ABB Maschinensicherheit Sicherheitsfunktionen nach EN ISO 13849-1 in Maschinen und Anlagen

Power and productivity
for a better world™

Wir entwickeln innovative Produkte und Lösungen zur Sicherheit von Maschinen

Wir machen es Ihnen leicht. In der Fortführung der Tradition von Jokab Safety ist es unsere Zielsetzung, innovative Produkte und Lösungen für die Sicherheit von Maschinen zu entwickeln. Unsere Vision: „Wir wollen für Sie der beste Partner für die Sicherheit Ihrer Maschinen sein". Viele Industriebereiche auf der ganzen Welt haben entdeckt, wie viel leichter es geworden ist, Schutzeinrichtungen und Sicherheitsfunktionen mit Komponenten und Beratung von uns zu bauen.

Erfahrung

Wir haben langjährige Erfahrungen mit der praktischen Anwendung von europäischen Richtlinien und Normen zur Sicherheit von Maschinen, um sowohl die Anforderungen des Gesetzgebers zu erfüllen, sowie auch die von Betreibern von Maschinen und Anlagen zu berücksichtigen. Wir vertreten Schweden in Normungsausschüssen zur Sicherheit von Maschinen, und wir arbeiten täglich mit der praktischen Umsetzung der grundlegenden Sicherheits- und Gesundheitsschutzanforderungen für Konstruktion und Bau von Maschinen. Nutzen Sie unsere Kompetenz für die Ausbildung und Beratung für Risikobeurteilungen nach der Maschinenrichtlinie und Sicherheit in Maschinen durch Sicherheitsfunktionen.

Systeme

Wir liefern alles, von der Lösung zur ausreichenden Risikominderung bis zu kompletten praktischen Umsetzung für einzelne Maschinen oder ganze Fertigungsstraßen. Wir kombinieren Sicherheitsanforderungen mit Produktionsanforderungen zu betriebsoptimalen Lösungen.

Produkte

Wir haben eine komplette Palette von Komponenten für Schutzeinrichtungen, die es leicht machen, Maschinen mit den erforderlichen Maßnahmen zur Risikominderung auszurüsten. Diese innovativen Produkte entwickeln wir kontinuierlich weiter, oft in Zusammenarbeit mit unseren Kunden.

Über Richtlinien und Normen

Wir sind aktiv an der Entwicklung von Normen beteiligt

Richtlinien und Normen zur Sicherheit von Maschinen sind für Hersteller von Maschinen und sicherheitsbezogenen Komponenten von allergrößter Bedeutung. Aus diesem Grund sitzen wir in mehreren internationalen Komitees, die Normen für zum Beispiel Industrieroboter, Schutzeinrichtungen und von sicherheitsbezogenen Teilen von Steuerungen erarbeiten. Aufgrund unserer weitreichenden Erfahrungen haben wir dort die Möglichkeit, darauf hinzuwirken, dass in neuen Normen die Anforderungen an Produktionsfreundlichkeit und maximale Sicherheit berücksichtigt werden. Selbstverständlich geben wir unser Fachwissen im Bereich Normen gern an unsere Kunden weiter.

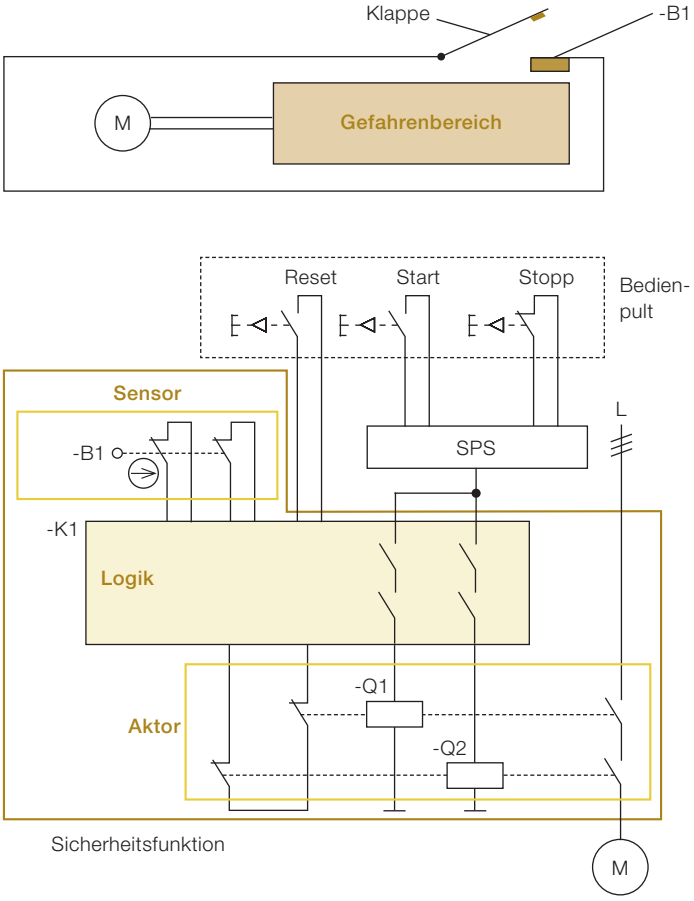
Definitionen in EN ISO 13849-1

PL_r	Der erforderlicher Performance Level PL_r ist ein angewandter Performance Level (PL), um die erforderliche Risikominderung für jede Sicherheitsfunktion zu erreichen.
PL	Der Performance Level PL ist ein diskreter Level, der die Fähigkeit von sicherheitsbezogenen Teilen einer Steuerung spezifiziert, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen.
PFH	(oder PFH_D) Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde.
Kategorie	Einstufung der sicherheitsbezogenen Teile einer Steuerung bezüglich ihres Widerstandes gegen Fehler und ihres nachfolgenden Verhaltens bei einem Fehler, das erreicht wird durch die Struktur der Anordnung der Teile, der Fehlererkennung und/oder ihrer Zuverlässigkeit.
$MTTF_d$	Die mittlere Zeit bis zum gefahrbringenden Ausfall $MTTF_d$ ist der Erwartungswert der mittleren Zeit bis zum gefahrbringenden Ausfall.
DC	Der Diagnosedeckungsgrad DC ist ein Maß für die Wirksamkeit der Diagnose, die bestimmt wird als das Verhältnis der Ausfallrate der bemerkten gefährlichen Ausfälle und Ausfallrate der gesamten gefährlichen Ausfälle einer Komponente.
DC_{avg}	Der durchschnittliche Diagnosedeckungsgrad DC_{avg} ist der Diagnosedeckungsgrad DC einer kompletten Sicherheitsfunktion.
CCF	Unter Ausfall infolge gemeinsamer Ursache CCF versteht man Ausfälle verschiedener Einheiten aufgrund eines einzelnen Ereignisses.
B_{10d}	Anzahl von Zyklen, bis 10 % der mechanischen, pneumatischen oder elektromechanischen Komponenten gefährlich ausgefallen sind.
T_{10d}	Mittlere Zeit bis 10 % der Komponenten gefährlich ausfallen. EN ISO 13849-1 geht von einer Gebrauchsdauer T_M der Komponenten von 20 Jahren aus. Wenn $T_{10d} < T_M$ ist, so muss diese Komponente nach der Zeitdauer T_{10d} bereits ausgetauscht werden.

EN ISO 13849-1 – die Norm für sicherheitsbezogene Teile von Steuerungen

Konstruktion und Bau von Schutzeinrichtungen, die ein ausreichendes Maß zur Risikominderung bieten und dennoch in der Praxis nicht hinderlich sind, erfordern Kenntnisse aus verschiedenen Bereichen. Ein wichtiger Aspekt ist die Konstruktion ausreichend zuverlässiger Sicherheitsfunktionen für die Schutzeinrichtungen. Als Hilfe dazu, für diese Sicherheitsfunktionen die Kategorie der Schaltung mit ihren sicherheitsbezogenen Teilen zu bestimmen und dann darzulegen, dass das ausreichende Maß an Risikominderung erreicht wird, dient Teil 1 der Norm zur Sicherheit von Maschinen EN ISO 13849-1. Eine Anleitung zur Validierung durch Analyse und Prüfung der vorgesehenen Sicherheitsfunktionen, der ausgeführten Kategorien und dem erreichten Performance Level gibt Teil 2 der Norm zur Sicherheit von Maschinen EN ISO 13849-2.

Mit unserer Broschüre möchten wir eine Einführung in die Norm und ihre Anwendung in Verbindung mit unseren Produkten geben. Zunächst machen wir uns mit den Definitionen wichtiger Begriffe in EN ISO 13849-1 vertraut. Da stellt sich als erstes die Frage, was ist eine Sicherheitsfunktion. Das wollen wir am Beispiel einer Bearbeitungsmaschine erläutern:



Die durch ein Gehäuse vollständig geschützte Bearbeitungsmaschine hat eine Klappe, wo zu bearbeitende Teile eingelegt und fertig bearbeitete entnommen werden können. Nach Öffnen der Klappe ist ein Gefahrbereich mit der Möglichkeit schwerer Verletzungen zugänglich; das ist der Bereich, wo gefahrbringende Bewegungen, verursacht durch den Antriebsmotor M bei offener Klappe zugänglich sind. Um diese gefahrbringenden Bewegungen bei offener Klappe zu verhindern, wurde am Beispiel der Bearbeitungsmaschine eine Sicherheitsfunktion derart eingebaut, dass durch einen sich an der Klappe befindlichen Sicherheitsschalter -B1 (Sensor), über das Sicherheitsrelais -K1 (Logik) die beiden Schütze -Q1/-Q2 (Aktor) ausgeschaltet sind. Damit ist ein gefahrloses Hantieren im Gefahrbereich möglich. Falls jetzt bei offener Klappe ein Startbefehl am Bedienpult gegeben werden würde, oder durch andere Signale der SPS oder im Falle eines Fehlers in der SPS ein Einschalten des Motors M herbeigeführt werden wollte, so ist das wegen der Sicherheitsfunktion nicht mehr möglich.

Die Sicherheitsfunktion

Eine Sicherheitsfunktion beginnt also bei einem Sensor, geht über eine Logik und endet bei einem Aktor. Die Aufgabe des Sensors ist es festzustellen, ob die Klappe geöffnet wurde bzw. offen ist. Die Aufgabe des Aktors ist es, eine mögliche Energiezufuhr zum Motor zu blockieren und somit gefahrbringende Bewegungen zu verhindern. Die Aufgabe der Logik besteht darin, die Signale des Sensors auszuwerten und das korrekte Ausschalten der Schütze festzustellen, sowie ein Bereitstellen der Energiezufuhr zum Motor nach Schließen der Klappe erst nach Betätigung des Reset-Tasters zuzulassen oder bei einem Fehler im Sensor oder Aktor die Energiezufuhr grundsätzlich zu verhindern. Bevor jedoch die im Beispiel der Bearbeitungsmaschine gezeigte Schaltung für eine Sicherheitsfunktion entworfen werden kann, muss ermittelt werden, welche Ansprüche an ihre Sicherheitsqualität zu stellen sind, damit einerseits die gesetzlichen Mindestanforderungen an die Sicherheit der Maschine erfüllt werden und andererseits der vorgegebene Kostenrahmen der Maschine eingehalten wird. An eine Sicherheitsfunktion werden also Anforderungen bezüglich ihrer erforderlichen Sicherheitsqualität gestellt. Je schwerer die möglichen Verletzungen im Gefahrbereich bei einem Anlauf des Motors, je häufiger in den Gefahrbereich gegriffen werden muss und je weniger die Möglichkeit zum Vermeiden der Verletzung besteht, umso weniger wahrscheinlich darf der Ausfall der Sicherheitsfunktion sein. Diese erforderliche Sicherheitsqualität für eine Sicherheitsfunktion wird in EN ISO 13849-1 erforderlicher Performance Level PL_r genannt und kann durch eine Risikoeinschätzung mittels eines Risikografs nach EN ISO 13849-1 Anhang A durch 3 Parameter ermittelt werden.

