgende Serviceleistungen erbringen, um die Software in Verbindung mit den Robotern

beim Kunden lauffähig zu installieren. Roboter und die dazugehörige Software werden nachfolgend **Gesamtsystem** genannt.

Dazu gehören
- Implementierung der Roboter,
- Schnittstellenanbindung sowie
- Ggf. Projektmanagement.

1.3.3 Kriterien für die Abnahme

Die Kriterien für die Abnahme werden oftmals in verschiedene Kategorien unterteilt. Diese können sein:

- Technische Leistung
- Verfügbarkeitstests der Roboter
- Test des Gesamtsystems (Software + Roboter), der realisierten Einbindung in vor Ort vorhandene Systeme
- Optional: Schulung der Mitarbeitenden durch den Hersteller oder Integrator

Für alle Kategorien werden im Vorfeld Akzeptanzwerte festgelegt. Diese Werte müssen vom System für eine erfolgreiche Abnahme erreicht werden. Auch die **Dauer der Abnahmeschritte** sollte im Vorfeld festgelegt werden. Die gewöhnliche Abnahmedauer beläuft sich zwischen 24 Stunden und 7 Tage.
Dabei wird die **technische Leistung** meistens in Picks pro Stunde sowie in Transporte pro Stunde angegeben. Unabhängig vom zu testenden Use Case kann man die Performance des Systems allerdings auch in UPH (Units per Hour) oder Missionen pro Stunde angeben.

Der Verfügbarkeitstest des Systems wird in Soll-Verfügbarkeit (gewünschtes Resultat) sowie Ist-Verfügbarkeit (aktuelle Leistung) gemessen. Im Vorfeld muss die zu erreichende Verfügbarkeit definiert werden. Die Berechnungen zur Verfügbarkeit des Systems wird in Prozent angegeben. Ein Beispiel: *“Pro Stunde sollte der Roboter maximal 5 Minuten in einem Fehlerstatus befinden. Daraus ergibt sich eine Verfügbarkeit von ~91,6% während der Einsatzzeit des Roboters”.*

Der Test des Gesamtsystems stellt sicher, dass alle Komponenten (auch mit Integration in ein WMS oder ein anderes Software-Tool) sicher funktionieren. Dabei wird auch die Verfügbarkeit und Fehlertoleranz dieser Softwaresysteme gemessen. Sollten Fehler während der Abnahme auftreten, muss geregelt werden, wer diese Fehler löst und in welchem Umfang diese Fehlerbehebung erfolgen kann.

Ein Teil der Abnahme ist die **Schulung der Mitarbeitenden**.

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

2.Die Bestimmung der Grenzen eines Integrierten Fertigungssystems (IMS) in der EN ISO 11161

In der **EN ISO 11161** erfolgt die Festlegung der Grenzen eines Integrierten Fertigungssystems (IMS) auf Basis der übergeordneten Norm zur Risikobeurteilung (**EN ISO 12100**), wird jedoch durch **spezifische Kriterien und praxisnahe Beispiele für verkettete Maschinenanlagen konkretisiert**.
Die Norm verlangt, dass der Integrator den genauen Betrachtungsrahmen des Gesamtsystems absteckt, um die Schnittstellen und daraus resultierende neue Gefährdungen strukturiert zu erfassen. Dies wird über vier wesentliche Dimensionen beschrieben:

2.1 Räumliche Grenzen (Ortsbezogene Grenzen)

- **Physischer Fußabdruck**: Bestimmung des exakten Bereichs, den das Gesamtsystem inklusive aller Einzelmaschinen, Materialfördersysteme und Schutzeinrichtungen einnimmt.
- **Wirkungsbereiche**: Festlegung von Arbeits- und Gefährdungsbereichen nach EN ISO 11161, insbesondere dort, wo sich die Bewegungsräume verschiedener Maschinen (z. B. Roboter und Transportbänder) überschneiden.
- **Zugangspunkte**: Definition aller physischen Schnittstellen, an denen Personen das System für Bedienung, Materialzufuhr oder Wartung betreten können.

2.2 Zeitliche Grenzen (Lebensdauer und Zyklen)

- **Lebensphasen**: Betrachtung der Grenzen von der Installation über den normalen Produktionsbetrieb bis hin zur Fehlersuche, Wartung und Demontage.
- **Verschleiß**: Schätzung der Lebensdauer kritischer Komponenten und der zeitlichen Intervalle für Sicherheitsprüfungen.

2.3 Grenzen der Verwendung (Bestimmungsgemäße Nutzung)

- **Betriebsarten**: Festlegung der zulässigen Betriebsmodi des Gesamtsystems sowie das Verhalten der Anlage, wenn Einzelmaschinen separat oder manuell gesteuert werden.
- **Spezifikationen**: Definition der verarbeiteten Produkte, Werkstoffe, maximalen Abmessungen, Gewichte und der Taktzeiten der verketteten Gesamtanlage.
- **Fehlbedienung**: Vorhersage von vernünftigerweise vorhersehbaren Fehlanwendungen durch das Bedienpersonal.

2.4 Schnittstellen und steuerungstechnische Grenzen

- **Steuerungsgrenzen**: Definition, welche Sicherheitsfunktionen global für das gesamte IMS wirken (z. B. ein übergreifender Not-Halt) und welche autonom auf Ebene der Einzelmaschinen verbleiben.

- **Schnittstellen der Energieversorgung**: Festlegung der Grenzen bei gemeinsamen Energiequellen (Pneumatik, Hydraulik, Elektrik) und wie Energie im Gefahrfall sicher systemweit oder zonenweise getrennt wird.
- Die Umsetzung des **Zonenkonzepts** und der **Aufteilung in Aufgabenbereiche (Task Zones)** nach EN ISO 11161 ermöglicht es, ein großes Integriertes Fertigungssystem (IMS) so aufzuteilen, dass bei einer Störung oder Wartung an einer Stelle nicht die gesamte Anlage stillstehen muss.

3. Das Konzept der Aufgabenbereiche (Task Zones)

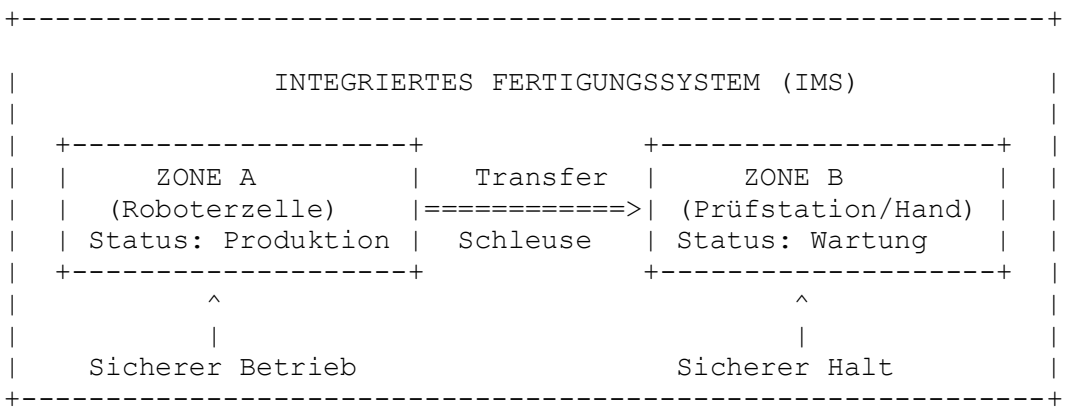
Anstatt die Anlage nur nach Maschinen aufzuteilen, betrachtet die Norm die **konkreten Tätigkeiten des Bedienpersonals**. Ein Aufgabenbereich wird durch den Ort und die Art der Interaktion definiert.

- **Identifikation**: Der Integrator muss für jeden Lebenszyklus der Anlage auflisten, welche Aufgaben (z. B. Material nachladen, Werkzeugwechsel, Störungsbeseitigung) wo anfallen.
- **Gefährdungsanalyse**: Für jede einzelne Zone wird ermittelt, welche Gefährdungen während dieser spezifischen Tätigkeit von den Maschinen in dieser Zone (oder angrenzenden Zonen) ausgehen.
- **Minimierung von Stillständen**: Das Ziel ist es, Schutzmaßnahmen so zu gestalten, dass nur die Zone stillgesetzt oder sicher verlangsamt wird, in der der Mensch arbeitet. Nachbarzonen produzieren sicher weiter.

---

4. Praktische Umsetzung des Zonenkonzepts

Die Aufteilung erfolgt in der Praxis über eine Kombination aus **physischer Trennung** und **sicherheitstechnischer Verschaltung**:



4.1 Festlegung physischer und sensorischer Grenzen

- **Trennende Schutzeinrichtungen**: Zonen werden oft durch Schutzzäune mit verriegelten Türen voneinander abgegrenzt.
- **Optoelektronische Systeme**: Lichtvorhänge oder Laserscanner definieren die Grenzen dort, wo Material fließen muss (z. B. an Übergabestationen). Sie erlauben den Materialtransport, stoppen aber die gefahrbringende Bewegung, sobald ein Mensch hineingreift.

