Berufs Bildung Baden

Fach: Automation

Thema: Funktionale Sicherheit von Maschinensteuerungen

Kapitel: Grundlagen der Maschinensicherheit

Autor: Roman Moser
Version: 1.0

Inhaltsverzeichnis

1. Grundlagen der Maschinensicherheit

Maschinen müssen so gebaut werden, dass Menschen, Tiere und Sachwerte sowie die Umwelt von Schäden geschützt sind. Neben der moralischen Pflicht, die Gesundheit seiner Arbeitnehmer zu schützen und zu bewahren, ist das Thema Maschinensicherheit für den Unternehmer und Maschinenbetreiber aber auch eine wirtschaftliche Frage. Jeder Arbeitsunfall führt zu einem Produktionsausfall und verursacht jährlich hohe Kosten.

Überall wo sich an Maschinen etwas bewegt, besteht grundsätzlich eine Gefahr. Deshalb sind z.B. viele Teile einer Maschine abgedeckt. An manchen Stellen hat es Sensoren, Not-Halt-Schalter, 2-Hand-Bediengeräte, Lichtgitter und vieles mehr.

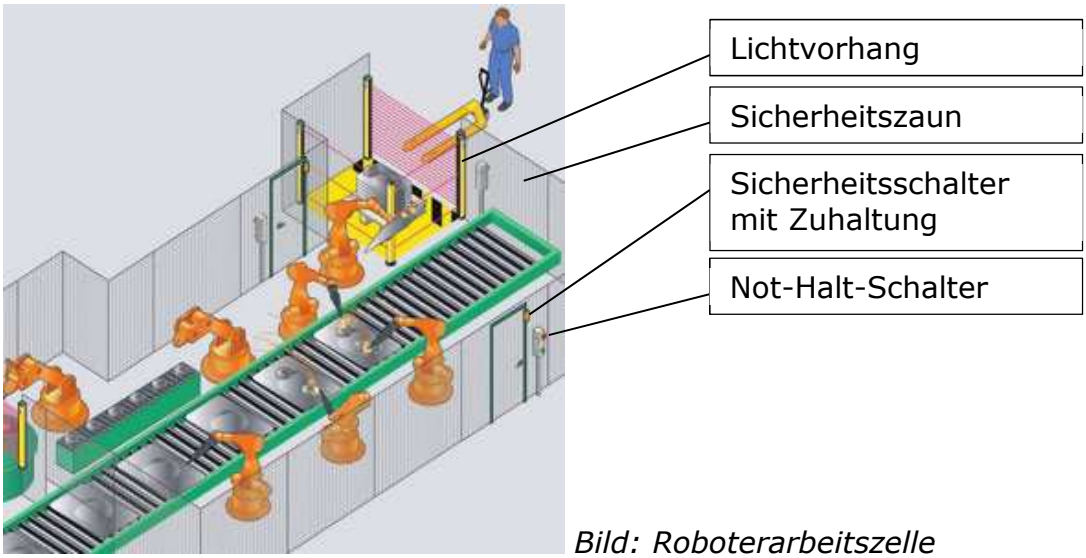


Bild: Roboterarbeitszelle

1.1 Richtlinien und Normen

Wenn ein Hersteller seine Maschinen verkaufen will, müssen verschiedene Richtlinien und Normen eingehalten werden. Bei Fragen betreffend der Sicherheit ist die **Maschinenrichtlinie** (MRL) von grösster Bedeutung. Die MRL gilt in der ganzen EU und auch in der Schweiz.

Eine **Norm** ist nicht zwingend, entspricht aber dem anerkannten Stand der Technik. Wenn man von vorhandenen Normen abweicht, muss die Wirksamkeit der gewählten Lösung bewiesen werden.
Eine **Richtlinie** hingegen muss zwingend eingehalten werden.
Die Maschinenrichtlinie verlangt, dass von Maschinen keine Gefahr ausgehen darf. Da eine 100%ige Sicherheit in der Technik nie garantiert werden kann, ist es das Ziel, die vorhandenen Gefahren durch **Risikoreduzierung** auf ein tolerierbares Restrisiko zu bringen. (→ Download der Maschinenrichtlinien: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:157:0024:0086:DE:PDF)

1.2 1-2-3 Methode

In der internationalen Norm EN ISO 12100-1 „Sicherheit von Maschinen – Grundbegriffe und allgemeine Gestaltungsleitsätze" ist die 1-2-3-Methode definiert, mit welcher die geforderte Sicherheit erreicht werden soll:

1. Schritt: Gefahren vermeiden

Risiko eliminieren und reduzieren durch **konstruktive Massnahmen** während der Planungs- und Entwicklungsphase einer Maschine.