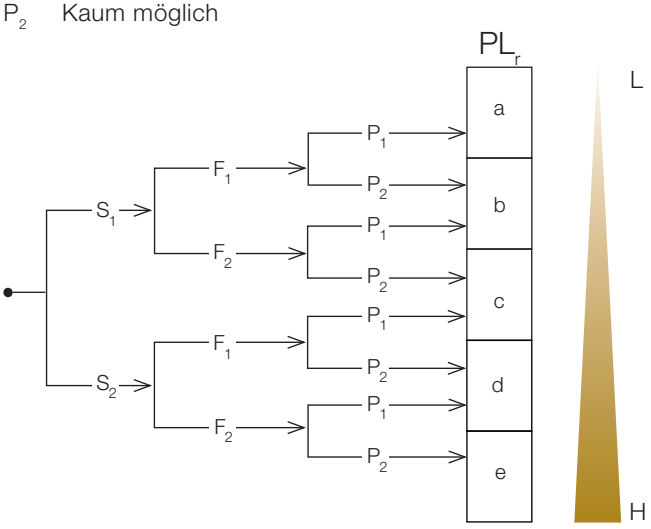
Der erforderliche Performance Level PL_r

Zur Risikoeinschätzung mittels des Risikografs werden die 3 Parameter S, F und P verwendet, und für jeden Parameter gibt es 2 Entscheidungsmöglichkeiten:

S Schwere der Verletzung
S_1 leichte, üblicherweise reversible Verletzung
S_2 schwere, üblicherweise irreversible Verletzung, einschließlich Tod

F Häufigkeit und/oder Dauer der Gefährdungsexposition
F_1 Selten bis weniger häufig und/oder kurze Zeit
F_2 Häufig bis dauernd und/oder lange Zeit

P Möglichkeit zur Vermeidung oder Begrenzung des Schadens
P_1 Möglich unter bestimmten Umständen
P_2 Kaum möglich



H im Risikograf bedeutet einen hohen und L einen niedrigen Beitrag zur Risikominderung. Ist das Ergebnis der Risikoeinschätzung z.B. S_2, F_1 und P_2, so wäre der erforderliche Performance Level PL_r = d, was einem hohen Beitrag zur Risikominderung entspricht. Nun liegt neben den Eigenschaften für die notwendige Sicherheitsfunktion auch der erforderliche Performance Level PL_r für die Sicherheitsfunktion vor und es kann die konstruktive Auslegung der Schaltung erfolgen. Nach erfolgter Konstruktion der Schaltung für die Sicherheitsfunktion stellt sich nun die Frage, ob bezüglich der Sicherheitsqualität auch die gestellten Anforderungen, die mit dem PL_r formuliert wurden, erfüllt wurden. Der Konstrukteur muss also unter Beweis stellen, dass seine für die Sicherheitsfunktion konstruierte Schaltung auch das an sie gesteckte Ziel erreicht. Hierzu muss vom Konstrukteur der tatsächliche Performance Level PL der Schaltung berechnet und mit dem PL_r verglichen werden.

Ist der tatsächliche Performance Level PL der Schaltung mindestens so gut wie der erforderliche Performance Level PL_r, so ist das Ziel erreicht.

Der Performance Level PL

Performance Level PL	Durchschnittliche Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde (PFH)		
a	$\geq 10^{-5}$	bis	$< 10^{-4}$
b	$\geq 3 \cdot 10^{-6}$	bis	$< 10^{-5}$
c	$\geq 10^{-6}$	bis	$< 3 \cdot 10^{-6}$
d	$\geq 10^{-7}$	bis	$< 10^{-6}$
e	$\geq 10^{-8}$	bis	$< 10^{-7}$

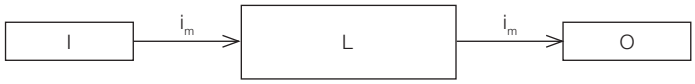
Zu ermitteln ist also für die Schaltung der Sicherheitsfunktion die „Durchschnittliche Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde". Hierfür wird die Abkürzung PFH verwendet. In manchen Dokumentationen wird anstatt der Abkürzung PFH auch PFH_D verwendet. Zu bemerken wäre, dass hier nur die gefahrbringenden Ausfälle (z.B. die Hauptkontakte eines Schütz öffnen sich nicht, wenn die Spulenspannung ausgeschaltet wird), jedoch aber nicht die nichtgefahrbringenden Ausfälle (z.B. die Hauptkontakte eines Schütz schließen sich nicht, weil die Spule des Schütz defekt ist) betrachtet werden. Dieser PFH-Wert wird mit negativen Zehnerpotenzen dargestellt, also je kleiner der PFH-Wert, umso weniger wahrscheinlich wird der gefahrbringende Ausfall. Der PFH-Wert wird in Bereiche eingeteilt und diese werden dann einem Performance Level zugeordnet. Z.B. entspricht der PFH-Bereich $\geq 10^{-7}$ bis $< 10^{-6}$ einem PL = d. Würde der berechnete PFH-Wert einer Sicherheitsfunktion $4{,}9 \times 10^{-7}$ sein, so würde das einem PL von d entsprechen. Falls z. B. der erforderliche Performance Level PL_r = d wäre, so würde beim Vergleich PL $\geq PL_r$ das Ergebnis sein, dass diese Schaltung den Anforderungen an die durchschnittliche Wahrscheinlichkeit eines gefahrbringenden Ausfalls genügt. Um einen Performance Level PL einer Schaltung für eine Sicherheitsfunktion berechnen zu können, muss man die Parameter, die für die PL-Berechnung erforderlich sind, kennen. Das sind:

- die Kategorie, die man auch als die vorgegebene Architektur der Schaltung verstehen kann und auch Aufschluss über die Art und Anzahl von Kanälen gibt
- der $MTTF_d$, was die mittlere Zeit bis zum gefahrbringenden Ausfall eines Kanals bedeutet
- der DC und DC_{avg}, mit dem Diagnosen von Komponenten oder der Sicherheitsfunktion zum Aufdecken von gefahrbringenden Fehlern bewertet werden
- der CCF, mit dem Maßnahmen zum Vermeiden des gleichzeitigen Ausfall von Kanälen bewertet werden

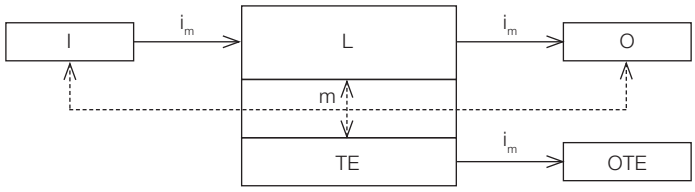
Die Kategorien B, 1, 2, 3 und 4

Die Kategorien stellen die Architekturen der sicherheitsbezogenen Teile einer Sicherheitsfunktion dar und können nicht nur als Schaltplan, sondern auch als logische Schaltbilder betrachtet werden:

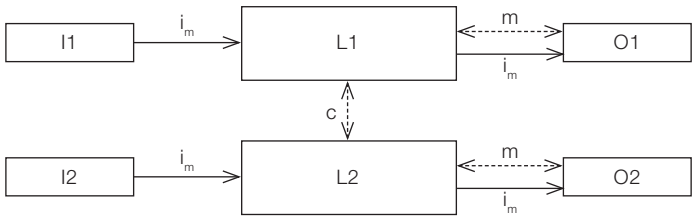
Kategorien B und 1 als 1-kanalige Architekturen



Kategorie 2 als 1-kanalige Architektur mit einer Testeinrichtung (auch Testkanal genannt)



Kategorien 3 und 4 als 2-kanalige Architekturen



An die Kategorien werden unterschiedliche Anforderungen gestellt bezüglich des Einhaltens grundlegender und bewährter Sicherheitsprinzipien, Verwendung bewährter Bauteile und Möglichkeiten von Fehlerausschlüssen. In den Anhängen A, B, C und D in EN ISO 13849-2 sind hierzu zahlreiche Beispiele gegeben. In den Kategorien 3 und 4 ist eine Einfehlertoleranz gefordert, und in Kategorie 4 darf eine Anhäufung von Fehlern nicht zum Versagen der Sicherheitsfunktion führen. Die Kategorie ist in der PL-Betrachtung ein maßgeblicher Parameter (siehe Säulendiagramm auf Seite 6).

Der $MTTF_d$

Beim $MTTF_d$ handelt es um eine reine statistische Größe für die mittlere Zeit zu einem gefahrbringenden Ausfall eines Kanals und der in einem Kanal befindlichen Bauteile. Der $MTTF_d$ eines Kanals wird in 3 Bereiche eingeteilt: niedrig – mittel – hoch. Der $MTTF_d$ ist in der PL-Betrachtung ein weiterer Parameter (siehe Säulendiagramm auf Seite 6). Für mechanische, elektromechanische und pneumatische Bauteile, also die verschleißbedingten, muss der $MTTF_d$ berechnet werden. Dies erfolgt aus dem B_{10d}-Wert des Bauteils, also der Anzahl von Zyklen, bis 10% der Bauteile gefährlich ausgefallen sind und der mittleren Zahl der jährlichen Betätigungen dieses Bauteils. Da die Gebrauchsdauer von sicherheitsbezogenen Teilen der Steuerung einer Sicherheitsfunktion nach EN ISO 13849-1 auf den Wert T_M = 20 Jahre begrenzt ist, muss für die verschleißbedingten Bauteile noch der T_{10d}-Wert, die mittlere Zeit, nach der 10% gefährlich ausgefallen sind, berechnet werden. Falls diese Zeit weniger als 20 Jahre beträgt, ist ein vorzeitiger Austausch erforderlich.

Der DC und der DC_{avg}

In den Kategorien 2, 3 und 4 sind Maßnahmen erforderlich, um rechtzeitig einen gefahrbringenden Ausfall der Sicherheitsfunktion zu erkennen, um dann Maßnahmen ergreifen zu können. Es sind also schaltungstechnische Vorkehrungen erforderlich, um möglichst viele gefahrbringende Ausfälle zu erkennen. Das bezeichnet man als Diagnose. Der Diagnosedeckungsgrad DC eines Bauteiles ist dann der Quotient aus, „erkennbaren gefahrbringenden Ausfällen" und „allen gefahrbringenden Ausfällen". Da in einem Kanal einzelne Bauteile mit einem unterschiedlichen DC-Wert auftauchen können, ist aus diesen DC-Werten der durchschnittliche Diagnosedeckungsgrad DC_{avg} zu ermitteln. Der DC_{avg} wird in 3 Bereiche eingeteilt: niedrig – mittel – hoch. Der DC_{avg} ist in der PL-Betrachtung ein weiterer Parameter (siehe Säulendiagramm auf Seite 6).

Der CCF

In den Kategorien 2, 3 und 4 ist es denkbar, dass durch ein einziges Ereignis gleichzeitig beide Kanäle ausfallen, was als „Ausfall gemeinsamer Ursache" CCF bezeichnet wird und was dann zum Versagen der Sicherheitsfunktion führen würde. In EN ISO 13849-1 Anhang F sind Maßnahmen beschrieben, der Möglichkeit eines gleichzeitigen Ausfalls entgegenzuwirken. Werden mindestens 65% dieser Maßnahmen erfolgreich praktiziert, so besteht ausreichender Schutz.

Systematischer Ausfall

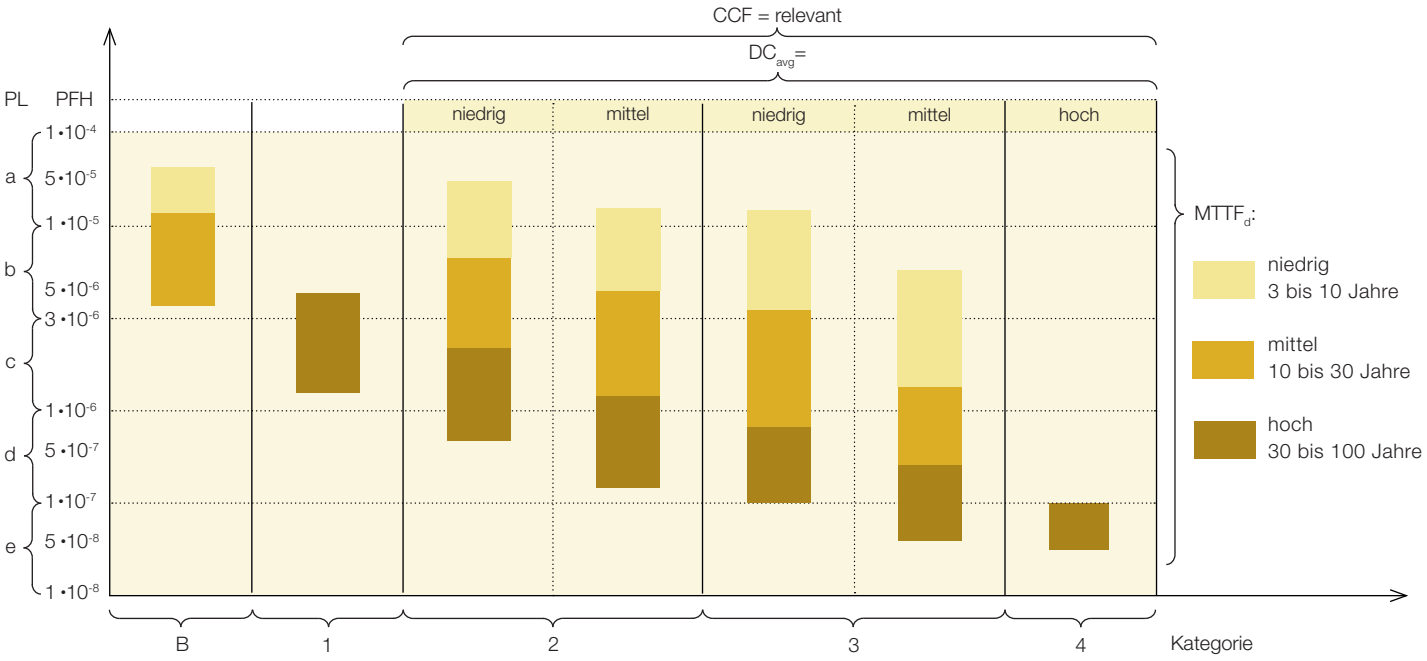
Hierunter versteht man Ausfälle mit deterministischem Bezug zu einer bestimmten Ursache, die nur durch Änderungen der Gestaltung oder des Herstellungsprozesses, Betriebsverfahren, Dokumentation oder zugehörenden Faktoren, beseitigt werden können. EN ISO 13849-1 behandelt auch das Thema der systematischen Ausfälle und informiert im Anhang G über Maßnahmen, diese zu vermeiden oder zu beherrschen.