4.2 Steuerungstechnische Hierarchie (Sicherheitszonen)

- **Lokaler vs. Globaler Halt**: Wird in *Zone B* eine Schutztür geöffnet, löst die Sicherheitssteuerung (z. B. ein Sicherheits-Bussystem) nur für die Aktoren dieser Zone einen sicheren Halt aus. Ein übergreifender Not-Halt-Taster stoppt hingegen immer das gesamte IMS.
- **Sichere Zustände**: Für die betroffene Zone wird je nach Aufgabe der passende Zustand gewählt – entweder der komplette Energieausfall (STW / Safe Torque Off) oder eine sicher reduzierte Geschwindigkeit (SLS), falls der Bediener Bewegungen beobachten muss.

4.3 Absicherung der Schnittstellen (Übergabebereiche)

- **Gefahrenübertritt verhindern**: Wenn *Zone A* weiterläuft, während *Zone B* betreten wird, darf keine gefahrbringende Bewegung von *Zone A* in *Zone B* hineinragen.
- **Sperren und Verriegeln**: Roboter in *Zone A* werden steuerungstechnisch (z. B. durch sichere Software-Achsbegrenzungen) daran gehindert, in den Grenzbereich zur *Zone B* zu fahren, solange dort die Schutztür offen ist.
- **Materialschleusen**: Werkstücke werden über Drehtische, Shuttles oder Einlaufschleusen von einer Zone in die nächste übergeben. Die Steuerung prüft per Sensorik, dass sich kein Mensch im Gefahrenbereich der Schleuse befindet, bevor die Übergabe startet.

5. Beispiel aus der Praxis: Verpackungsstraße

In einer verketteten Anlage füllt eine Maschine Flaschen ab (**Zone 1**),
ein Roboter packt sie in Kartons (**Zone 2**)
und ein Palettierer stapelt die Kartons (**Zone 3**).
Muss der Bediener in **Zone 3** eine Palette manuell entnehmen, blockiert ein Lichtvorhang diese Zone.
Der Palettierer stoppt. Der Verpackungsroboter in **Zone 2** arbeitet jedoch weiter und legt Kartons auf ein temporäres Pufferband, bis die Störung in Zone 3 behoben ist.
Die Gesamtanlage läuft ohne Totalausfall weiter.

In einem Integrierten Fertigungssystem (IMS) nach **EN ISO 11161** ist das Not-Halt-System eine der kritischsten Sicherheitsfunktionen.
Da mehrere autarke Maschinen miteinander verkettet sind, darf die Not-Halt-Funktion nicht mehr nur isoliert betrachtet werden.

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

Nachfolgend ist die genaue steuerungstechnische und funktionale Umsetzung des Not-Halt-Konzepts dargestellt:

---

6. Das Not-Halt-System im IMS

Das übergeordnete Ziel der EN ISO 11161 ist es, dass eine Gefährdung an einer Stelle der Anlage sofort und sicher beherrscht werden kann, ohne unbeteiligte Bereiche unnötig zu gefährden oder Folgerisiken (z. B. durch Materialstau) zu erzeugen.

6.1 Die Hierarchie der Not-Halt-Funktion

Die Norm unterscheidet strikt zwischen zwei Ebenen der Not-Halt-Absicherung:

- **Globaler Not-Halt (Gesamtsystem):** Betätigt ein Bediener einen globalen Not-Halt-Taster, müssen **alle** gefahrbringenden Bewegungen des gesamten IMS sofort stillgesetzt werden. Diese Taster sind meist an zentralen Bedienpults oder Hauptzugängen platziert.
- **Lokaler Not-Halt (Zonen-Not-Halt):** Ist die Anlage in logische Sicherheitszonen unterteilt, kann ein Not-Halt-Taster so verschaltet sein, dass er nur die zugehörige Zone (und eventuell direkt gekoppelte Nachbarzonen) stoppt. Dies ist jedoch an strenge Bedingungen geknüpft.

6.2 Kriterien für die Aufteilung in Not-Halt-Zonen

Ein lokaler Not-Halt ist nur dann zulässig, wenn folgende Kriterien der EN ISO 11161 erfüllt sind:

- **Eindeutige Zuordnung:** Für den Bediener muss visuell sofort erkennbar sein, welcher Taster welche Zone abschaltet (z. B. durch klare Kennzeichnung oder räumliche Nähe).
- **Keine Gefahrenübertragung:** Der Stopp einer Zone darf in einer anderen, weiterlaufenden Zone keine neuen Gefahren verursachen (z. B. kein unkontrolliertes Herabfallen von Teilen vom Übergabeband).
- **Sichtverbindung:** Der Bediener muss die Auswirkungszone des Tasters beim Betätigen vollständig einsehen können.

6.3 Steuerungstechnische Verknüpfung

- **Verkettung der Signale:** Die lokalen Sicherheitssteuerungen der Einzelmaschinen müssen signaltechnisch mit der übergeordneten IMS-Sicherheitssteuerung (z. B. via sichere Bussysteme wie PROFIsafe oder Safety over EtherCAT) verbunden sein.
- **Stopp-Kategorien (nach EN ISO 13850):**
  - **Stopp-Kategorie 0:** Unverzögertes Abschalten der Energiezufuhr (ungeregeltes Stillsetzen).

- **Stopp-Kategorie 1:** Gesteuertes Stillsetzen, bei dem die Energie erst abgeschaltet wird, wenn der Stillstand erreicht ist (wichtig für schwere Roboterachsen oder Spindeln, die aktiv gebremst werden müssen).

- **Spannungsfreiheit vs. Sichere Zustände:** Ein Not-Halt bedeutet nicht zwingend, dass die Anlage komplett stromlos ist. Es bedeutet, dass alle *gefahrbringenden Bewegungen* sicher abgeschaltet sind (z. B. über den Zustand *Safe Torque Off / STO* der Antriebe). Ventile für Klemmvorrichtungen müssen oft unter Druck bleiben, damit Werkstücke nicht herunterfallen.

---

7. Die Dokumentationspflichten des Integrators

Da beim IMS verschiedene Maschinen zusammengefügt werden, entsteht rechtlich eine „Gesamtheit von Maschinen“ (oft als „Anlagenverkettung“ bezeichnet). Der **Integrator** übernimmt hierbei die Rolle des Herstellers der Gesamtanlage und trägt die volle Verantwortung.

Die EN ISO 11161 fordert eine lückenlose Dokumentation, die folgende Elemente umfassen muss:

7.1 Die übergreifende Risikobeurteilung (Gesamt-IMS)

Dies ist das wichtigste Dokument. Der Integrator darf nicht einfach die Risikobeurteilungen der Einzelmaschinen abheften. Er muss dokumentieren:

- Welche **neuen Gefährdungen** entstehen an den Schnittstellen (z. B. Materialübergaben, logische Verknüpfungen)?
- Wie wurden die Grenzen des IMS (räumlich, zeitlich, Verwendung) exakt definiert?
- Die Begründung für die Aufteilung der *Task Zones* und des Not-Halt-Konzepts.

7.2 Der Sicherheits-Schnittstellenplan (Interface Specification)

Eine detaillierte Beschreibung aller physischen, energetischen und steuerungstechnischen Schnittstellen:

- **Signalaustausch:** Welche Sicherheitsrelevante Signale (z. B. „Zone bereit“, „Not-Halt aktiv“, „Schutztür offen“) werden wie zwischen den Einzelmaschinen ausgetauscht?
- **Performance Level (PL):** Nachweis nach **EN ISO 13849-1**, dass die kombinierten Sicherheitsfunktionen (z. B. Not-Halt-Kette über drei Maschinen hinweg) den erforderlichen Performance Level (häufig PL d oder PL e) erreichen.

7.3 Die Betriebsanleitung für das Gesamtsystem

Die Betriebsanleitung muss das IMS als Einheit beschreiben. Wesentliche Inhalte sind:

- **Gesamt-Bedienkonzept:** Wie wird die Anlage zentral gestartet, gestoppt und nach einem Not-Halt wieder quittiert (Re-Start-Prozedur)?
- **Verhalten bei Störungen:** Klare Anweisungen, wie der Bediener eine Störung in *Zone A* behebt, während *Zone B* im Automatikbetrieb verbleibt.

- **Restrisiken:** Deutliche Kennzeichnung von Gefahren, die trotz aller Schutzmaßnahmen an den Schnittstellen verbleiben.

7.4 Konformitätserklärung und CE-Kennzeichnung

- **CE-Zeichen für die Gesamtanlage:** Der Integrator stellt eine umfassende **EU-Konformitätserklärung** für das gesamte IMS aus und bringt ein neues, übergeordnetes CE-Typenschild an der Anlage an.
- **Einbauerklärungen:** Die unvollständigen Maschinen oder CE-Erklärungen der Einzelmaschinen werden als Anhang in die technische Dokumentation des IMS integriert.

Das Verfahren zum Wiederanlauf nach einem Not-Halt gehört zu den kritischsten Abläufen im Integrierten Fertigungssystem (IMS), da hierbei die meisten Unfälle durch unerwartete Maschinenbewegungen passieren. Die **EN ISO 11161** verweist hierzu auf die Grundsätze der **EN ISO 13850** (Not-Halt) und **EN ISO 12100**.

Danach folgt die methodische Validierung der Schnittstellen ein.