2. Schritt: Gefahren sichern

Risiko reduzieren durch den Einsatz von Sicherheitsprinzipien und sicherheitsbezogenen Geräten.

3. Schritt: Auf Restgefahren hinweisen

Risiko reduzieren durch Ausbildung des Personals und Warnhinweise über die Restrisiken.

1.3 CE-Kennzeichnung

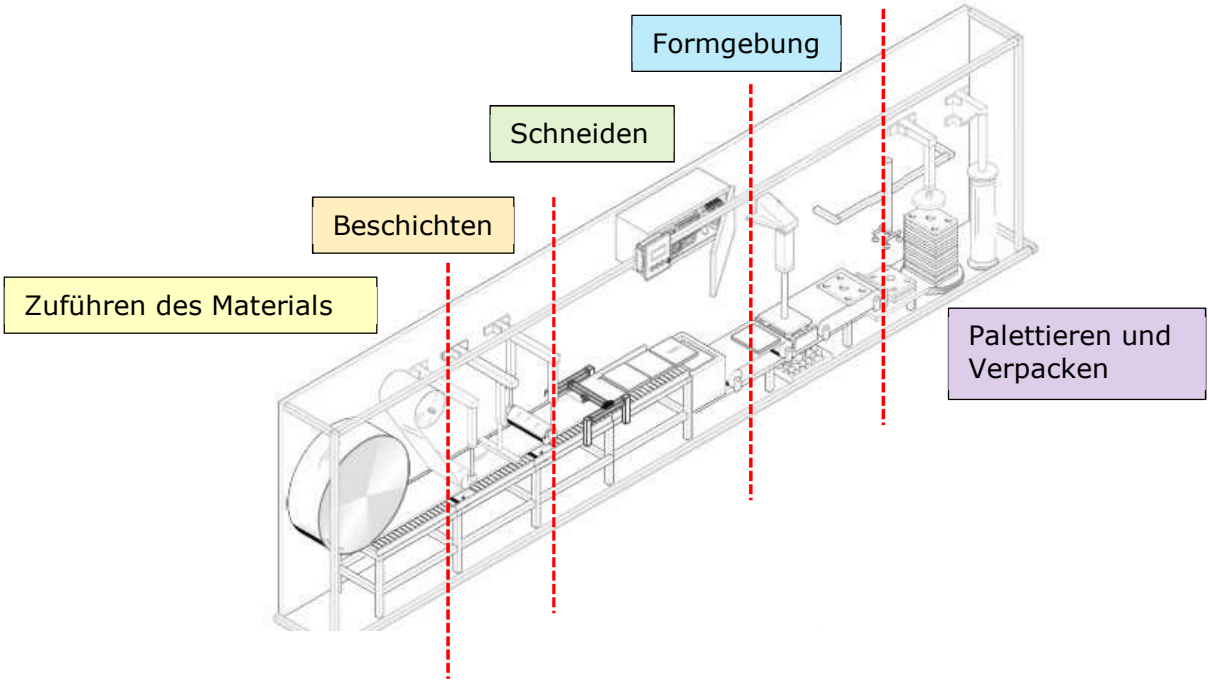
Alle Maschinen, die in Europa auf den Markt gebracht werden, müssen das CE Zeichen tragen. Für viele Maschinen kann der Hersteller dieses Zeichen selber anbringen. **Es bedeutet, dass der Hersteller bestätigt, die Maschine nach den nötigen Normen gebaut zu haben.**

Der Hersteller muss dazu eine **Konformitätserklärung** erstellen. Dies beinhaltet folgende Unterlagen:

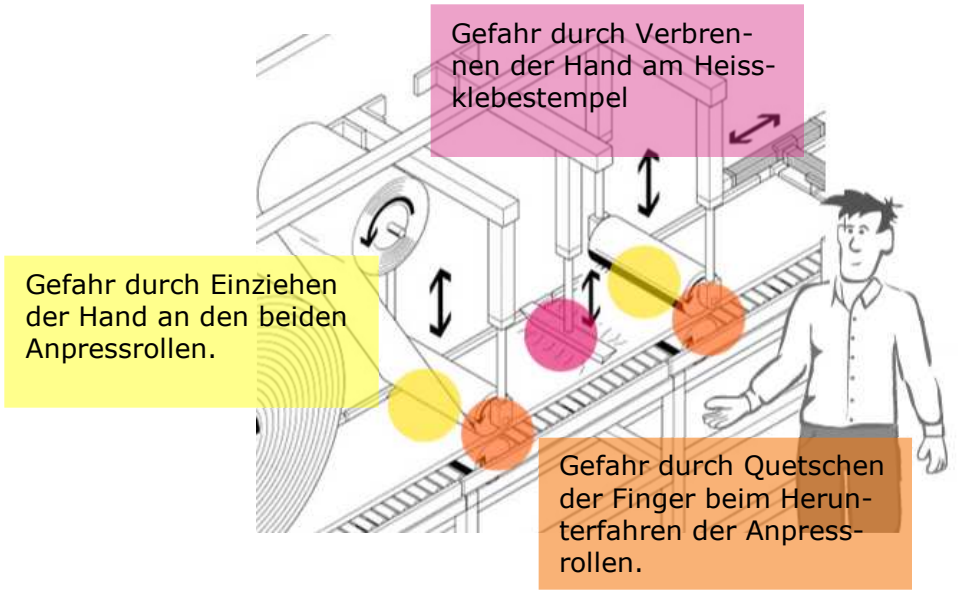
- Risikobeurteilung (=Risikoanalyse und Risikobewertung)
- Bedienungsanleitung
- Technische Dokumentation

Für die **Risikoanalyse** muss man die vorhandene Maschine in Teilfunktionen (Module) aufgliedern und jede einzelne Teilfunktion auf mögliche Gefahren untersuchen. Dazu gehören auch die Aufstellung, Inbetriebnahme, Unterhalt sowie Demontage und Entsorgung!

Beispielbereiche der Risiko- resp. Gefahrenanalyse an einer Industrieanlage welche Schaumstoffpolster für Transportcontainer herstellt:



Für jeden einzelnen Gefahrenbereich müssen alle denkbaren Ereignisse, welche in den verschiedenen Betriebsarten möglich sind, aufgelistet und bewertet werden. Für den Bereich „Beschichten" der obigen Anlage zur Herstellung von Schaumstoffpolstern ergeben sich folgende Gefährdungen:



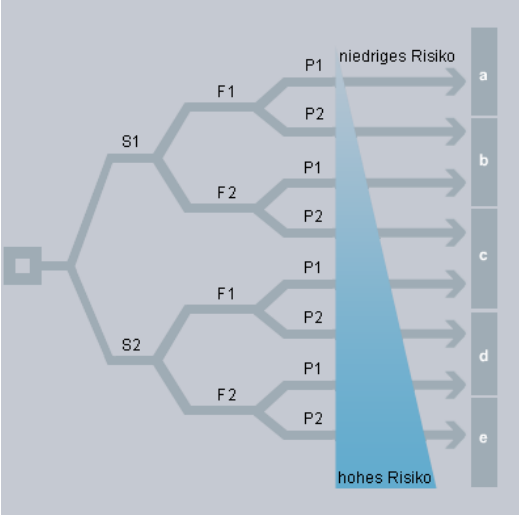
Danach müssen nach der 1-2-3-Methode mögliche Lösungen gesucht werden, welche den Sicherheits- und Gesundheitsanforderungen der Maschinenrichtlinie genügen.

Für die Auslegung der sicherheitsbezogenen Teile von Maschinen können zwei Normen angewendet werden.

– EN ISO 13849-1 (→ Norm für den Maschinenbauer)

– EN 62061 (→ Norm für den Hersteller von Sicherheitskomponenten)

Die **EN ISO 13849-1** gilt für alle Sicherheitsfunktionen (elektrische, mechanische, pneumatische, hydraulische). Die Risikobeurteilung nach dieser Norm stellt man in einem Risikographen dar.