Validierung

Die Gestaltung der sicherheitsbezogenen Teile einer Sicherheitsfunktion muss validiert werden. Die Validierung muss zeigen, dass die entsprechenden Anforderungen der relevanten Abschnitte von EN ISO 13849-1 erfüllt werden. In EN ISO 13849-2 sind die Validierungsverfahren, die Validierungsleitsätze und eine sinnvolle Vorgehensweise beschrieben und anhand von Beispielen erläutert. Die Verwendung unserer zertifizierten oder baumustergeprüften Bauteile in Sicherheitsfunktionen erleichtert und verkürzt die Validierung erheblich.

Das Säulendiagramm

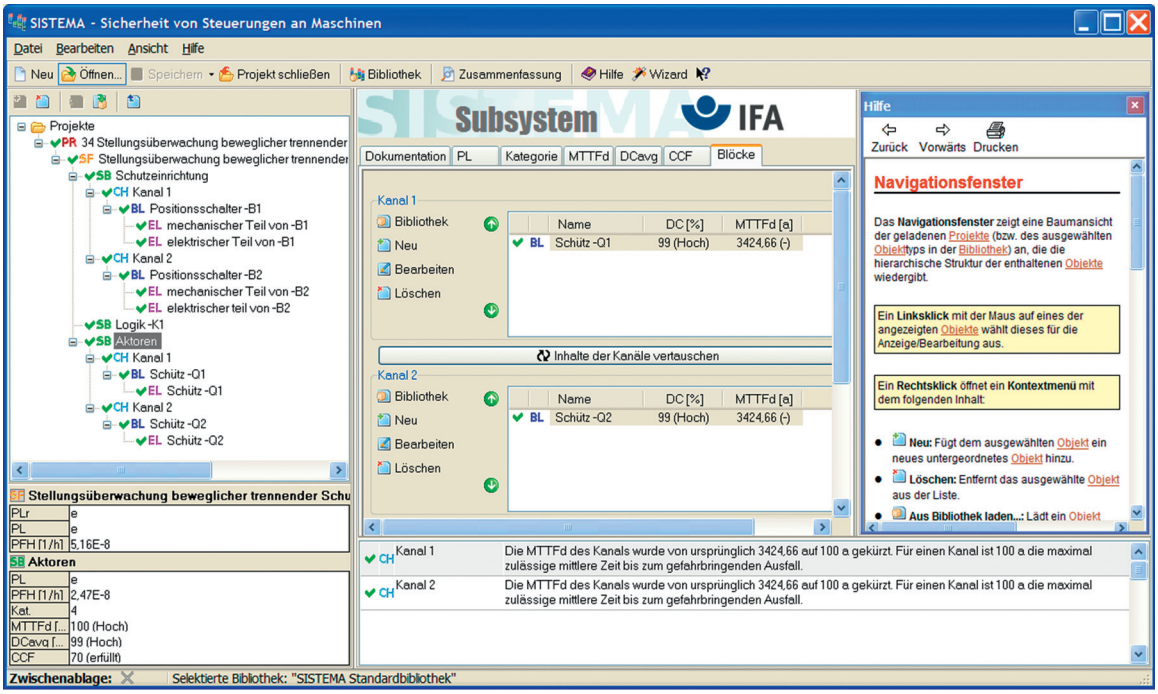
Es ermöglicht eine Übersicht über die Zusammenhänge von Kategorie, $MTTF_d$, DC_{avg} und CCF um einen PL zu erreichen



SISTEMA

Zum Erbringen des Nachweises, dass der PL ≥ PL_r ist, muss der PL einer jeden Sicherheitsfunktion rechnerisch ermittelt werden. Hierzu bietet sich das vom Institut für Arbeitsschutz (IFA) kostenlos zur Verfügung gestellte Software-Tool SISTEMA an.

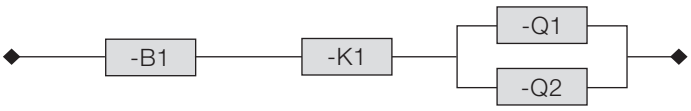
Für die Anwendung dieses Software-Tools erhalten Sie von uns eine Bibliothek, in der für unsere Produkte die sicherheitsrelevanten Daten hinterlegt sind. Damit wird eine schnelle und übersichtliche Berechnung des PL aller Sicherheitsfunktionen gewährleistet und dokumentiert.



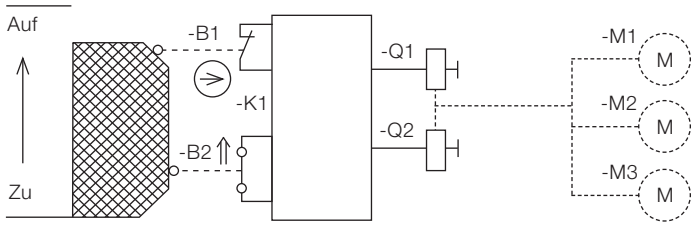
Identifizieren von Sicherheitsfunktionen

und Darstellung mit der Blockmethode nach EN ISO 13849-1 Anhang B – das Bindeglied zur PL-Berechnung mit SISTEMA

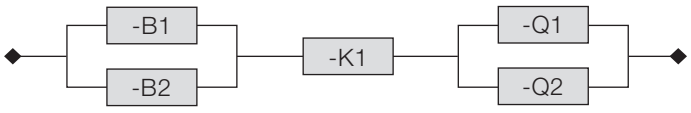
Mit der Blockmethode nach EN ISO 13849-1 Anhang B wird das sicherheitsbezogene Blockdiagramm zur Darstellung der logischen Struktur der Sicherheitsfunktion entworfen, was dann eine sehr einfache Umsetzung in die Grundelemente von SISTEMA ermöglicht. Jede Komponente in der Sicherheitsfunktion soll einen Block darstellen, und für jede Komponente werden die sicherheitstechnischen Daten zur Eingabe in SISTEMA benötigt. Im Beispiel der Bearbeitungsmaschine auf Seite 3 ist eine einzige Sicherheitsfunktion enthalten, was mit folgendem sicherheitstechnischen Blockdiagramm dargestellt wird:



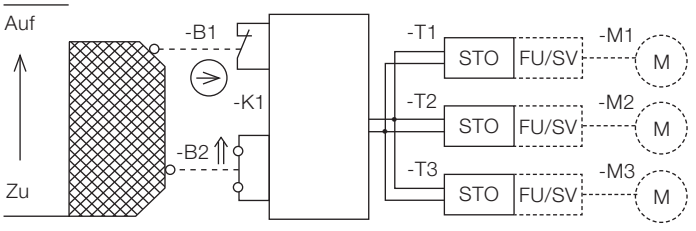
In der Praxis hat sich als Vorgehensweise bewährt, die an der Wirkung der Sicherheitsfunktion beteiligten Komponenten, beginnend in der Sensorebene über die beteiligten Logiken und ggf. Kontaktvervielfältigungen bis zur Aktorebene zu verfolgen und auch darauf zu achten, wo eine 2-Kanaligkeit darzustellen ist. Im Beispiel der Bearbeitungsmaschine von Seite 3 beginnt die Sicherheitsfunktion bei -B1, einem Sicherheitsschalter, in dem zwar 2 Kanäle enthalten sind, aber es nur eine Komponente ist. Dies trifft auch auf das Sicherheitsrelais -K1 zu. Die Aktorebene ist auch 2-kanalig, aber hier verteilt auf 2 Komponenten, die beiden Schütze -Q1 und -Q2, die als 2 Kanäle dann auch im sicherheitsbezogenen Blockdiagramm auftauchen. Würden in dieser Bearbeitungsmaschine an der Klappe 2 Sicherheitsschalter sein und die beiden Schütze -Q1/-Q2 die Energie zu drei Motoren trennen,

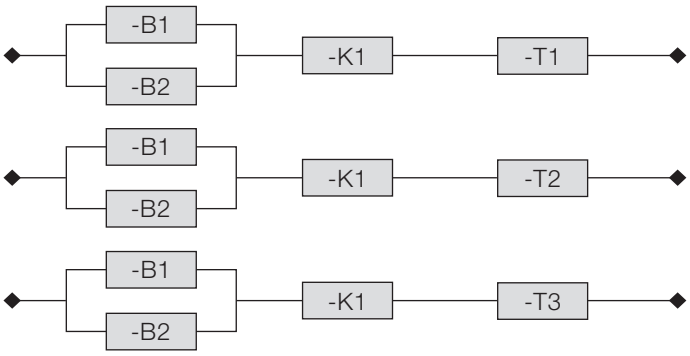


so sähe das sicherheitsbezogene Blockdiagram so aus:

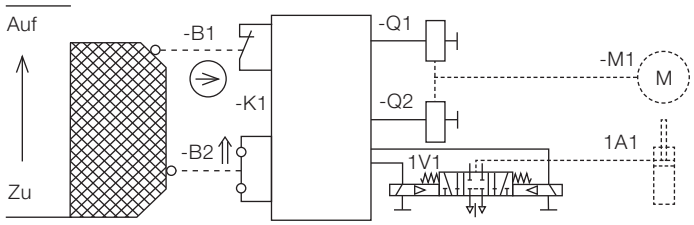


Wenn jetzt anstatt der beiden Schütze -Q1 und -Q2 für jeden Motor ein Frequenzumrichter oder ein Servoverstärker mit einem sicheren Halt, auch STO (Safe Torque Off) genannt, eingebaut werden würde, so liegt eine völlig neue Situation dahingehend vor, dass jetzt in der Aktorebene an 3 Stellen eine sichere Energietrennung zu den Motoren vorliegt, was bedeutet, dass jetzt 3 Sicherheitsfunktionen vorhanden sind:

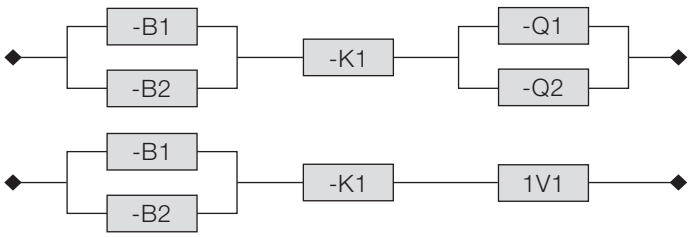




Falls die sicherheitstechnischen Daten der 3 Aktoren identisch sind, würde man hier aber nur für eine Sicherheitsfunktion den PL berechnen. Würde man im Beispiel der Bearbeitungsmaschine von Seite 3 an der Klappe 2 Sicherheitsschalter vorsehen und in der Aktorebene zusätzlich ein pneumatisches Ventil vorhanden sein,



wäre hier jetzt für 2 Sicherheitsfunktionen der PL zu berechnen, wie das sicherheitstechnische Blockdiagramm es zeigt:



In den 3 Fallstudien (Seite 10, 12 und 14) zeigen wir, wie mit unseren innovativen Produkten Sicherheitsfunktionen in
– einer Verpackungsmaschine,
– einer Roboterzelle und
– einer Werkzeugmaschine
schnell und einfach realisiert werden und stellen hier auch für einige Sicherheitsfunktionen die sicherheitsbezogenen Blockdiagramme dar. In den 3 Fallstudien werden wir außerdem 3 verschiedene Möglichkeiten der Anwendung von Logikeinheiten verwenden und die Vorteile auf Seite 18 vergleichen.

Der Gesamtrahmen zur Anwendung von EN ISO 13849-1

Die Anwendung von EN ISO 13849-1 ist in einem Gesamtrahmen aus Risikobeurteilung und Risikominderung eingebunden. Wie sieht dieser Gesamtrahmen aus? Maschinen für den industriellen/gewerblichen Einsatz zum Verkauf oder für den eigenen Gebrauch müssen die „Grundlegenden Sicherheits- und Gesundheitsschutzanforderungen für Konstruktion und Bau von Maschinen" der Maschinenrichtlinie 2006/42/EG Anhang I einhalten.