---

8. Part 1: Das Verfahren zum Wiederanlauf (Reset / Re-Start)

Ein Wiederanlauf darf **niemals** direkt durch das Entriegeln des Not-Halt-Tasters oder das Schließen einer Schutztür ausgelöst werden. Es handelt sich um einen zweistufigen, streng kontrollierten Prozess.

8.1 Die Quittierung (Reset) der Sicherheitsfunktion

- **Entriegeln des Tasters:** Der betätigte Not-Halt-Taster wird mechanisch entriegelt (z. B. durch Drehen oder Ziehen). Dadurch ist das System aber nur *bereit* zur Quittierung, es läuft noch nicht an.
- **Der Reset-Befehl:** Der Bediener muss einen separaten, blau oder weiß gekennzeichneten Reset-Taster betätigen.
- **Platzierung des Reset-Tasters:** Dieser Taster muss zwingend **außerhalb des Gefahrenbereichs** so platziert sein, dass der Bediener die gesamte betroffene Sicherheitszone (Task Zone) vollständig einsehen kann. Er muss optisch prüfen können, dass sich keine Person mehr in der Anlage befindet.
- **Flankensteuerung:** Die Sicherheitssteuerung darf den Reset nur bei einer *fallenden Flanke* (beim Loslassen des Tasters) oder einem dynamischen Signal akzeptieren. Ein dauerhaft blockierter oder festgeklebter Reset-Taster darf das System nicht freischalten.

8.2 Der eigentliche Wiederanlauf (Start / Re-Start)

- **Separater Startbefehl:** Erst wenn die Sicherheitssteuerung durch den Reset „grünes Licht“ gibt, kann über die normalen Bedienkomponenten (z. B. Start-Taster am HMI) die Produktion wieder gestartet werden.

- **Zonenbasierter Re-Start:** Wurde nur eine lokale *Task Zone* gestoppt, wird auch nur diese quittiert und wieder angefahren. Die Nachbarzonen laufen währenddessen ungestört weiter.
- **Sicherheitsgerichtete Sequenz:** Bei komplexen IMS fordert die Norm oft eine bestimmte Einschaltreihenfolge (z. B. erst Hilfsenergien/Pneumatik zuschalten, dann Antriebe in Regelung nehmen, dann Automatik starten), um unkontrollierte Druckluftstöße oder Achsbewegungen zu vermeiden.

---

9. Part 2: Vertiefung der Schnittstellen-Validierung

Die Schnittstellen-Validierung ist die messtechnische und funktionale Überprüfung, ob die Verkettung der Einzelmaschinen sicher ausgeführt wurde. Hierbei passieren in der Praxis die meisten Fehler. Wir vertiefen hierzu die **Validierung der logischen und zeitlichen Signalübertragung (Performance Level & Reaktionszeit)** nach EN ISO 13849-2.

9.1 Das Kernproblem an der Schnittstelle

Wenn Maschine A (z. B. ein Roboter) ein Stopp-Signal an Maschine B (z. B. ein Transportband) sendet, verlässt das Signal den Verantwortungsbereich der ersten Steuerung. Die Validierung muss nachweisen, dass dieser Signalweg fehlersicher und rechtzeitig funktioniert.

9.2 Validierung der funktionalen Logik (Sicherheits-Kreuzvergleich)

Der Integrator muss durch systematische Tests (Black-Box- und White-Box-Tests) nachweisen, dass Querschlüsse, Kabelbrüche oder Softwarefehler an der Schnittstelle nicht zum Sicherheitsverlust führen.

- **Testmethode (Fehlersimulation):** An der physischen Schnittstelle (z. B. einer Klemmenleiste oder einem IO-Link-Modul) wird ein Drahtbruch oder ein Kurzschluss gegen 24V simuliert.
- **Erwartetes Ergebnis:** Die Sicherheitssteuerungen beider Maschinen müssen den Fehler sofort erkennen (Diagnosedeckungsgrad / DC) und das IMS in einen sicheren Zustand (Stopp) überführen. Ein Wiederanlauf muss gesperrt sein, bis der Fehler behoben ist.

9.3 Validierung der Gesamtsicherheitsabstandes (Nachlaufmessung)

Ein kritischer Aspekt an der Schnittstelle ist die **Gesamtreaktionszeit (T)**. Wenn ein Lichtvorhang an der Grenze zwischen zwei Zonen unterbrochen wird, setzt sich eine Kette von Verzögerungen in Gang:

$$\text{Gesamtreaktionszeit }(T)=t_{\text{Sensor}}+t_{\text{Logik A}}+t_{\text{Übertragung}}+t_{\text{Logik B}}+t_{\text{Aktor B (Bremszeit)}}$$

- **Die Übertragungszeit ($t_{\text{Übertragung}}$):** Bei der Validierung wird geprüft, wie lange das Signal über das sichere Netzwerk (z. B. PROFIsafe) von Steuerung A zu Steuerung B benötigt. Diese Zeit muss im Sicherheitsprogramm fest definiert und überwacht werden (sogenannte *F-Time* oder *Watchdog-Zeit*).
- **Die messtechnische Überprüfung:** Der Integrator führt eine **Nachlaufmessung** mit speziellen Messgeräten durch. Dabei wird der Lichtvorhang elektronisch unterbrochen und gleichzeitig über einen Seilzug- oder Lasersensor gemessen, wie viele Millisekunden die

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

mechanische Achse der Nachbarmaschine benötigt, um komplett zum Stillstand zu kommen.

- **Abgleich mit dem Sicherheitsabstand:** Mit dem gemessenen Wert wird nach **EN ISO 13855** berechnet, ob der physische Abstand des Lichtvorhangs zur Gefahrstelle groß genug ist, damit eine hineingreifende Person die Gefahrstelle nicht erreicht, bevor die Maschine steht.

9.4 Protokollierung der Validierung

Jeder dieser Tests muss im **Validierungsbericht** dokumentiert werden:

- Wer hat den Test durchgeführt?
- Welche Seriennummern/Software-Prüfsummen (CRC-Werte) hatten die beteiligten Sicherheitssteuerungen?
- Welches konkrete Fehlerszenario wurde simuliert und wie hat das System reagiert?

Nachfolgend ist ein praxisnahes Beispiel aufgeführt, für ein Testprotokoll zur Schnittstellen-Validierung, strukturiert nach den Vorgaben der **EN ISO 11161** und **EN ISO 13849-2**.
Danach folgt die Vorgehensweise beim Retrofit von Bestandsmaschinen.

---

10. Part 1: Beispiel für ein Validierungs-Testprotokoll

Dieses Protokoll dokumentiert den Test der sicherheitsgerichteten Schnittstelle zwischen einer neuen Roboterzelle (**Maschine A**) und einem bestehenden Transportband (**Maschine B**).
Prüfprotokoll zur Schnittstellen-Validierung (Auszug)

Projekt-Daten			
Projektname:	IMS-Erweiterung Linie 4	**Datum der Prüfung:**	10.07.2026
Anlagen-ID:	IMS-2026-L4	**Prüfer:**	Max Mustermann (Safety Eng.)
Schnittstelle:	X32 (Sicherheitskopplung)	**Normenbasis:**	EN ISO 11161, EN ISO 13849-2

10.1 Systemkonfiguration & Softwarestände

- **Steuerung Maschine A (Roboter):** Siemens CPU 1515F (Firmware V3.1) // **CRC-Prüfsumme F-Programm:** `0x4F8A_2B31`
- **Steuerung Maschine B (Band):** Allen-Bradley GuardLogix 5580 // **CRC-Prüfsumme F-Programm:** `0x9E11_FF02`
- **Kopplungsart:** Physische zweikanalige 24V-Verdrahtung über Sicherheitsrelais (kein Bus)
- **Geforderter Performance Level (PLr): PL d, Kategorie 3**

10.2 Durchführung der funktionalen und Fehlersimulations-Tests

Test-ID	Testbeschreibung / Fehlerszenario	Erwartete Reaktion (Soll)	Tatsächliche Reaktion (Ist)	Status (i.O. / n.i.O.)
T-IF-01	**Funktionstest:** Betätigung Not-Halt-Taster an Maschine A während Automatikbetrieb.	Maschine A stoppt sofort (Stop-Kat 0). Signal an Maschine B wird unterbrochen. Maschine B stoppt verzögert (Stop-Kat 1).	Wie erwartet. Roboter stoppt (STO). Transportband bremst rampegesteuert bis Stillstand.	**i.O.**
T-IF-02	**Drahtbruch Kanal 1:** Abklemmen der Ader für Kanal 1 (Signal „Roboter bereit“) an Schnittstellenklemmleiste X32:1.	Beide Steuerungen müssen den Kanalfehler erkennen. Sicherer Stopp beider Maschinen. Wiederanlauf gesperrt.	Wie erwartet. Sicherheitsrelais meldet Symmetriefehler. Maschinen stoppen. Reset nicht möglich.	**i.O.**
T-IF-03	**Querschluss-Test:** Physisches Brücken von Kanal 1 (X32:1) gegen Fremdeinspeisung +24V DC.	Die Kurzschlussfestigkeit/Taktsignalauswertung muss ansprechen. Sofortige Abschaltung der Ausgänge.	Wie erwartet. Fehlermeldung „Kurzschluss gegen P“ im Diagnosepuffer. Anlage stoppt sicher.	**i.O.**
T-IF-04	**Re-Start-Sperre:** Schließen der Schutztür an Maschine A ohne Betätigung des Reset-Tasters.	Antriebe dürfen nicht automatisch anlaufen. Sicherheitskette bleibt offen.	Wie erwartet. Sicherheitsrelais verbleibt im Zustand „gesperrt“. Keine Bewegung.	**i.O.**