Risikoeinschätzung:
Bestimmung des erforderlichen Performance Levels (PLr) (EN ISO 13849-1)

Zielwert, der mit der Schutzmaßnahme mindestens erreicht werden muss.

S - Schwere der Verletzung
S1: leichte, reversible Verletzung
S2: ernste, irreversible Verletzung oder Tod

F - Häufigkeit und/oder Dauer der Gefährdungsexposition
F1: selten oder weniger häufig und/oder kurz
F2: häufig bis dauernd und/oder lang

P - Möglichkeit der Vermeidung der Gefährdung
P1: möglich unter bestimmten Bedingungen
P2: unmöglich

Ergebnis: Erforderlicher Performance Level

Das Vorgehen ist wie folgt:

1) Die Schwere der Verletzung analysieren (S).
2) Die Häufigkeit oder Dauer der Gefährdung untersuchen (F).
3) Die Möglichkeit der Vermeidung der Gefährdung betrachten (P).

Je nach Gefahrensituation an der Maschine wird aufgrund der getroffenen Entscheidungen der erforderliche „**Performance Level**" **PL a** bis **PL e** definiert. Die einzelnen Performance-Level a bis e definieren die **Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde** für die gesamte Sicherheitskette und somit auch die Anforderungen an die Sicherheitsrelais und die nötige Schaltung.

Beispielwerte:
PL a: 1 Ausfall ab 10 Tausend Stunden
PL e: 1 Ausfall ab 10 Millionen Stunden

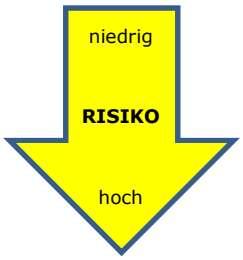
Bereits bei der Vorgängernorm EN 954-1 (bis 2009) wurde das Vorgehen mit dem Risikographen angewandt. Die Sicherheitskategorien waren B, 1, 2, 3 und 4. Es wurde nicht mit Ausfallwahrscheinlichkeiten gearbeitet, sondern mit der Struktur der Schaltung. Wenn man bewährte Schaltungsbeispiele verwendet hat, konnte man „sicher" sein, dass die Sicherheit gewährleistet war ohne Rücksicht auf die Qualität der Bauteile. **Die neue Norm EN ISO 13849-1 ist anspruchsvoller, weil sie die Ausfallwahrscheinlichkeit der ganzen Sicherheitskette (vom Sensor über die Verarbeitung bis zum Aktor) berücksichtigt und somit die Qualität der Geräte und Bauteile enthält.**

Zur Bewertung von sicherheitsbezogenen Maschinensteuerungen kann im Internet unter dem Begriff **SISTEMA** (**Si**cherheit von **Ste**uerungen an **Ma**schinen) ein Software-Assistent heruntergeladen werden.

Die EN 62061 bezieht sich ausschliesslich auf elektrische bzw. elektronische Steuerungssysteme für Sicherheitsaufgaben wie z.B. Sicherheits-SPSen und Sicherheits-Bussysteme. Das erforderliche Sicherheitsniveau wird als „**Safety Integrity-Level**" **SIL** bezeichnet. Man unterscheidet die Stufen **SIL 1, SIL 2 und SIL 3**.

Der Zusammenhang zwischen dem Performance Level (EN ISO 13849-1) und dem Safety Integrity Level (EN 62061) lässt sich wie folgt darstellen:

Performance Level PL	Mittlere Wahrscheinlich-keit eines gefährlichen Ausfalls pro Stunde	Safety Integrity Level SIL
a	$\geq 10^{-5}$ bis $< 10^{-4}$	Keine besonde-ren Sicherheits-anforderungen
b	$\geq 3x10^{-6}$ bis $< 10^{-5}$	1
c	$\geq 10^{-6}$ bis $< 3x10^{-6}$	1
d	$\geq 10^{-7}$ bis $< 10^{-6}$	2
e	$\geq 10^{-8}$ bis $< 10^{-7}$	3



Letztlich führen beide Normen zum Ziel!