Herstellerpflicht nach Anhang I der Maschinenrichtlinie

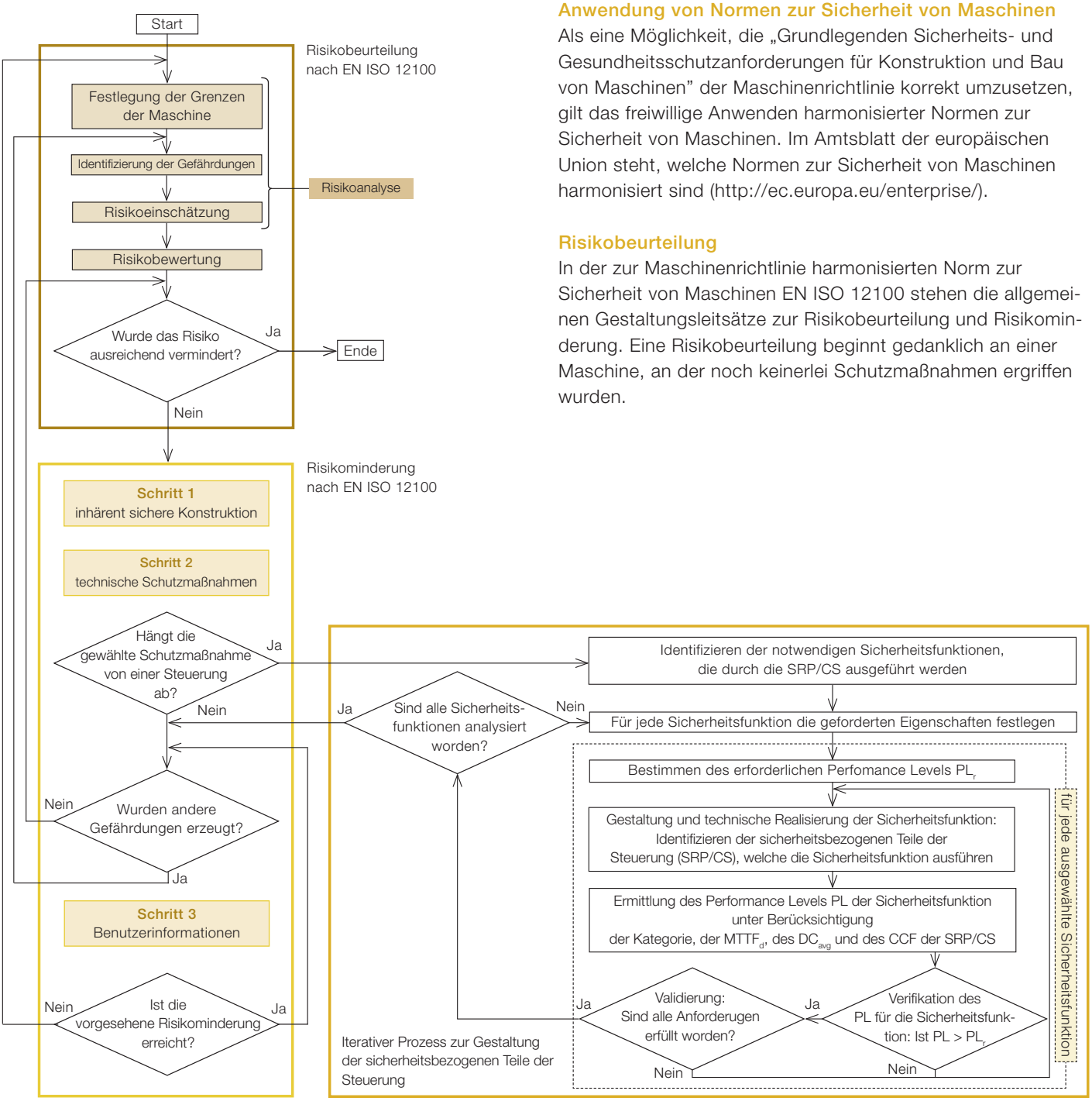
Der Hersteller einer Maschine oder sein Bevollmächtigter hat dafür zu sorgen, dass eine Risikobeurteilung vorgenommen wird, um die für die Maschine geltenden Sicherheits- und Gesundheitsschutzanforderungen zu ermitteln. Die Maschine muss dann unter Berücksichtigung der Ergebnisse der Risikobeurteilung konstruiert und gebaut werden, was häufig das Ergreifen von Maßnahmen zur Risikominderung zur Folge hat.

Anwendung von Normen zur Sicherheit von Maschinen

Als eine Möglichkeit, die „Grundlegenden Sicherheits- und Gesundheitsschutzanforderungen für Konstruktion und Bau von Maschinen" der Maschinenrichtlinie korrekt umzusetzen, gilt das freiwillige Anwenden harmonisierter Normen zur Sicherheit von Maschinen. Im Amtsblatt der europäischen Union steht, welche Normen zur Sicherheit von Maschinen harmonisiert sind (http://ec.europa.eu/enterprise/).

Risikobeurteilung

In der zur Maschinenrichtlinie harmonisierten Norm zur Sicherheit von Maschinen EN ISO 12100 stehen die allgemeinen Gestaltungsleitsätze zur Risikobeurteilung und Risikominderung. Eine Risikobeurteilung beginnt gedanklich an einer Maschine, an der noch keinerlei Schutzmaßnahmen ergriffen wurden.



Festlegen der Grenzen der Maschine

Darunter versteht man das Festlegen von z.B.
– der bestimmungsgemäßen Verwendung
– aller Funktionen und Betriebsarten
– des Bewegungsraums
– der Schnittstelle Mensch/Maschine
– der Lebensdauer der Maschine
– den Wartungsintervallen
– der Betriebstemperatur
– den Eigenschaften der zu verarbeitenden Materialien / Stoffe

Identifizierung der Gefährdungen

Bei diesem Vorgang werden alle
– Gefährdungen
– Gefährdungssituationen
– Gefährdungsereignisse
ermittelt.

Risikoeinschätzung

Hier wird das wahrscheinliche Ausmaß des Schadens und die Wahrscheinlichkeit seines Eintritts bestimmt.

Risikobewertung

Jetzt wird auf der Risikoanalyse beruhend beurteilt, ob die Ziele zur Risikominderung erreicht wurden. Also z.B. nur noch Restrisiken übrig sind nach Anwendung der Normen zur Sicherheit von Maschinen. Wurden alle Risiken hinreichend gemindert, so ist der Vorgang beendet.

Risikominderung

Hat sich aber herausgestellt, dass nicht alle Risiken hinreichend gemindert sind, so beginnt nun der Vorgang der schrittweisen Risikominderung. Im Schritt 1 muss als erstes versucht werden, „inhärent sicher zu konstruieren", also ohne trennende oder nichttrennende Schutzeinrichtungen Gefährdungen zu beseitigen oder mit den Gefährdungen verbundenen Risiken zu vermindern.

Das ist oft nicht völlig möglich, so dass dann im Schritt 2 technische Schutzmaßnahmen zur Anwendung kommen. Also z.B. bei einer Maschine die Gefahrbereiche durch ein Gehäuse oder einen Zaun abgegrenzt werden. Um aber dem Mensch einen Zutritt zu einem Gefahrbereich, z.B. zum Beseitigen von Störungen oder Nachlegen von Teilen zu ermöglichen, werden dann Türen vorgesehen. An diesen Türen werden dann als Schutzmaßnahme sog. Sicherheitsschalter angebaut, damit beim Öffnen einer Tür durch eine Steuerung die gefahrbringenden Bewegungen im Gefahrbereich beendet werden und solange beendet bleiben, bis der Mensch den Gefahrbereich wieder verlassen hat und die Tür wieder geschlossen wurde.

Schutzmaßnahme ist von einer Steuerung abhängig

Erst an dieser Stelle ist im Ablauf der Risikominderung der Punkt erreicht, an dem eine Schutzmaßnahme von einer Steuerung abhängt, und jetzt beginnt der „Iterative Prozess zur Gestaltung der sicherheitsbezogenen Teile von Steuerungen" für die hier notwendige Sicherheitsfunktion nach EN ISO 13849-1 und -2.

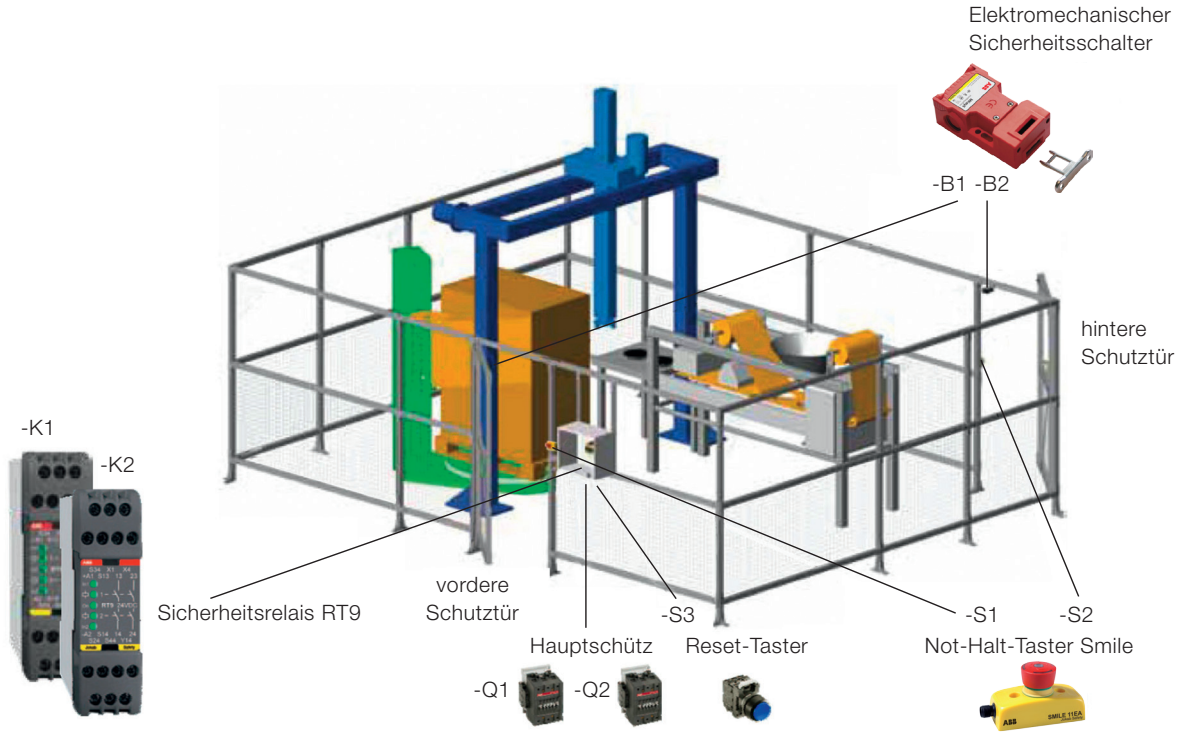
Iterativer Prozess nach EN ISO 13849-1

Im nebenstehenden Diagramm ist dargestellt, wie dieser iterative Prozess abzulaufen hat.

Erst aus den im Schritt 2 erforderlichen Risikominderungsmaßnahmen, die auch die Bedürfnisse des unter Produktionsstress stehenden Bedienpersonals zu berücksichtigen haben, resultieren die Schutzmaßnahmen und notwendigen Sicherheitsfunktionen mit ihren geforderten Eigenschaften. Die große Palette unserer innovativen Produkte zum Einsatz für trennende und nichttrennende Schutzeinrichtungen und zum Realisieren der sicherheitsbezogenen Teile von Steuerungen für Sicherheitsfunktionen und das Know-how unserer Mitarbeiter erleichtert Ihnen wesentlich, alle gestellten Anforderungen zu erfüllen. Steht der erforderliche Performance Level PL_r für jede Sicherheitsfunktion fest, so ist es mit der Vielfalt unserer Produkte nicht schwer, kostengünstig die technische Realisierung der Sicherheitsfunktionen zu bewältigen. Unter Anwendung der sicherheitsbezogenen Blockdiagramme und unserer SISTEMA-Bibliothek mit den sicherheitstechnischen Kenndaten unserer Produkte ist dann schnell mit dem Software-Tool SISTEMA des IFA der Nachweis erbracht, dass für die Hardware der Sicherheitsfunktionen der $PL \geq PL_r$ ist. Das Validieren nach EN ISO 13849-2 mit unseren zertifizierten und baumustergeprüften Produkten ist einfach und schnell zu bewältigen.

Sicherheitsrelais RT9

Sicherheitsfunktionen in einer Verpackungsmaschine
Fallstudie 1



Funktionsbeschreibung

In dieser Verpackungsmaschine werden Teile in eine Folie verpackt. Die zu verpackenden Teile werden 2 mal pro Stunde per Hand zugeführt und die verpackten abgeholt. Alle 7-8 Stunden wird die leere Folienrolle entnommen und eine volle eingelegt. Gelegentlich ist eine Störung zu beseitigen. Die Maschine soll an 365 Tagen im Jahr im 3-Schicht- Betrieb, pro Schicht 8 Stunden, in Funktion sein.