10.3 Messtechnische Überprüfung (Nachlaufmessung nach EN ISO 13855)

- **Gefahrbringende Bewegung:** Einlaufwalze Transportband (Maschine B).
- **Auslöser:** Lichtvorhang an der Zonengrenze (Sensor `B1`).
- **Gemessene Gesamthemmzeit (\(T\)): 340 ms** (inkl. 80 ms Bremszeit des Bandes).
- **Erforderlicher Sicherheitsabstand (berechnet):** \(S = 1600 \times 0,34\,\text{s} + 250\,\text{mm} = \mathbf{794\,\text{mm}}\).
- **Tatsächlicher physischer Abstand an der Anlage: 920 mm**.
- **Ergebnis:** Der Sicherheitsabstand ist ausreichend. (**i.O.**)

Unterschrift Prüfer: *M. Mustermann*

11. Part 2: Retrofit von Bestandsmaschinen ohne moderne Netzwerkschnittstelle

Wenn der Integrator eine ältere Maschine (z. B. Baujahr 1994, Relaissteuerung, kein Profisafe/EtherCAT) in ein modernes IMS einbinden muss, steht er vor der Herausforderung, die Signale **fehlersicher und ohne Zeitverlust** zu übertragen. Die EN ISO 11161 fordert hier eine methodische Vorgehensweise:

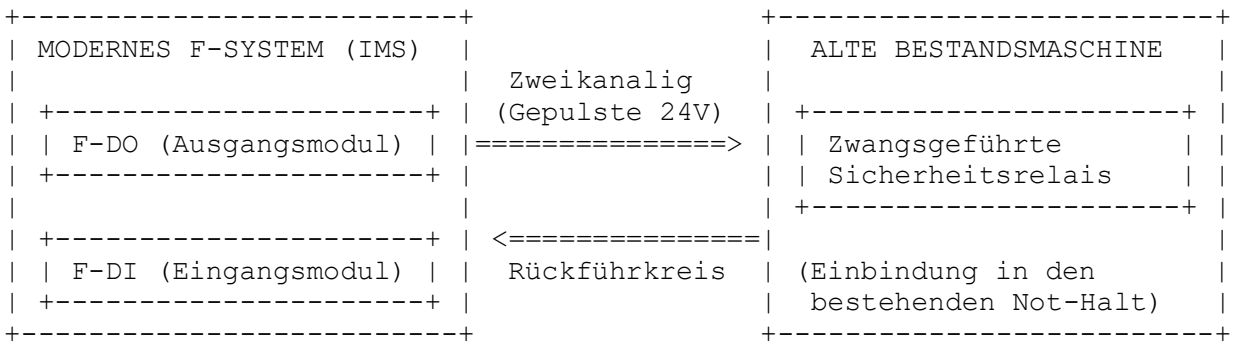
11.1 Bestandsaufnahme und Wesentliche Veränderung prüfen

Bevor technisch eingegriffen wird, muss geklärt werden, ob die Einbindung in das IMS eine **„wesentliche Veränderung“** der Bestandsmaschine nach dem Produktsicherheitsrecht darstellt.

- Wenn durch die Verkettung neue Gefahren entstehen, die die alte Maschine allein nicht absichern kann, wird sie rechtlich, wie eine Neumaschine behandelt. Der Integrator muss für sie (im Rahmen der Gesamtanlage) eine neue CE-Zertifizierung durchführen.

11.2 Technische Umsetzung der Kopplung (Hardware-Retrofit)

Da keine Datenbits übertragen werden können, erfolgt die Kopplung hartverdrahtet über **potenzialfreie Kontakte**:



- **Zwangsgeführte Relais:** Es werden Koppelrelais mit zwangsgeführten Kontakten (nach EN 61810-3) zwischengeschaltet. Nur diese garantieren, dass ein Verschweißen eines Kontakts im Rückführkreis der Sicherheitssteuerung erkannt wird.
- **Taktung gegen Querschluss:** Die 24V-Signale, die zur alten Maschine gesendet werden, werden von der modernen F-SPS mit einem **Taktsignal (Pulse)** hinterlegt. So wird verhindert, dass ein simpler Kabelschaden (Drahtbruch oder Brücke gegen Fremd-24V) als Dauersignal „Sicher“ interpretiert wird.
- **Eingriff in den alten Not-Halt-Kreis:** Die Kontakte des neuen Koppelrelais werden physisch in Reihe in den bestehenden, analogen Not-Halt-Schandkreis der

Bestandsmaschine eingeschleift. Fällt das IMS aus, unterbricht das Relais den Kreis der alten Maschine.

11.3 Das Problem der Bremswege und Nachlaufzeiten

Alte Maschinen besitzen oft keine modernen Frequenzumrichter mit sicheren Bremsrampen (SS1) oder sicherer Drehmomentabschaltung (STO). Beim Abschalten der Energie trudeln sie unkontrolliert aus.

- **Lösung:** Der Integrator muss entweder eine **mechanische Bremse nachrüsten** oder den Zugang zu dieser Zone über eine **Zuhaltung (Schutztürverriegelung)** absichern. Die Tür öffnet sich dann erst nach Ablauf einer definierten Zeitsteuerung (Zeit-Relais), wenn die Bestandsmaschine nachweislich stillsteht.

Nachfolgend ist die technische Umsetzung dargestellt, für die Einbindung einer modernen Sicherheitssteuerung in den analogen Not-Halt-Kreis einer Bestandsmaschine.

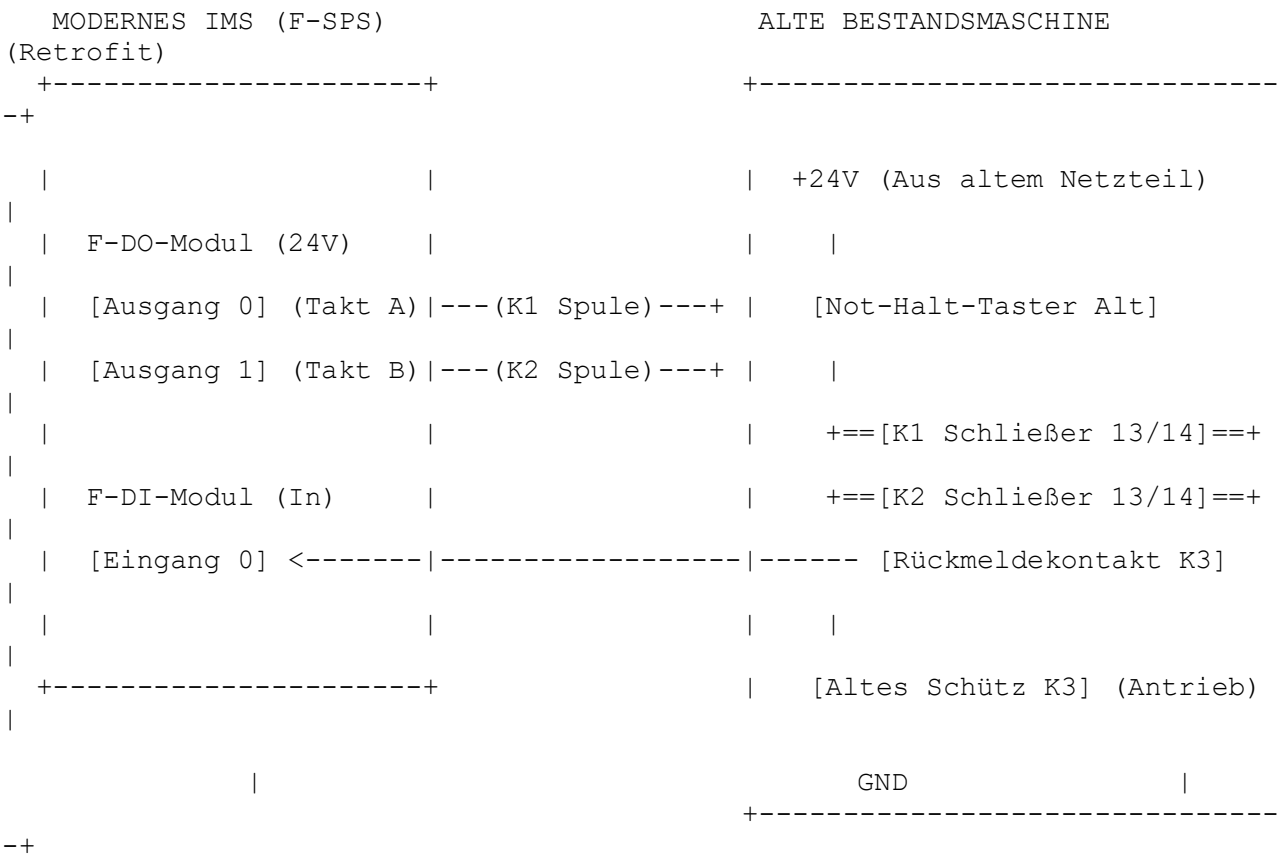
Danach folgen die organisatorischen Maßnahmen für gemischte Anlagen.

---

12. Part 1: Schaltbeispiel für die analoge Not-Halt-Einbindung

Das Ziel ist es, dass das moderne IMS die Bestandsmaschine im Notfall sicher abschalten kann, und umgekehrt die Bestandsmaschine ihren Status an das IMS meldet. Dies wird über **zwangsgeführte Sicherheitsrelais (Kopplungsrelais)** realisiert, um den geforderten Performance Level (meist PL d) zu erreichen.

12.1 Prinzip Skizze der Schaltung



12.2 Funktionsweise der Schaltung

1. **Sicherer Ausgang des IMS (F-DO):** Die moderne Sicherheits-SPS steuert zwei separate Koppelrelais (`K1` und `K2`) an. Die Ausgänge führen eine **Taktung (Muting/Prüfpulse)** aus. Erkennt die F-SPS, dass ein Signal trotz Taktung dauerhaft auf 24V liegt (z. B. durch einen Querschluss im Kabelweg), schaltet sie sofort ab.
2. **Reihenschaltung im alten Sicherheitskreis:** Die Schließerkontakte (NO) von `K1` und `K2` werden **in Reihe** mit den bestehenden Not-Halt-Tastern der Bestandsmaschine verdrahtet.
    - *Normalbetrieb:* Das IMS ist fehlerfrei \(\rightarrow \) `K1` und `K2` sind angezogen \(\rightarrow \) Kontakte geschlossen \(\rightarrow \) Die Bestandsmaschine kann laufen.
    - *Not-Halt im IMS:* `K1` und `K2` fallen ab \(\rightarrow \) Kontakte öffnen \(\rightarrow \) Der Sicherheitskreis der Bestandsmaschine wird unterbrochen \(\rightarrow \) Das alte Hauptschütz (`K3`) fällt ab.
3. **Der Rückführkreis (EDM - External Device Monitoring):** Ein Hilfskontakt (Öffner / NC) des alten Schützes `K3` wird zurück auf einen sicheren Eingang (F-DI) des IMS geführt. Das IMS prüft vor jedem Start, ob `K3` wirklich abgefallen war. Sowie ein Kontakt verschweißt, verweigert das IMS den nächsten Anlauf.

13. Part 2: Organisatorische Maßnahmen (Schulung der Bediener)

Bei „gemischten Anlagen“ (Kombination aus modernen Touch-Panels und alten Relais-Bedienpulten) ist das Risiko für Fehlbedienungen besonders hoch. Die **EN ISO 11161** fordert daher neben den technischen Schutzmaßnahmen ein strenges Konzept für die Schulung und Organisation.

13.1 Kennzeichnung und visuelle Führung (Das größte Risiko minimieren)

- **Eindeutigkeit der Not-Halt-Taster:** Bediener müssen im Bruchteil einer Sekunde wissen, welcher Taster was stoppt.
    - Ein Not-Halt-Taster an der alten Maschine, der nun die *gesamte* Anlage (IMS) stoppt, muss deutlich mit einem Schild „Zentraler Not-Halt“ gekennzeichnet werden.
    - Taster, die nur lokal wirken, müssen farblich abgegrenzt oder mit Zonenplänen (z. B. „Stoppt nur Zone B“) direkt am Taster versehen werden.
- **Inaktive Taster abdecken:** Befindet sich eine Bestandsmaschine im Wartungsmodus und ist steuerungstechnisch komplett vom IMS getrennt, müssen deren Not-Halt-Taster abgedeckt werden (z. B. mit gelben Klappkappen), damit Helfer im Notfall nicht auf einen wirkungslosen Taster drücken.

13.2 Spezifische Schulungsinhalte für gemischte Anlagen

Die Unterweisung der Bediener und des Instandhaltungspersonals muss folgende Besonderheiten abdecken:

- **Das asymmetrische Stopp-Verhalten:** Die Bediener müssen wissen, dass die Maschinen unterschiedlich schnell stoppen. Während der neue Roboter per CSS (Safe Stop) in 200 ms steht, trudelt die alte Drehmaschine vielleicht noch 3 Sekunden aus.
- **Die Re-Start-Logik:** Bei alten Maschinen reichte oft ein Ziehen des Pilztasters und das Drücken von „Start“. Im IMS müssen die Bediener geschult werden, dass immer zuerst der **blaue/weiße Reset-Taster der Zone** mit freier Sicht in den Gefahrenbereich gedrückt werden muss, bevor die Anlage am Hauptpult gestartet werden kann.
- **Verhalten bei Systemausfall (Schnittstellenfehler):** Wenn die Kopplung (siehe Schaltbeispiel oben) einen Fehler erkennt, gehen beide Maschinen in den Stopp. Die Bediener müssen geschult werden, dass eine Fehlermeldung an der neuen Anlage (z. B. „Schnittstellenfehler Bestandsmaschine“) die Ursache in der alten Verkabelung oder einem hängenden alten Schütz haben kann.

13.3 Organisatorische Absicherung bei Wartung (LOTO - Lockout/Tagout)

Da die alte Maschine oft über eine eigene, separate Energieeinspeisung (Hauptschalter) verfügt, reicht es bei Wartungsarbeiten nicht aus, nur das IMS abzuschalten.

- **Vorschrift:** Es muss eine spezifische **Arbeitsanweisung (SOP)** erstellt werden. Diese legt fest, dass bei Arbeiten an der Schnittstelle *beide* Hauptschalter (IMS und Bestandsmaschine) mit persönlichen Vorhängeschlössern gegen Wiedereinschalten gesichert werden müssen.

14. Praxisbeispiel: Betriebsanweisung (SOP) für den Fehlerfall

Hier ist ein konkretes Praxisbeispiel für eine **Standardarbeitsanweisung (SOP - Standard Operating Procedure)** im Fehlerfall. Sie ist speziell für eine gemischte Anlage (modernes IMS gekoppelt mit einer analogen Bestandsmaschine via Sicherheitsrelais) konzipiert und dient als Dokumentation für die Pflichten des Betreibers nach **EN ISO 11161**.

14.1 Standardarbeitsanweisung (SOP) – Sicherheits-Schnittstellenfehler

Dokumenten-ID: SOP-IMS-ERR-04
Gültig ab: 10.07.2026
Anlage: IMS-Verpackungslinie 4 (Haupt-SPS & Retrofit-Kartonierer)
Zielgruppe: Anlagenbediener, Maschinenführer, Instandhaltungspersonal

14.2 Situationsbeschreibung (Wann gilt diese SOP?)

Diese SOP tritt in Kraft, wenn das Integrierte Fertigungssystem (IMS) unerwartet stoppt und am Hauptbedienpanel (HMI) die folgende Fehlermeldung angezeigt wird:

„Fehler Code E-702: Sicherheits-Schnittstellenfehler zu Bestandsmaschine M4 (Kartonierer) – Zeitüberschreitung / Kanalfehler im Rückführkreis.“

Auswirkung: Das gesamte IMS (inklusive des Roboters) geht in den sicheren Zustand (Safe Torque Off - STO). Die analoge Bestandsmaschine M4 wird über die Koppelrelais zwangsabgeschaltet. Ein normaler Wiederanlauf ist blockiert.

14.3 Sofortmaßnahmen für den Anlagenbediener

Schritt 1: Visuelle Kontrolle der Gesamtanlage

- Prüfen Sie, ob Personen im Gefahrenbereich der Roboterzelle oder des Kartonierers M4 stehen.
- Prüfen Sie, ob ein Not-Halt-Taster gedrückt wurde (auch an der alten Maschine M4).
- **Schritt 2: Lokalisierung des Fehlers**
- Gehen Sie zum analogen Schaltschrank der Bestandsmaschine M4.
- Prüfen Sie die Meldeleuchten am Koppelgehäuse (neben dem alten Bedienpult):
    - **LED „K1/K2 OK“ (Grün) AUS:** Der Fehler liegt auf der Seite des IMS (Signal kommt nicht an).

- **LED „Rückführung K3“ (Rot) LEUCHTET:** Der Fehler liegt an der Bestandsmaschine (altes Hauptschütz hängt oder ist verschweißt).

Schritt 3: Erster Quittierungsversuch (Nur bei entriegelten Tastern)

1. Stellen Sie sicher, dass alle mechanischen Not-Halt-Taster entriegelt sind.
2. Drücken Sie den **blauen Reset-Taster „Zone Schnittstelle“** am Schaltschrank des IMS (Position mit voller Einsicht auf die Übergabestation).
3. Bleibt der Fehler bestehen, rufen Sie umgehend die **Instandhaltung (Elektrik)**. Bediener dürfen keine Schaltschränke öffnen!