Risikobeurteilung (Auszug)

Es bestehen Gefährdungen durch Quetschen beim Entnehmen der verpackten und Einlegen der zu verpackenden Teile, beim Wechsel der Folienrolle und bei Störungsbeseitigung, falls einer der Antriebe im Falle eines Fehlers in der Steuerung der Maschine oder durch einen versehentlich gegebenen Start anlaufen würde. Das Bedienpersonal kann im Falle eines Anlaufes der Antriebe in Folge der Schnelligkeit der mechanischen Bewegungen eine Verletzung nicht vermeiden. Die Schwere der Verletzungen sind Fleischwunden, die nach ärztlicher Versorgung ohne Komplikationen heilen würden.

Risikominderung

Es ist konstruktiv nicht möglich, eine ausreichende Risikominderung durch inhärent sichere Konstruktion zu erreichen, so dass als technische Schutzmaßnahmen eine trennende Schutzeinrichtung in Form eines Schutzzaunes vorgesehen wird. Um die vorgesehenen Arbeiten ausführen zu können, werden 2 Türen vorgesehen mit je einem elektromechanischem Sicherheitsschalter, um über eine Sicherheitsfunktion beim Öffnen einer oder beider Türen die Antriebe an einem unerwarteten Anlauf zu hindern. Als ergänzende Schutzmaßnahme werden für die Handlung im Notfall für aufkommende Gefährdungen für Personen, Schäden an der Maschine oder an laufenden Arbeiten 2 Not-Halt-Taster vorgesehen. Der Schutzzaun, die Lage der beiden Türen mit Sicherheitsschalter und der Not-Halt-Taster sind im obigen Bild dargestellt. Durch die vordere Tür wird die Maschine üblicherweise betreten, um die zu verpackenden Teile zuzuführen und die verpackten abzuholen oder Störungen zu beseitigen und durch die hintere Tür zum Tausch der Folienrolle.

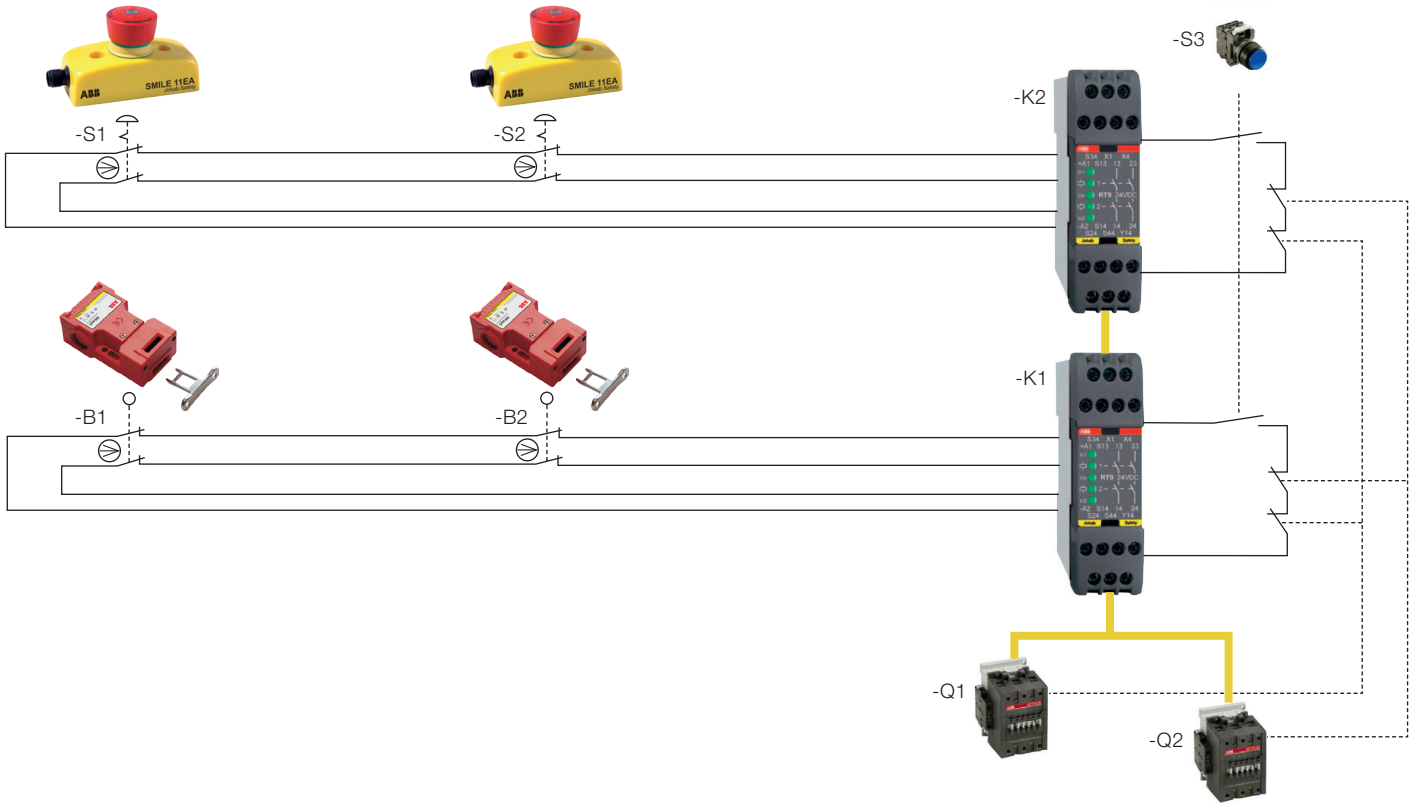
Sicherheitsfunktionen

Identifizieren der Sicherheitsfunktionen und Festlegen der Eigenschaften:

Fall A: Öffnen einer Schutztür muss durch sichere Trennung der Strom-Energie zu den Antrieben die gefahrbringenden Bewegungen verhindern.

Fall B: Betätigung eines Not-Halt-Taster muss durch sichere Trennung der Strom-Energie zu den Antrieben die gefahrbringenden Bewegungen verhindern.

Nach dem Schließen aller Schutztüren, bzw. dem Entriegeln aller Not-Halt-Taster darf die sichere Trennung der Strom-Energie erst nach Betätigung des Reset-Tasters aufgehoben werden. Jetzt erst kann die Maschine durch einen separaten Startbefehl wieder in Gang gesetzt werden.



Bestimmung des erforderlichen Performance Levels PL_r:

Aus der Funktionsbeschreibung, der Risikobeurteilung und den Maßnahmen zur Risikominderung ergibt sich im Fall A für die vordere Tür:
S_1 (leichte, üblicherweise reversible Verletzung)
F_2 (häufige Gefährdungsexposition)
P_2 (Vermeidung des Schadens kaum möglich)
Aus dem Risikograf, siehe Seite 4, ergibt das PL_r = c
Dieser PL_r wird auch für den Fall B übernommen.

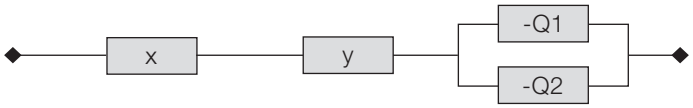
Gestaltung der Hardware der Sicherheitsfunktion:

Gewählt wurde die oben dargestellte Schaltung, welche der Kategorie 3 entspricht. Da es bei einer Reihenschaltung von elektromechanischen Sicherheitsschaltern und/oder elektromechanischen Not-Halt-Tastern zu einer Fehlerzustandmaskierung im Sicherheitsrelais kommt, wurden zwei Abschaltkreise vorgesehen, wobei selbst hier folgende Einschränkungen noch erforderlich sind, um mindestens einen niedrigen Diagnosedeckungsgrad DC zu erreichen:
1. Die vordere Schutztür wird häufig benutzt (≥ 2 mal pro Stunde) und die hintere selten (1 mal in 7 Stunden).
2. Es wird unterstellt, dass nur einer der beiden Not-Halt-Taster im Notfall betätigt wird.
Die Strom-Energie wird durch 2 Schaltschütze getrennt.
Bei Kategorie 3 müssen die grundlegenden und bewährten Sicherheitsprinzipien angewendet werden, eine Einfehlertoleranz wird gefordert und Fehlerausschlüsse sind möglich, siehe Anhang D in EN ISO 13849-2.

Ermittlung des Performance Levels PL:

Ermittlung erfolgt mit Software-Tool SISTEMA. Die Bauteildaten-B1, -B2, -S1, -S2, -K1, -K2 und -Q1/-Q2 werden aus unserer SISTEMA-Bibliothek kopiert, der $MTTF_d$ wird aus den B_{10d}-Werten und der Anzahl der mittleren Betätigungen pro Jahr berechnet und die DC-Werte werden aus Anhang E von EN ISO 13849-1 entnommen bzw. gemäß unseren Datenblattangaben eingesetzt.

Sicherheitsbezogene Blockdiagramme:



Fall A	Sicherheitsfunktion 1: x = -B1 | y = -K1
	Sicherheitsfunktion 2: x = -B2 | y = -K1
Fall B	Sicherheitsfunktion 3: x = -S1 | y = -K2
	Sicherheitsfunktion 4: x = -S2 | y = -K2

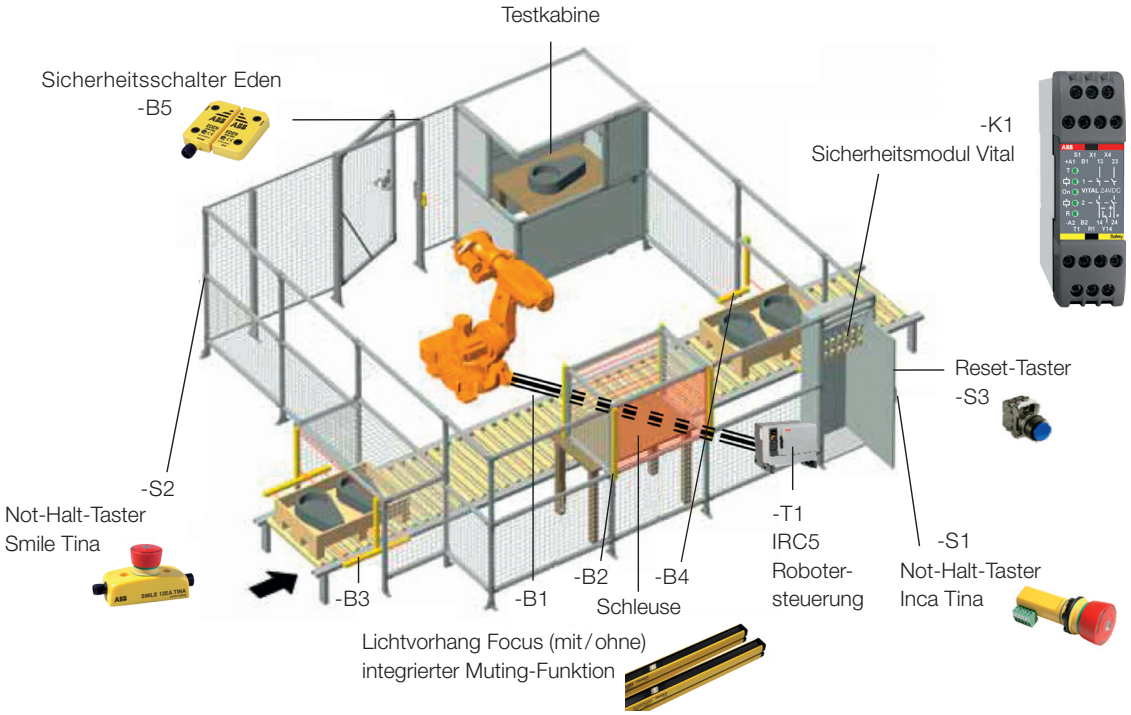
Ergebnis:

Es lässt sich für alle Sicherheitsfunktionen zeigen: PL ≥ PL_r

Hinweis: Verwendung elektromechanischer Sensoren in Reihenschaltung bedeutet einen entsprechend hohen Schaltungs- und Installationsaufwand sowie Einschränkungen im DC-Wert. Eine auch hier bessere anwendbare elektronische Lösung zeigt die Fallstudie 2.

Sicherheitsmodul Vital 1

Sicherheitsfunktionen für eine Roboterzelle
Fallstudie 2



Funktionsbeschreibung

In diese Roboterzelle werden Werkstücke durch einen Rollentransporteur transportiert und nach einem fehlerfreien Test an der anderen Seite wegtransportiert. Mit Hilfe des Roboters werden die Werkstücke in die Testkabine zum Testen gelegt. Ein Arbeitszyklus dauert 2 Minuten. Die Werkstücke, die den Test nicht bestanden haben, was ca. 5 mal pro Stunde der Fall sein wird, werden durch den Roboter in einer Schleuse abgelegt, aus der sie zur Nachbearbeitung von Hand entnommen werden können. Mit Betriebsstörungen in der Testzelle und am Förderband ist alle 45 Minuten zu rechnen. Eine Programmanpassung des Roboters sowie eine Reinigung wird 1 mal pro Woche stattfinden. Die Roboterzelle soll an 365 Tagen im Jahr im 3-Schicht-Betrieb, pro Schicht 8 Stunden, in Funktion sein.