14.4 Maßnahmen für das Instandhaltungspersonal (Elektro-Fachkraft)

Besteht der Fehler nach dem Reset weiterhin, liegt ein Hardware- oder Synchronisationsfehler an der analogen Schnittstelle vor.

```
[MESSUNG AN DER SCHNITTSTELLE X32]
     |
     +---> Liegen 24V an K1/K2 an?
               |
               +---> JA: Prüfen, ob Schütz K3 mechanisch hängt
(Verschweißung).
               |
               +---> NEIN: Prüfen auf Erdschluss/Querschluss in der Zuleitung
(F-SPS).
```

Schritt 1: Sicherheitsabsicherung (LOTO)

- Vor Messungen an den Schützen: Schalten Sie den Hauptschalter des IMS **UND** den Hauptschalter der Bestandsmaschine M4 aus.
- Sichern Sie beide Schalter mit Ihrem persönlichen Vorhängeschloss gegen Wiedereinschalten (Lockout/Tagout).

Schritt 2: Technische Fehlersuche an der Hardwareschnittstelle

1. **Prüfung des Rückführkreises (EDM):** Öffnen Sie den Schaltschrank von Maschine M4. Prüfen Sie das alte Hauptschütz `K3`. Wenn die Kontakte verschweißt sind, öffnet der Hilfskontakt (NC) nicht mehr. Das IMS erkennt dies als Manipulations- oder Hardwarefehler.
    - *Maßnahme:* Tauschen Sie das Schütz `K3` gegen ein baugleiches Original-Ersatzteil aus.
2. **Prüfung auf Querschluss / Drahtbruch:** Messen Sie an der Schnittstellen-Klemmleiste `X32` die Kanäle 1 und 2 gegen Masse.
    - Liegt ein permanentes 24V-Signal ohne die Taktung der F-SPS an, liegt ein Kabelkurzschluss vor.
    - *Maßnahme:* Kabelverbindung zwischen den Schaltschränken austauschen oder beschädigte Ader isolieren.

14.5 Kontrollierter Wiederanlauf nach Fehlerbehebung

Nachdem die Instandhaltung die Hardware repariert hat, muss die Anlage zwingend in dieser Reihenfolge wieder in Betrieb genommen werden:

1. Werkzeuge und Messgeräte aus beiden Schaltschränken entfernen. Schränke schließen.
2. Vorhängeschlösser (LOTO) an beiden Hauptschaltern entfernen.
3. Erst Hauptschalter M4 (Bestandsmaschine) einschalten, danach Hauptschalter IMS einschalten.
4. **Wichtig:** Die Fachkraft und der Bediener prüfen gemeinsam, dass der Gefahrenbereich komplett leer ist.
5. Drücken des **blauen Reset-Tasters** an der Schnittstellen-Zone (fallende Flanke triggert die Sicherheits-SPS).
6. Die Fehlermeldung am HMI verschwindet. Die Anlage ist wieder im Zustand „Bereit“.
7. Starten der Produktion über das Haupt-HMI.

---

15. Simulation von Fehlerzuständen im Rahmen der wiederkehrenden Prüfungen (UVV / jährliche Sicherheitsprüfung

Im Rahmen der wiederkehrenden Prüfungen (oft als UVV-Prüfung oder jährliche Prüfung nach **Betriebssicherheitsverordnung / EN ISO 11161** bezeichnet) reicht es nicht aus, nur die Not-Halt-Taster zu drücken. Der Prüfer muss **gezielt Fehler in die Sicherheitskette einspeisen**, um zu beweisen, dass die Diagnosefunktionen der Steuerung (der sogenannte *Diagnosedeckungsgrad / DC*) nach wie vor fehlerfrei arbeiten. Diese Prüfungen müssen von einer **befähigten Person** (Safety-Experte oder zertifizierter Prüfer) durchgeführt und in einem Prüfbuch dokumentiert werden.
Die Simulation solcher Fehlerzustände erfolgt in der Praxis über drei methodische Schritte:

15.1 Simulation von Hardware-Fehlern (Fehlereinspeisung)

Um die Ausfallsicherheit (Kategorie 3 oder 4 nach EN ISO 13849-1) an den Schnittstellen des Integrierten Fertigungssystems zu testen, werden physische Defekte simuliert:

- **Simulation eines Drahtbruchs (Einkanaliger Ausfall):**
  - *Durchführung:* An der Schnittstellen-Klemmleiste (z. B. `X32` aus dem vorherigen Beispiel) wird bei laufender Anlage eine einzelne Ader eines Sicherheitskanals abgeklemmt.
  - *Soll-Reaktion:* Die Anlage muss sofort stoppen. Nach dem Wiederanklemmen der Ader darf die Anlage **nicht** anlaufen, wenn nur der Start-Knopf gedrückt wird. Die Steuerung muss den asynchronen Zustand

der beiden Kanäle erkennen und sperren, bis ein bewusster Sicherheits-Reset (blauer Taster) erfolgt.

- **Simulation eines Querschlusses (Fremdeinspeisung):**
  - *Durchführung:* Der Prüfer legt im ausgeschalteten Zustand eine Brücke von einer externen, dauerspannungsführenden 24V-Leitung auf einen der beiden Sicherheitskanäle der Schnittstelle.
  - *Soll-Reaktion:* Beim Einschalten oder spätestens beim Startversuch muss die moderne F-SPS das Fehlen ihres eigenen Taktsignals (Prüfpuls) bemerken. Sie muss eine Fehlermeldung ausgeben („Kurzschluss gegen P“) und den Anlauf der Bestandsmaschine sowie des gesamten IMS blockieren.

15.2 Simulation von hängenden/verschweißten Schützen (EDM-Test)

Besonders bei älteren Bestandsmaschinen (Retrofit) neigen die Leistungsschütze durch Alterung zum Verschweißen der Kontakte. Der Rückführkreis (External Device Monitoring / EDM) muss dies abfangen.

- **Simulation eines Schützfehlers:**
  - *Durchführung:* Da man ein Schütz für den Test nicht physisch beschädigen möchte, wird der Hilfskontakt (Öffner/NC), der die Stellung des Schützes an die F-SPS meldet, an der Klemmleiste dauerhaft überbrückt (Simulation von „Schütz ist dauerhaft abgefallen“) oder abgeklemmt (Simulation von „Schütz hat angezogen und öffnet nicht mehr“).
  - *Soll-Reaktion:* Wenn das IMS einen Startbefehl erhält, vergleicht die Sicherheitssteuerung den Soll-Zustand des Ausgangs mit dem Ist-Zustand des Rückführkreises. Stimmen diese nicht überein, bricht die F-SPS den Startvorgang innerhalb weniger Millisekunden ab und verriegelt das System dauerhaft.

15.3 Prüfung der zeitlichen Bedingungen (Nachlauf- und Divergenzzeiten)

Sicherheitssteuerungen überwachen, wie synchron Signale eingehen. Weichen die Kanäle zeitlich zu weit voneinander ab, liegt ein Fehler vor.

- **Simulation von Zeitüberschreitungen (Divergenz Test):**
  - *Durchführung:* Bei zweikanaligen mechanischen Schutztürschaltern wird ein Kanal künstlich verzögert (z. B. durch langsames, unvollständiges Schließen der Tür oder durch ein simuliertes Zeitrelais im Testaufbau).
  - *Soll-Reaktion:* Überschreitet die Zeitdifferenz zwischen dem Schließen von Kanal 1 und Kanal 2 das in der Software definierte Fenster (Sollwert meist **max. 500 ms**), muss die Steuerung auf Störung schalten.
- **Wiederholung der Nachlaufmessung:**
  - Der Prüfer löst das Not-Halt-System unter Volllast aus und misst mit einem kalibrierten Nachlaufmessgerät, ob die mechanischen Bremsen der Bestandsmaschine oder der Roboterachsen innerhalb der zulässigen Millisekunden (aus der originalen Risikobeurteilung) stoppen. Erhöhte Werte deuten auf mechanischen Bremsenverschleiß hin.

15.4 Wichtige Dokumentationspflicht für den Betreiber

Jeder dieser simulierten Fehlerzustände muss im **UVV-Prüfprotokoll** exakt festgehalten werden. Der Prüfer trägt ein:

1. Welcher Fehler wurde simuliert? (z. B. „Ader X32:1 gelöst“)
2. Hat das System wie vorgeschrieben reagiert? (Ja/Nein)
3. Wurde die Fehlermeldung am HMI korrekt angezeigt? (Ja/Nein)

Möchten Sie wissen, welche **rechtlichen Konsequenzen** es für den Betreiber hat, wenn eine solche jährliche Prüfung Mängel an der IMS-Schnittstelle aufdeckt, oder sollen wir ein anderes Thema im Bereich der **Maschinensicherheit** vertiefen?

15.5 Rechtliche Konsequenzen für den Betreiber, wenn eine solche jährliche Prüfung Mängel an der IMS-Schnittstelle aufdeckt.

Wenn eine wiederkehrende Prüfung (z. B. nach der Betriebssicherheitsverordnung / BetrSichV) erhebliche Mängel an der sicherheitsgerichteten Schnittstelle eines Integrierten Fertigungssystems (IMS) aufdeckt, hat dies für den Betreiber **unmittelbare rechtliche und betriebliche Konsequenzen**.
Im deutschen und europäischen Recht gilt das Prinzip:
Der Betreiber ist für den sicheren Betrieb der Arbeitsmittel verantwortlich.
Er kann diese Verantwortung im laufenden Betrieb nicht mehr auf den damaligen Hersteller oder Integrator abwälzen.