Risikobeurteilung (Auszug)

Es bestehen Gefährdungen durch Quetschen und Stoßen für das Bedienpersonal durch die Bewegungen des Roboters bei den vorstehend beschriebenen Tätigkeiten mit der Folge sehr schwerer Verletzungen einschließlich Tod. Bei einem im Normalstopp befindlichen Roboter ist im Falle eines Fehlers in der Steuerung mit einem unerwarteten Anlauf zu rechnen. In Folge der Schnelligkeit der mechanischen Bewegungen kann eine Verletzung nicht vermieden werden.

Risikominderung

Es ist konstruktiv nicht möglich, eine ausreichende Risikominderung durch inhärent sichere Konstruktion zu erreichen, so dass als technische Schutzmaßnahmen eine trennende Schutzeinrichtung in Form eines Schutzzaunes vorgesehen wird. Um die vorgesehenen Arbeiten ausführen zu können, wird eine Tür mit einem Sicherheitsschalter vorgesehen, um über eine Sicherheitsfunktion beim Öffnen den Roboter zu stoppen und dann an einem unerwarteten Anlauf zu hindern. An den Ein- und Austrittsöffnungen beim Rollentransporteur werden Lichtvorhänge angebracht mit einer Muting-Funktion, so dass zwischen einem gewollten Ein- und Auslauf der Werkstücke und einem Zutritt einer Person sicherheitstechnisch unterschieden werden kann.

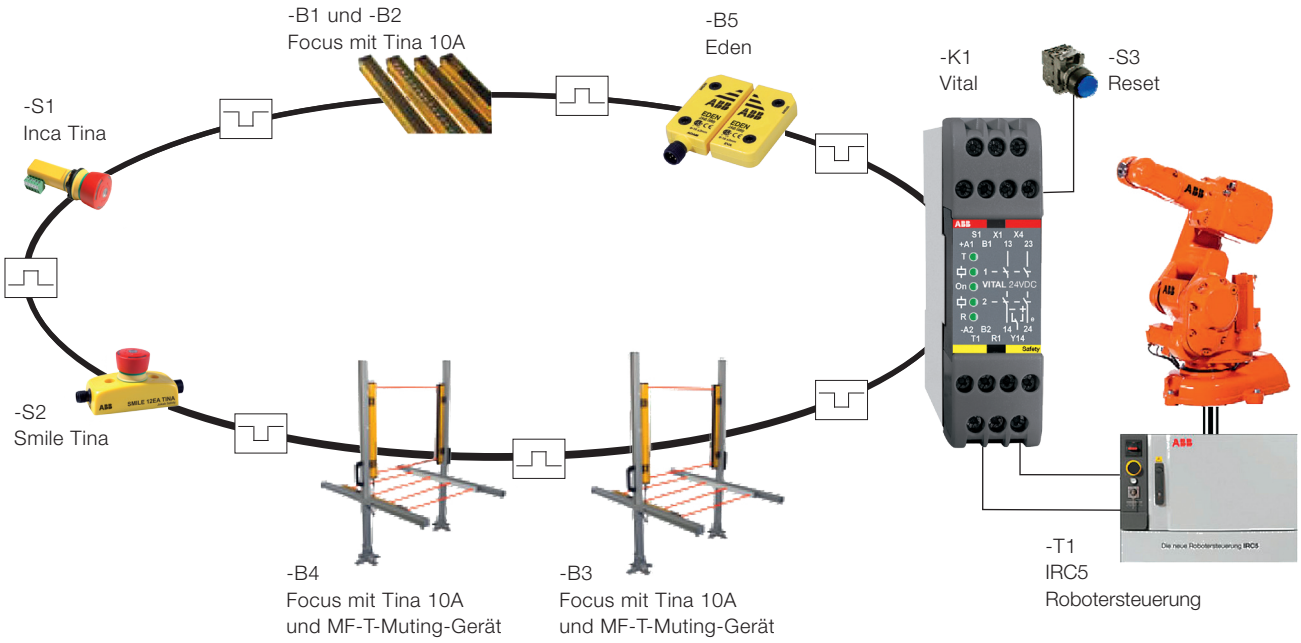
Die Schleuse enthält 2 Lichtvorhänge, die so gesteuert werden, dass der Roboter gestoppt wird, wenn gleichzeitig er und eine Person in der Schleuse hantieren wollen. Als ergänzende Schutzmaßnahme werden für die Handlung im Notfall für aufkommende Gefährdungen für Personen, Schäden an der Maschine oder an laufenden Arbeiten 2 Not-Halt-Taster vorgesehen. Der Schutzzaun, die Lage der Tür mit dem Sicherheitsschalter, die Lichtvorhänge und die Not-Halt-Taster sind im obigen Bild dargestellt.

Sicherheitsfunktionen

Identifizieren der Sicherheitsfunktionen und Festlegen der Eigenschaften:

– Öffnen der Schutztür, oder
– Ansprechen eines der Lichtvorhang-Systeme am Ein- oder Auslauf oder der Schleuse, oder
– Betätigung eines Not-Halt-Taster

muss durch sicheres Stoppen des Roboters gefahrbringende Bewegungen verhindern.



Nach dem Schließen der Schutztür, bzw. dem Entriegeln aller Not-Halt-Taster oder dem Auslösen eines der Lichtvorhang-Systeme darf der sichere Stopp erst nach Betätigung des Reset-Tasters aufgehoben werden. Jetzt erst kann die Maschine durch einen separaten Startbefehl wieder in Gang gesetzt werden.

Bestimmung des erforderlichen Performance Levels PL_r:

Aus der Funktionsbeschreibung, der Risikobeurteilung und den Maßnahmen zur Risikominderung ergibt sich:
S_2 (schwere Verletzung, einschließlich Tod)
F_2 (häufige Gefährdungsexposition)
P_2 (Vermeidung des Schadens kaum möglich)
Aus dem Risikograf, siehe Seite 4, ergibt das PL_r = e
Dieser PL_r wird auch für die Handlung im Notfall übernommen.

Gestaltung der Hardware der Sicherheitsfunktion:

Gewählt wurde die oben dargestellte Schaltung mit den gezeigten Komponenten im dynamischen Kreis des Sicherheitsmoduls Vital, welche der Kategorie 4 entsprechen, und das Erfüllen eines Performance Level PL = e ermöglicht. Eine Reihenschaltung von bis zu 30 Komponenten reduziert den PL = e nicht. Der sichere Zustand des Roboters wird durch die in unsere neue Robotersteuerung IRC5 eingebauten Sicherheitsfunktionen mit PL = e ermöglicht. Bei Kategorie 3 und 4 müssen die grundlegenden und bewährten Sicherheitsprinzipien angewendet werden, eine Einfehlertoleranz ist gefordert und bei Kategorie 4 darf eine Anhäufung von Fehlern nicht zum Verlust der Sicherheitsfunktion führen, Fehlerausschlüsse sind möglich, siehe Anhang D in EN ISO 13849-2.

Ermittlung des Performance Levels PL:

Ermittlung erfolgt mit Softwaretool SISTEMA. Die Bauteildaten -B1 bis -B5, -S1, -S2, -K1 werden aus unserer SISTEMA-Bibliothek kopiert, die sicherheitstechnischen Werte für die Komponente -T1, unsere Robotersteuerung IRC5 der neuesten Generation, werden dem IRC5-Datenblatt entnommen.

Sicherheitsbezogene Blockdiagramme:

Sicherheitsfunktion 1: x = -B1
Sicherheitsfunktion 2: x = -B2
Sicherheitsfunktion 3: x = -B3
Sicherheitsfunktion 4: x = -B4
Sicherheitsfunktion 5: x = -B5
Sicherheitsfunktion 6: x = -S1
Sicherheitsfunktion 7: x = -S2

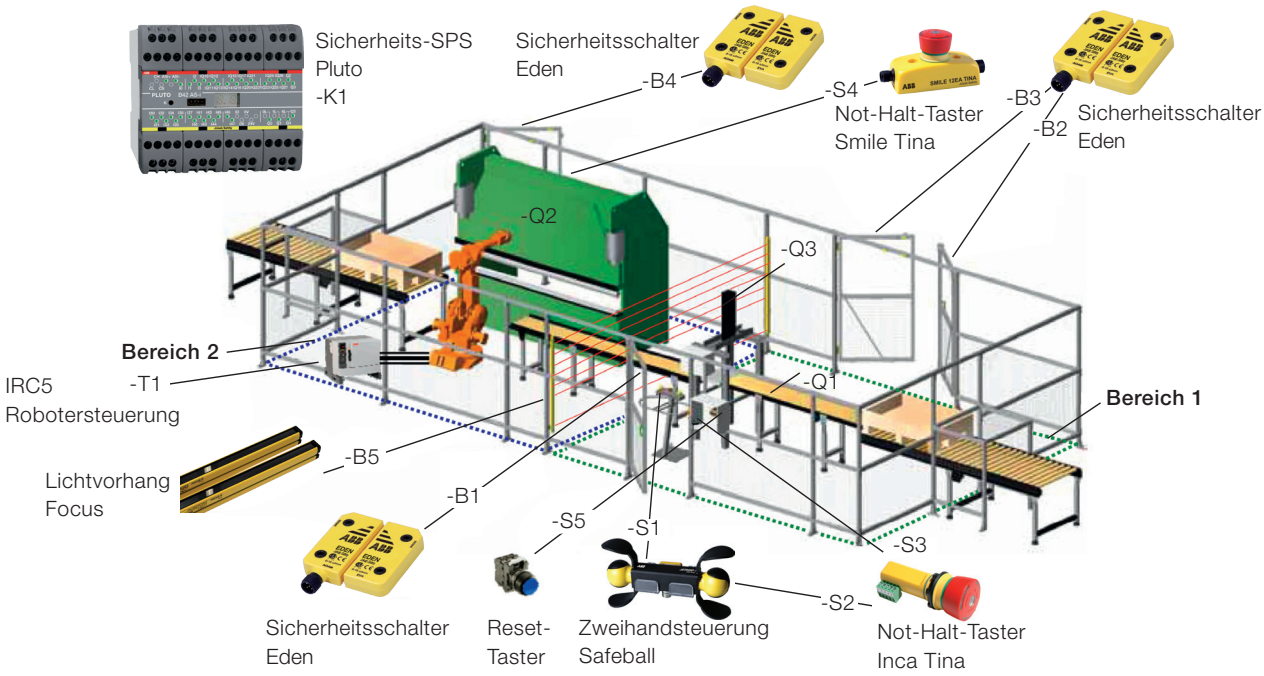
Ergebnis:

Es lässt sich für alle Sicherheitsfunktionen zeigen: PL ≥ PL_r

Hinweis: Bei Verwendung unserer zertifizierten und/oder baumustergeprüfter elektronischen Komponenten, was in diesem Beispiel der Fall ist, garantieren wir die Anforderungen auch hinsichtlich des Einhaltens der für unsere Komponenten relevanten grundlegenden und bewährten Sicherheitsprinzipien, der Einfehlertoleranz und an eine Anhäufung von Fehlern, den DC-Wert und CCF.

Sicherheits-SPS Pluto

Sicherheitsfunktionen in einer Werkzeugmaschine mit Roboter Fallstudie 3



Funktionsbeschreibung

Die zu bearbeitenden Werkstücke werden in einer Box durch ein Rollenband zugeführt und vom Bedienpersonal in die pneumatische Werkzeugmaschine -Q3 (Bereich 1) eingelegt und dort bearbeitet. Der Start erfolgt manuell durch das Bedienpersonal. Das bearbeitete Werkstück wird anschließend vom Bedienpersonal auf das Förderband -Q1 gelegt und vor die hydraulische Presse -Q2 (Bereich 2) transportiert. Dort wird das Werkstück durch den Roboter -T1 in die hydraulische Presse -Q2 eingelegt und automatisch weiterbearbeitet. Anschließend legt der Roboter -T1 das Werkstück in eine Box ab, die durch ein Rollenband abgeführt wird. Im Bereich 2 müssen gelegentlich Störungen im Ablauf durch das Bedienpersonal beseitigt werden. Der Arbeitszyklus liegt pro Werkstück bei 2 Minuten.

Risikobeurteilung (Auszug)

Es bestehen Gefährdungen bei den vorstehend beschriebenen Tätigkeiten für das Bedienpersonal durch Quetschen bei der pneumatischen Werkzeugmaschine -Q3 mit der Folge schwerer Verletzungen, durch Quetschen und Scheren bei der hydraulischen Presse -Q2 mit der Folge sehr schwerer Verletzungen, durch Quetschen und Stoßen durch die Bewegungen des Roboters -T1 mit der Folge sehr schwerer Verletzungen einschließlich Tod. Bei im Normalstopp befindlicher Presse, Werkzeugmaschine oder Roboter ist im Falle eines Fehlers in der Steuerung mit einem unerwarteten Anlauf zu rechnen. In Folge der Schnelligkeit der mechanischen Bewegungen kann eine Verletzung nicht vermieden werden.