Die Konsequenzen gliedern sich in drei Stufen:

1. Unmittelbare betriebsrechtliche Konsequenzen

- **Stilllegungspflicht bei „erheblichen Mängeln“**: Stellt der Prüfer fest, dass die Schnittstelle fehlerhaft ist (z. B. weil ein Not-Halt-Signal nicht an die Bestandsmaschine übertragen wird oder ein Schütz verschweißt ist und der Rückführkreis versagt), darf die Anlage **nicht weiterbetrieben werden**. Der Prüfer ist verpflichtet, dies im Protokoll zu vermerken.
- **Entzug der Betriebserlaubnis**: Der Betreiber muss die betroffene Zone oder das gesamte IMS sofort stilllegen (Sperrung der Anlage). Ein Weiterbetrieb mit defekter Sicherheitseinrichtung ist eine bewusste Missachtung der BetrSichV (§ 4 „Anforderungen an die Bereitstellung und Benutzung von Arbeitsmitteln“).

2. Ordnungswidrigkeiten und Strafrecht (Präventiv – auch ohne Unfall!)

Schon das bloße Betreiben einer mangelhaften Anlage ohne Unfallfolge kann geahndet werden:

- **Bußgelder**: Nach § 22 BetrSichV i.V.m. § 25 Arbeitsschutzgesetz (ArbSchG) können Bußgelder von **bis zu 30.000 Euro** gegen das Unternehmen oder die verantwortliche Führungskraft (z. B. den Produktionsleiter oder Geschäftsführer) verhängt werden.
- **Straftatbestand bei Vorsatz**: Werden Mängel im Prüfbericht ignoriert und die Mitarbeiter wissentlich an der unsicheren Anlage weiterbeschäftigt, wandelt sich die Ordnungswidrigkeit nach § 26 ArbSchG in eine **Straftat**. Hier drohen Geldstrafen oder Freiheitsstrafen von bis zu einem Jahr für die verantwortlichen Personen.

15.6 Zivil- und strafrechtliche Konsequenzen im Falle eines Unfalls

Kommt es aufgrund des ignorierten Schnittstellenmangels zu einem Personenunfall, greift das volle Spektrum des Straf- und Haftungsrechts:

- **Strafverfahren wegen fahrlässiger Körperverletzung oder Tötung**: Die Staatsanwaltschaft ermittelt direkt gegen die im Prüfbericht genannten Verantwortlichen (Geschäftsführung, Sicherheitsingenieur, Instandhaltungsleiter). Es wird geprüft, wer vom Mangel wusste und den Betrieb nicht gestoppt hat (§ 222, § 229 StGB).
- **Regressansprüche der Berufsgenossenschaft (BG)**: Die gesetzliche Unfallversicherung zahlt zwar zunächst die Behandlungskosten des verunfallten Mitarbeiters. Bei *grober Fahrlässigkeit* (und das Ignorieren eines UVV-Mängelberichts gilt juristisch als solche) fordert die BG jedoch die **gesamten Heilungs- und Rentenkosten vom Betreiber bzw. den verantwortlichen Personen persönlich zurück** (Regress nach § 110 SGB VII). Dies kann in die Millionenhöhe gehen.
- **Zivilrechtliche Haftung (Schadensersatz)**: Der verunfallte Mitarbeiter oder dessen Angehörige können Schmerzensgeldansprüche geltend machen.

---

16. Das korrekte Vorgehen für den Betreiber bei Mängeln

Um diesen Konsequenzen zu entgehen, muss der Betreiber bei der Entdeckung von Mängeln ein standardisiertes Protokoll einhalten:

1. **Sofortige Sperrung**: Anlage abschalten und gegen Wiedereinschalten sichern (LOTO).
2. **Fristsetzung zur Behebung**: Einteilung der Mängel in *„Gefahr im Verzug“* (Sofortstopp) oder *„Geringfügiger Mangel“* (Behebung innerhalb einer kurzen Frist, z. B. 2 Wochen, sofern das Risiko durch organisatorische Maßnahmen vorübergehend minimiert werden kann – bei Sicherheitskopplungen ist dies aber fast nie zulässig).
3. **Nachprüfung**: Nach der Reparatur durch die Instandhaltung oder einen externen Dienstleister muss eine dokumentierte Nachprüfung der Schnittstelle erfolgen, bevor die Anlage wieder für die Produktion freigegeben wird. Möchten Sie wissen, wie der Betreiber die **Verantwortung innerhalb des Unternehmens** (z. B. durch eine schriftliche Pflichtenübertragung auf den Produktionsleiter) rechtssicher delegieren kann, oder interessiert Sie, wie eine **Mängelliste im Prüfbuch** rechtssicher formuliert sein muss?

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

17. Die rechtssichere Pflichtenübertragung (Delegation)

Beschreibung der Möglichkeiten für den Betreiber, die Verantwortung innerhalb des Unternehmens (z. B. durch eine schriftliche Pflichtenübertragung auf den Produktionsleiter) rechtssicher zu delegieren.

Die rechtssichere Delegation von Unternehmerpflichten ist das zentrale Werkzeug für die Geschäftsführung, um die persönliche straf- und zivilrechtliche Haftung im Bereich der Maschinensicherheit zu steuern.

Nachfolgend ist die genaue Vorgehensweise zur Pflichtenübertragung dargestellt, gefolgt von der Struktur einer rechtssicheren Mängelliste.

17.1 Part 1: Die rechtssichere Pflichtenübertragung (Delegation)

Nach **§ 13 Abs. 2 Arbeitsschutzgesetz (ArbSchG)** und **§ 9 Abs. 2 Gesetz über Ordnungswidrigkeiten (OWiG)** kann der Betreiber (Vorstand/Geschäftsführung) Personen ermächtigen, Aufgaben des Arbeitsschutzes in eigener Verantwortung wahrzunehmen. Eine solche Delegation ist jedoch nur dann rechtssicher, wenn sie die **„Vier Säulen der Delegation“** erfüllt:

17.2 Form und Inhalt der Übertragung

Die Pflichtenübertragung muss **zwingend schriftlich** erfolgen und von beiden Parteien unterzeichnet werden. Eine mündliche Absprache ist im Ernstfall vor Gericht wertlos. Das Dokument muss den Aufgabenbereich präzise beschreiben. Pauschale Formulierungen wie „*Herr X ist für die Sicherheit der Linie 4 zuständig*“ sind unwirksam.

Besser: „Herr X übernimmt die Pflichten des Betreibers zur Sicherstellung der wiederkehrenden Prüfungen gemäß § 14 BetrSichV für die Gesamtanlage IMS-Linie 4.“

17.3 Die Auswahlpflicht (Sorgfältige Auswahl)

Der Betreiber darf Pflichten nur auf Personen übertragen, die **fachlich qualifiziert und persönlich geeignet** sind. Der Produktionsleiter muss das notwendige Fachwissen besitzen, um beispielsweise die Relevanz eines Schnittstellenfehlers überhaupt einschätzen zu können. Ist er ein reiner Betriebswirt ohne technische Qualifikation, ist die Delegation fehlerhaft (Auswahlverschulden des Geschäftsführers).

17.4 Die Ausstattungspflicht (Ressourcen und Befugnisse)

Verantwortung ohne Macht funktioniert rechtlich nicht. Dem Produktionsleiter müssen mit der Übertragung explizit zwei Dinge eingeräumt werden:

- **Finanzielle Mittel:** Ein eigenes Budget, um notwendige Reparaturen an der IMS-Schnittstelle oder Nachlaufmessungen sofort und ohne Rücksprache beauftragen zu können.

- **Weisungsbefugnis / Stilllegungsrecht:** Das vertraglich fixierte Recht, die Anlage bei Gefahr im Verzug (z. B. bei einem defekten Sicherheitsrelais) **sofort stillzulegen**, selbst wenn dadurch Produktionsziele verfehlt werden.

17.5 Die Überwachungspflicht (Kontrollpflicht des Unternehmers)

Die Geschäftsführung ist nach der Delegation *nicht* aus der Verantwortung entlassen. Sie verlagert lediglich ihre *Handlungspflicht* in eine *Kontrollpflicht*. Der Geschäftsführer muss stichprobenartig prüfen, ob der Produktionsleiter seinen Aufgaben nachkommt.

- *Praxis-Tipp:* Einmal im Quartal das Prüfbuch der IMS-Anlagen anfordern und die Unterschriften des Produktionsleiters kontrollieren. Wird dies versäumt, haftet die Geschäftsführung wegen Organisationsverschuldens.

17.6 Part 2: Rechtssichere Formulierung einer Mängelliste im Prüfbuch

Wenn bei der jährlichen Prüfung Mängel an der IMS-Schnittstelle festgestellt werden, muss die Mängelliste so formuliert sein, dass sie **dokumentenfest** ist. Sie dient im Falle eines Unfalls als zentrales Beweismittel für Gerichte und Berufsgenossenschaften.

Eine rechtssichere Mängelliste muss nach dem **„4-W-Prinzip“** aufgebaut sein:

Was ist defekt?

Wogegen verstößt es?

Wie gefährlich ist es?

Wer muss es bis **W**ann tun?