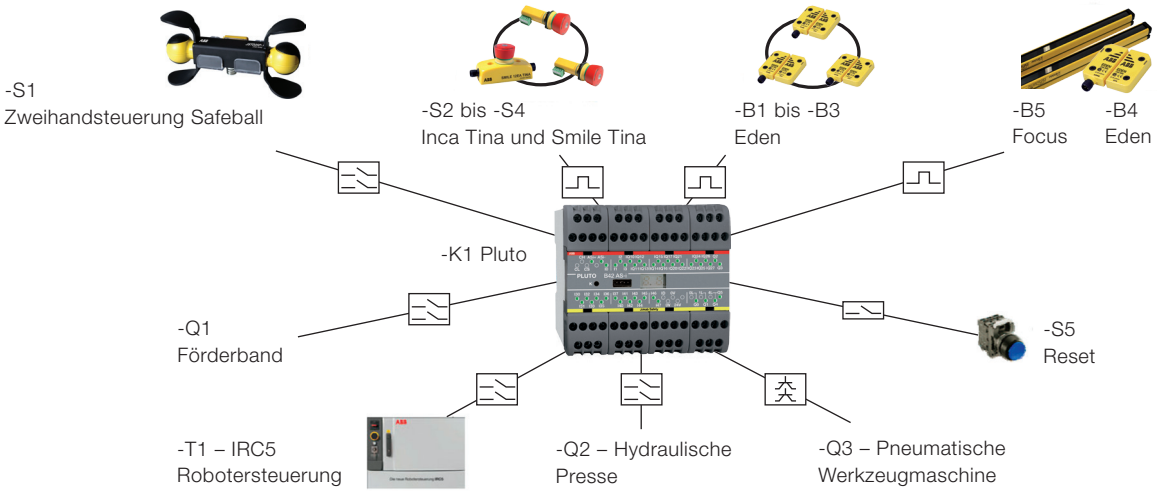
Risikominderung

Es ist konstruktiv nicht möglich, eine ausreichende Risikominderung durch inhärent sichere Konstruktion zu erreichen, so dass als technische Schutzmaßnahmen eine trennende Schutzeinrichtung in Form eines Schutzzaunes vorgesehen wird. Um die vorgesehenen Arbeiten ausführen zu können werden 4 Türen -B1 bis -B4 vorgesehen mit je einem Sicherheitsschalter. Die beiden Bereiche 1 und 2 werden durch einen Lichtvorhang -B5 abgegrenzt. An der pneumatischen Werkzeugmaschine -Q3 wird eine Zweihandsteuerung -S1 vorgesehen. Durch Sicherheitsfunktionen wird erreicht, dass beim Betreten des Bereiches 2 durch die Tür -B4 oder den Lichtvorhang -B5 der Roboter -T1 und die Presse -Q2 stoppt und ein unerwarteter Anlauf verhindert wird. Die pneumatische Werkzeugmaschine -Q3 im Bereich 1 wird mittels der Zweihandsteuerung -S1 durch eine Bedienperson bei geschlossenen Türen -B1 bis -B3 betätigt. Wird der Bereich 1 durch weitere Personen betreten, signalisiert durch Öffnen einer der Türen -B1 bis -B3 oder dem Lichtvorhang -B5, so wird die Zweihandsteuerung -S1 blockiert. Als ergänzende Schutzmaßnahme werden für die Handlung im Notfall für aufkommende Gefährdungen für Personen, Schäden an der Maschine oder an laufenden Arbeiten 3 Not-Halt-Taster -S2 bis -S4 vorgesehen. Der Schutzzaun, die Lage der Türen mit den Sicherheitsschaltern, der Lichtvorhang und die Not-Halt-Taster sind im obigen Bild dargestellt.

Sicherheitsfunktionen

Identifizieren der Sicherheitsfunktionen und Festlegen der Eigenschaften:

– Öffnen der Schutztür -B4, oder
– Ansprechen des Lichtvorhangs -B5, oder



– Betätigung eines der Not-Halt-Taster -S2 bis -S4 muss durch sicheres Stoppen des Roboters -T1 und der hydraulischen Presse -Q2 gefahrbringende Bewegungen verhindern.
– Öffnen der Schutztüren -B1 bis -B3, oder
– Ansprechen des Lichtvorhangs -B5, oder
– Nichtbetätigen der Zweihandsteuerung -S1, oder
– Betätigung eines der Not-Halt-Taster -S2 bis -S4 muss durch sicheres Stoppen der pneumatischen Werkzeugmaschine -Q3 gefahrbringende Bewegungen verhindern.
– Betätigung eines der Not-Halt-Taster -S2 bis -S4 muss das Förderband -Q1 sicher stoppen.
Nach dem Schließen der Schutztür -B4, bzw. dem Entriegeln aller Not-Halt-Taster oder dem Auslösen des Lichtvorhangs -B5 darf der sichere Zustand im Bereich 2 erst nach Betätigung des Reset-Tasters -S5 aufgehoben werden. Jetzt ist ein in Gang setzen durch separate Startbefehle möglich.

Bestimmung des erforderlichen Performance Levels PLr:

Aus der Funktionsbeschreibung, der Risikobeurteilung und den Maßnahmen zur Risikominderung ergibt sich:
– für Anhalten Roboter -T1 und hydraulische Presse -Q2
  S_2 (schwere Verletzung, einschließlich Tod)
  F_1 (gelegentliche Gefährdungsexposition)
  P_2 (Vermeidung des Schadens kaum möglich)
  Aus dem Risikograf, siehe Seite 4, ergibt das PL_r = d
– für Anhalten pneumatische Werkzeugmaschine -Q3
  S_2 (schwere Verletzung, einschließlich Tod)
  F_2 (häufige Gefährdungsexposition)
  P_2 (Vermeidung des Schadens kaum möglich)
  Aus dem Risikograf, siehe Seite 4, ergibt das PL_r = e
  Dieser PL_r wird auch für die ergänzenden Schutzmaßnahmen Handlung im Notfall übernommen.

Gestaltung der Hardware der Sicherheitsfunktion:

Gewählt wurde die oben dargestellte Schaltung mit den gezeigten Bauteilen in 3 dynamischen Kreisen der Sicherheits-SPS Pluto in Kategorie 4, was das Erfüllen eines Performance Level PL = e ermöglicht. Eine Reihenschaltung von bis zu 10 Komponenten reduziert den PL = e nicht. Der sichere Zustand des Roboters -T1 wird durch die in unserer neuen Robotersteuerung IRC5 eingebauten Sicherheitsfunktionen mit PL = e ermöglicht. Bei Kategorie 3 und 4 müssen die grundlegenden und bewährten Sicherheitsprinzipien angewendet werden, eine Einfehlertoleranz ist gefordert und bei Kategorie 4 darf eine Anhäufung von Fehlern nicht zum Verlust der Sicherheitsfunktion führen sowie Fehlerausschlüsse sind möglich, siehe Anhang D in EN ISO 13849-2.

Ermittlung des Performance Levels PL:

Ermittlung erfolgt mit Software-Tool SISTEMA. Die Bauteildaten -B1 bis -B5, -S1 bis -S5, -K1 werden aus unserer SISTEMA-Bibliothek kopiert, die sicherheitstechnischen Werte für den Roboter -T1, dem Datenblatt der Robotersteuerung IRC5 entnommen. Die sicherheitstechnischen Werte für das Förderband -Q1, die hydraulische Presse -Q2 und die pneumatische Werkzeugmaschine -Q3 werden den jeweiligen Betriebsanleitungen entnommen.

Sicherheitsbezogene Blockdiagramme:

Auf die Darstellung der einzelnen Blockdiagramme der zahlreichen Sicherheitsfunktionen haben wir im Rahmen des Umfangs dieser Broschüre verzichtet.

Ergebnis:

Es lässt sich für alle Sicherheitsfunktionen zeigen: $PL \geq PL_r$

Hinweis: Bei Verwendung unserer zertifizierten und/oder baumustergeprüften elektronischen Komponenten, was in diesem Beispiel der Fall ist, garantieren wir die Anforderungen auch hinsichtlich des Einhaltens der für unsere Komponenten relevanten grundlegenden und bewährten Sicherheitsprinzipien, der Einfehlertoleranz und an eine Anhäufung von Fehlern, den DC-Wert und CCF.

Sicherheitsbezogene Anwendungssoftware SRASW

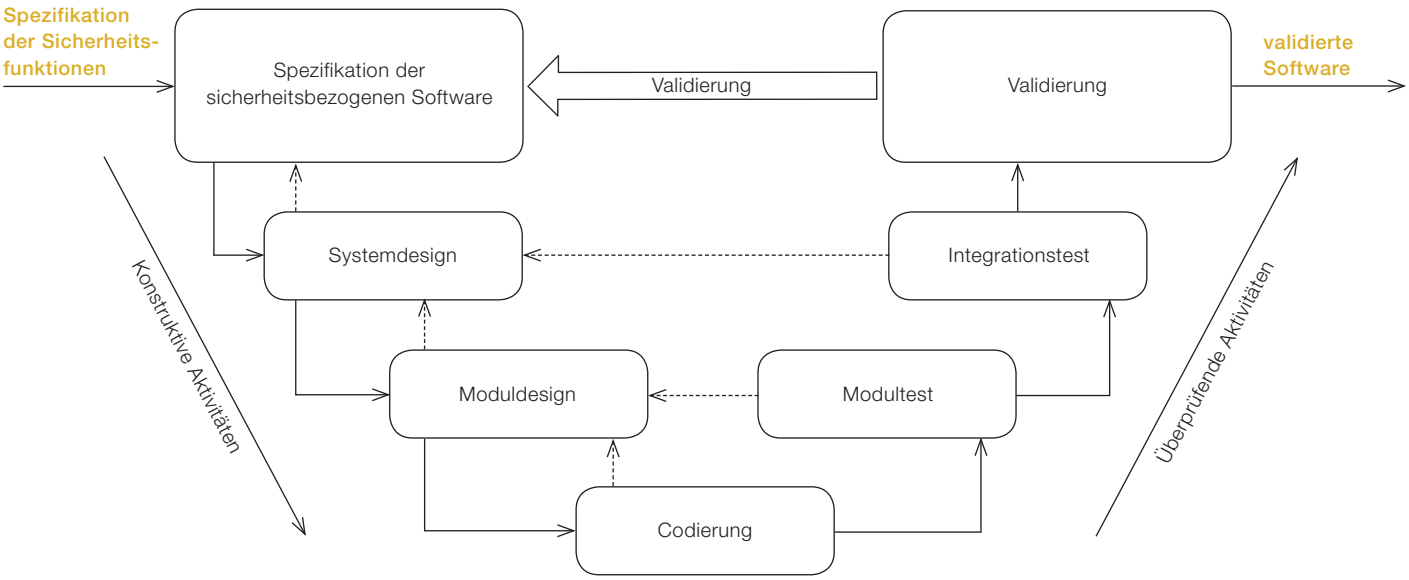
Bei Anwendung einer Sicherheits-SPS werden die Sicherheitsfunktionen nicht wie bei Einsatz von Sicherheitsrelais oder Sicherheitsmodulen, wie in den Fallbeispielen 1 und 2 dieser Broschüre verwendet, durch die Verdrahtung bestimmt, sondern durch eine Software. Diese Software nennt sich sicherheitsbezogene Anwendungssoftware SRASW (Safety Related Application Software). Da diese Software an der Ausführung der Sicherheitsfunktionen beteiligt ist, muss sie einen möglichst hohen Grad an Fehlerfreiheit aufweisen.

EN ISO 13849-1 beschreibt im Abschnitt 4.6 „Software-Sicherheitsanforderungen" die Anforderungen an die zu erstellende sicherheitsbezogene Anwendungssoftware. Alle Tätigkeiten im Lebenszyklus der sicherheitsbezogenen Anwendungssoftware müssen hauptsächlich die Vermeidung von Fehlern berücksichtigen, die während des Softwarelebenszyklus, siehe das auf dieser Seite gezeigte vereinfachte V-Modell, eingebracht werden. Das Hauptziel der Anforderungen ist, lesbare, verständliche, testbare und wartbare Software zu erhalten.

Für sicherheitsbezogene Anwendungssoftware SRASW gibt es keinen Performance Level PL, den gibt es nur für die sicherheitsbezogene Hardware, welche die Sicherheitsfunktionen ausführen. Als Orientierungsmaßstab für die Fehlerfreiheit der sicherheitsbezogenen Anwendungssoftware dient deshalb der erforderliche Performance Level PL_r der Sicherheitsfunktionen.

Ist der PL_r a bis e, so müssen die Basisanforderungen nach EN ISO 13849-1 Abschnitt 4.6.1 und 4.6.3 an die SRASW eingehalten werden, dazu zählt auch, dass das Erstellen der SRASW nach dem vereinfachten V-Modell vorgenommen wird. Ist der PL_r c, d oder e, so müssen zusätzlich Maßnahmen nach EN ISO 13849-1 Abschnitt 4.6.3 a) bis j) mit steigender Wirksamkeit zur Fehlervermeidung ergriffen werden.