Siehe nachfolgende Mängelliste

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

17.7 Struktur und Beispiel einer rechtssicheren Mängelliste

Prüfpunkt / Ort	Festgestellter Mangel (Was & Wogegen)	Risikoeinstufung / Maßnahme	Frist / Verantwortlich	Erledigt am / Visum
IMS-Linie 4 Schnittstelle X32 (Kopplung zu M4)	**Sicherheitsrelais K1 schaltet bei Not-Halt nicht ab.** Der Rückführkreis (EDM) ist mechanisch überbrückt. Die Einfehlersicherheit nach EN ISO 13849-1 (Kat. 3, PL d) ist nicht mehr gegeben. *Verstoß gegen § 4 & § 14 BetrSichV.*	**Gefahr im Verzug!** Sofortige Sperrung und Stilllegung der Schnittstellen-Zone B. Weiterbetrieb der Gesamtanlage im Automatikmodus untersagt.	**Sofort** Hr. Schmitt (Instandhaltung)	10.07.2026 *M. Schmitt*
Zonengrenze Lichtvorhang B1	**Nachlaufzeit überschritten.** Die gemessene Stoppzeit der Bestandsmaschine M4 beträgt 520 ms statt der projektierten 340 ms. Der Sicherheitsabstand nach EN ISO 13855 ist zu gering. *Verstoß gegen Arbeitsstättenrichtlinie (ASR).*	**Erheblicher Mangel.** Mechanische Bremse der Maschine M4 nachjustieren oder Schutztürzuhaltung nachrüsten. Bis zur Behebung: Zugang mechanisch sperren.	**Innerhalb von 7 Tagen** (bis 17.07.2026) Fr. Weber (Produktion)	14.07.2026 *E. Weber*

Warum diese präzise Formulierung wichtig ist:

- **Klare Risikobewertung:** Durch Begriffe wie „Gefahr im Verzug“ oder „Erheblicher Mangel“ weiß jeder Verantwortliche sofort, ob die Maschine sofort gestoppt werden muss.
- **Eindeutige Normenbeispiele:** Die Nennung der verletzten Normen oder Verordnungen (z. B. BetrSichV) nimmt dem Betreiber die Möglichkeit, den Mangel als „Gefälligkeitsurteil“ des Prüfers abzutun.
- **Frist und Name:** Die Zuordnung zu einer konkreten Person verhindert, dass die Behebung in der Abteilung untergeht. Das Feld „Erledigt am“ mit Visum schließt den rechtlichen Haftungskreis nach der Reparatur.

Nachfolgend ist das rechtssichere Musterdokument aufgeführt, für die Pflichtenübertragung sowie die anschließende rechtliche Definition für den Zustand „Gefahr im Verzug“.

17.8 Part 1: Textvorlage für die Pflichtenübertragung (Muster)

Diese Vorlage können Sie als eigenständiges Dokument auf dem Firmenbriefkopf aufsetzen.

Schriftliche Übertragung von Unternehmerpflichten (Delegation)
gemäß § 13 Abs. 2 Arbeitsschutzgesetz (ArbSchG) und § 9 Abs. 2 Gesetz über Ordnungswidrigkeiten (OWiG)
Zwischen:
Unternehmen: *[Firmenname, Straße, PLZ, Ort]*
Vertreten durch die Geschäftsführung: *[Name des Geschäftsführers]*
– nachfolgend **„Unternehmer“** genannt –
Und:
Mitarbeiter/in: *[Vorname Nachname]*
Funktion: Produktionsleiter / Technische Leitung
– nachfolgend **„Verantwortlicher“** genannt –

§ 1 Übertragener Aufgaben- und Verantwortungsbereich
Dem Verantwortlichen wird hiermit die eigenverantwortliche Wahrnehmung der Betreiberpflichten für den sicheren Betrieb, die Instandhaltung und die wiederkehrenden Sicherheitsprüfungen gemäß Betriebssicherheitsverordnung (BetrSichV) für folgenden Anlagenbereich übertragen:

- **Anlage:** Integriertes Fertigungssystem (IMS) – *[z. B. Verpackungslinie 4 / Kenn-ID: IMS-2026-L4]* inklusive aller verketteten Schnittstellen und Bestandsmaschinen.

§ 2 Konkrete Pflichten und Aufgaben
Die Übertragung umfasst insbesondere folgende Pflichten:

1. **Prüfwesen:** Sicherstellung und Überwachung der Durchführung von regelmäßigen, wiederkehrenden Prüfungen (UVV / BetrSichV) durch befähigte Personen.
2. **Mängelbeseitigung:** Die unverzügliche Veranlassung der Behebung von sicherheitstechnischen Mängeln, die im Rahmen von Prüfungen oder im laufenden Betrieb festgestellt werden.
3. **Unterweisung:** Die Sicherstellung der regelmäßigen, dokumentierten Sicherheitsunterweisung aller Bediener und Instandhalter (insb. bzgl. Zonenkonzept und Not-Halt-System).

§ 3 Befugnisse, Budget und Stilllegungsrecht
Zur Erfüllung dieser Aufgaben wird der Verantwortliche mit folgenden Rechten ausgestattet:

1. **Finanzielle Befugnis:** Der Verantwortliche erhält ein jährliches Budget in Höhe von *[Betrag, z. B. 15.000,–]* EUR zur freien Verfügung für notwendige Sicherheitsreparaturen und Prüfungen.
2. **Weisungs- und Stilllegungsrecht:** Der Verantwortliche besitzt die ausdrückliche Befugnis, die oben genannte Anlage oder Teile davon bei Feststellung von erheblichen Mängeln oder **Gefahr im Verzug sofort stillzulegen**. Wirtschaftliche Produktionsinteressen sind diesem Stilllegungsrecht untergeordnet.

§ 4 Kontrollvorbehalt und Berichtspflicht
Der Verantwortliche berichtet der Geschäftsführung einmal pro *[z. B. Quartal]* schriftlich über den Sicherheitsstatus der Anlage und den Stand der Prüfbucheinträge. Der Unternehmer behält sich das Recht zu unangekündigten Stichprobenkontrollen vor (Überwachungspflicht).

Ort, Datum: _____

Unterschrift Geschäftsführer (Unternehmer) Unterschrift Produktionsleiter (Verantwortlicher)

17.9 Part 2: Kriterien für die Einstufung „Gefahr im Verzug“

Im Arbeitsschutz- und Haftungsrecht ist **„Gefahr im Verzug“** ein unbestimmter Rechtsbegriff, der jedoch durch die Rechtsprechung und die Berufsgenossenschaften (DGUV) sehr präzise eingegrenzt ist.

Ein Mangel **muss** als „Gefahr im Verzug“ eingestuft werden, wenn das **Risiko eines schweren Unfalls unmittelbar bevorsteht und nicht mehr durch den normalen, zeitlichen Ablauf von Reparaturprozessen abgewartet werden kann**.

An einer IMS-Schnittstelle müssen Sie die Einstufung zwingend anhand folgender drei Kriterien vornehmen:

Kriterium 1: Versagen der ersten Sicherheitsebene (Verlust der Redundanz)

- **Definition:** Eine Schutzeinrichtung ist funktionslos oder manipuliert, und es gibt kein zweites technisches System, das den Fehler abfängt.
- **Beispiel IMS:** Das Koppelrelais `K1` der analogen Schnittstelle hat verschweißte Kontakte. Der Roboter würde bei einem Not-Halt an der Bestandsmaschine einfach weiterlaufen. Da hierbei die *Kategorie 3 (Einfehlersicherheit)* komplett aufgehoben ist, besteht **sofortige Lebensgefahr** für den Bediener beim Betreten der Schnittstellen-Zone.

Kriterium 2: Unmittelbare Erreichbarkeit der Gefahrstelle (Sicherheitsabstand)

- **Definition:** Der Schutz vor einer gefährlichen Bewegung ist zeitlich oder räumlich nicht mehr wirksam.
- **Beispiel IMS:** Die Nachlaufmessung ergibt, dass die alte Bestandsmaschine nach dem Auslösen des Lichtvorhangs so lange austrudelt, dass ein Mensch die rotierende Walze physisch erreichen kann, bevor sie steht. Da der Mensch **während der regulären Arbeit** verletzt werden kann, ist dies eine akute Gefahr.

Kriterium 3: Unvorhersehbares oder unkontrolliertes Verhalten (Fehlende Beherrschbarkeit)

- **Definition:** Die Steuerung verliert die Kontrolle über die gefahrbringenden Bewegungen, oder Sicherheitsfunktionen sind unzulässig überbrückt.
- **Beispiel IMS:** Nach einem Not-Halt läuft eine Maschine automatisch wieder an (automatischer Re-Start ohne manuellen Reset-Befehl am blauen Taster). Da dieses Verhalten für den Bediener völlig überraschend kommt, ist ein Unfall extrem wahrscheinlich.

Was bedeutet das für die Praxis?

Sobald einer dieser Zustände im Prüfbuch vermerkt wird, greift die **„Null-Toleranz-Regel“**. Jede Weiterarbeit an dieser Anlage ist ab diesem Moment eine **Vorsatztat** des Verantwortlichen. Die einzige rechtssichere Maßnahme ist das physische Absperren der Anlage (Hauptschalter aus, Schloss vor), bis das Ersatzteil eingebaut und die Funktion neu validiert wurde.

Wiesbaden, den 12.07.2026

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