Das klingt nicht gerade einfach, ist aber mit unserem Software-Tool, dem Pluto Manger einfach zu lösen.



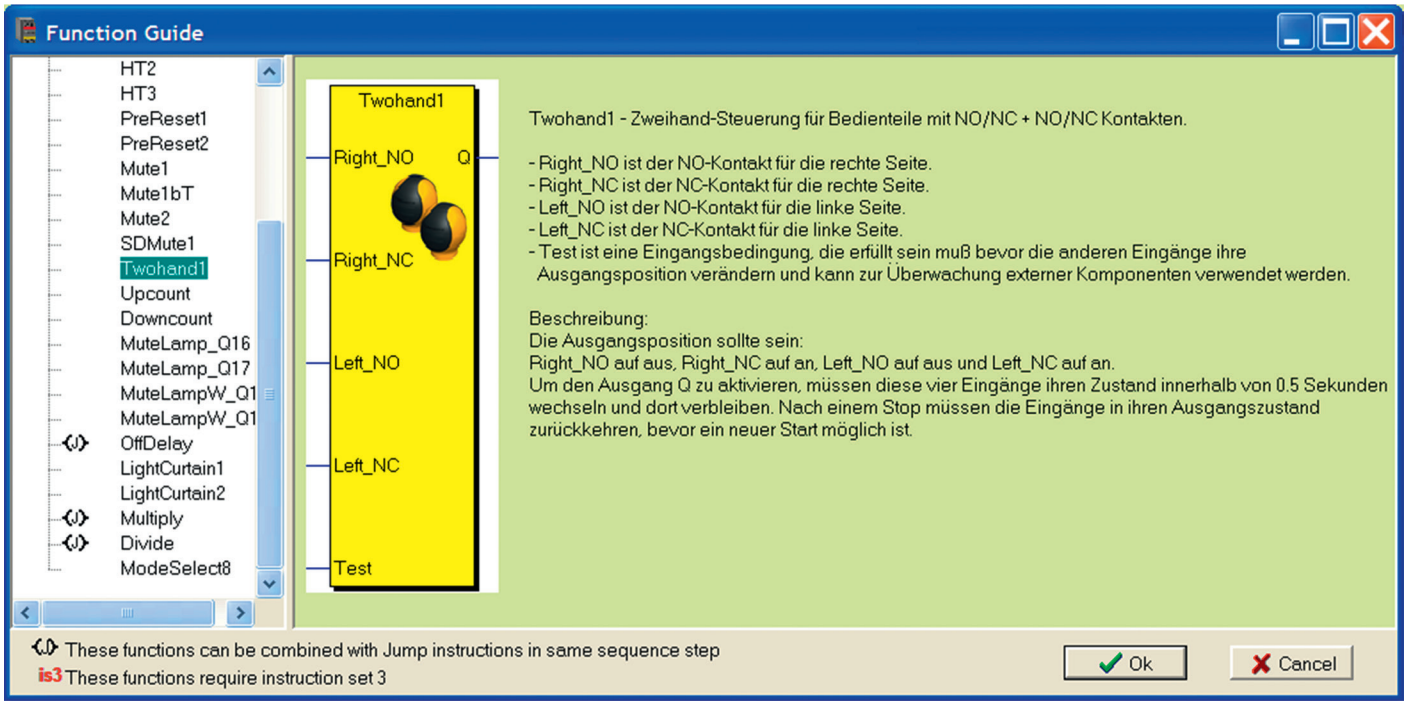
Ergebnis
Verifikation

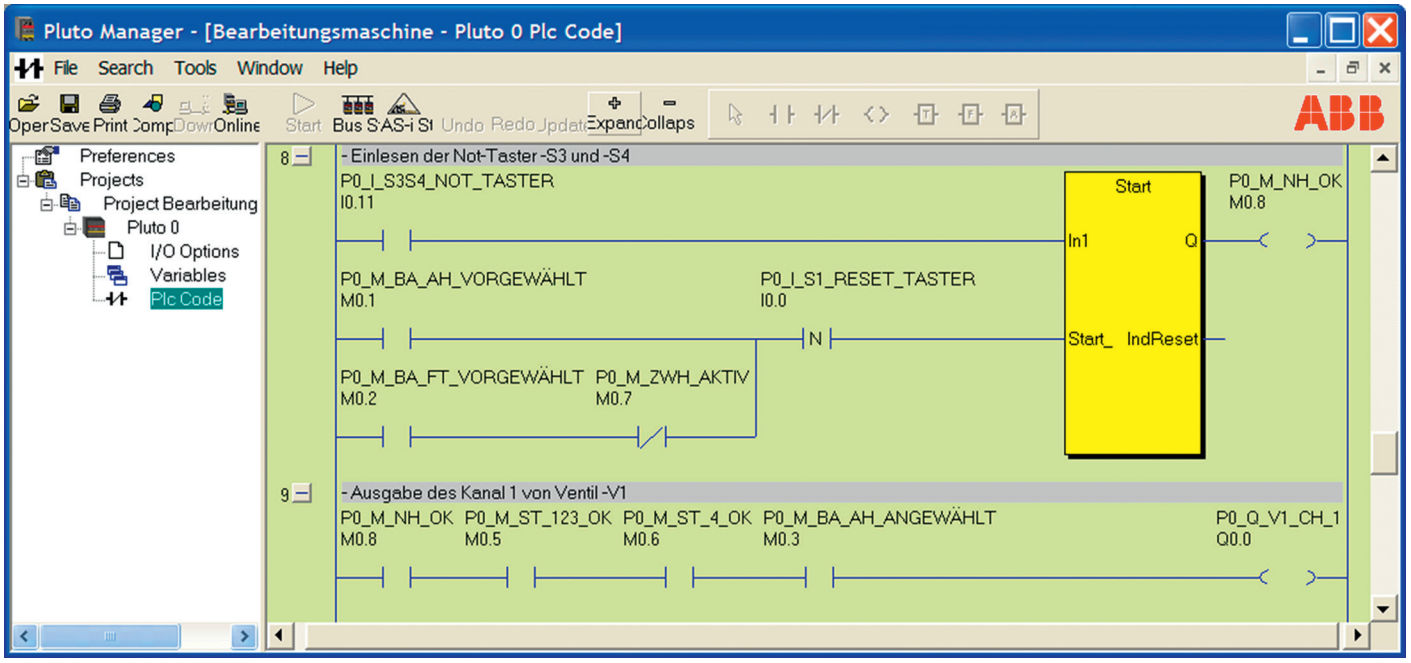
Ergebnis bezeichnte das, was in einer Phase erstellt wurde und dient als Eingabe für die nächste Phase
Verifikation bezeichnet die qualitätssichernde Aktivität, ob das Ergebnis einer Phase den Vorgaben entspricht
Validierung bezeichnet hier die abschließende spezielle Form der Verifikation der gesamten Software

Unser Pluto Manger erfüllt alle Anforderungen zum Erstellen sicherheitsbezogener Anwendungssoftware nach EN ISO 13849 -1 bis hin zum höchsten Grad der Fehlervermeidung. Programmiert wird mit der im SPS-Bereich weit verbreiteten Kontaktplan-Sprache (KOP) unter Verwendung der im Menü vorhandenen Kontakt-Symbole, Timer und weiterer wichtiger Komponenten und Funktionsbausteine über die Drag-and Drop-Methode. Also einfach das Symbol oder den Funktionsbaustein mit der Maus in das Programmierfeld ziehen und verwenden. Unsere zahlreichen Software-Funktionsbausteine sind zertifiziert und werden aus der im Pluto Manger enthaltenen Funktions-Bibliothek ganz einfach übernommen und verwendet.

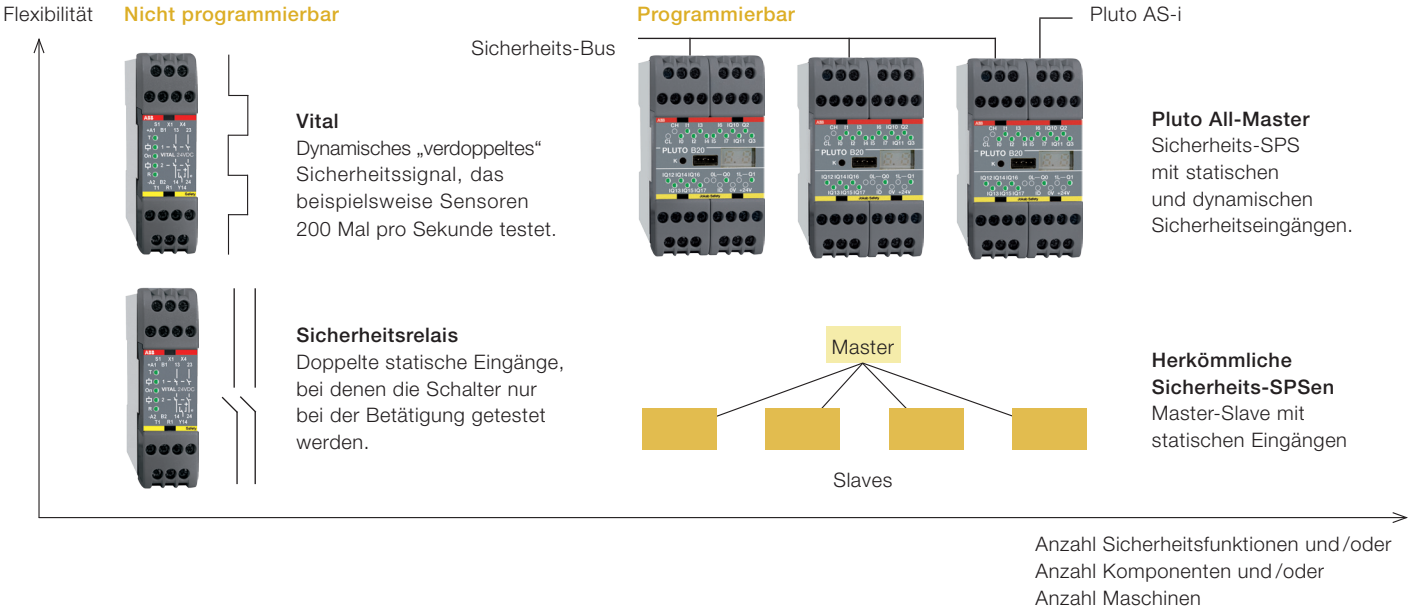
Das obere Bild zeigt einen Teil der Funktionsbibliothek mit ausgewählter Zweihandsteuerung einschließlich einer integrierten Beschreibung.

Das untere Bild zeigt einen Ausschnitt aus einem Programm einer Bearbeitungsmaschine.





Sicherheitsrelais RT9, Sicherheitsmodul Vital 1 oder Sicherheits-SPS Pluto



Zum Erreichen von PL = e mit einem konventionellen Sicherheitsrelais wie z. B. RT9 wird verlangt, dass man beide Kanäle und nur Sicherheitsschalter einer einzigen Schutzeinrichtung anschließt. Bei einer Reihenschaltung wie im Fallbeispiel 1 kann unter bestimmten Einschränkungen in der Benutzung der Schutzeinrichtungen (was aber nicht gerade praxisgerecht ist) ein PL = d erreicht werden.

Vital ist ein Sicherheitsmodul, das den Anschluss und die Überwachung einer Vielzahl von Sicherheitskomponenten in Reihe ermöglicht und das bei einem PL = e.

Das Vital-Sicherheitsmodul baut auf einem dynamischen Konzept auf und kann somit häufig mehrere Sicherheitsrelais ersetzen. Würde man im Fallbeispiel 1 elektronische Sicherheitsschalter Eden und Not-Halt-Taster Smile Tina einsetzen, so würde nur eine einzige Sicherheitslogik benötigt, nämlich das Vital-Sicherheitsmodul.

Eine weitere flexiblere Lösung wäre eine Sicherheits-SPS Pluto. Pluto hat, wie auch Vital, die Möglichkeit der Nutzung von dynamischen Signalen zur Erreichung des höchsten Performance Level PL = e

Vorteile mit Vital

- Mit PL e ist es möglich, bis zu 30 Sicherheitskomponenten in Reihe anzuschließen
- Keine Programmierung notwendig
- Möglichkeit zur Kombination verschiedener Sicherheitskomponenten z. B. Not-Halt-Taster, Lichtvorhänge, Sicherheitsschalter
- Einfache Konfiguration der Schaltung
- Auch elektromechanische Schalter können verwendet werden, ergänzt mit Tina-Modulen

Vorteile mit Pluto

- Pluto ist ein All-Master-System mit Kommunikation über einen separaten Sicherheits-Bus
- Plutos große Flexibilität erleichtert die Gestaltung von Schutzeinrichtungen mit vielen Sicherheitsfunktionen
- Eine einzige Software für alle Plutos in einem System aus bis zu 32 Plutos, verbunden mit dem Sicherheits-Bus
- Einfache Programmierung durch Verwendung von zertifizierten Funktionsbausteinen.

Produktionsoptimale Schutzmaßnahmen und Schutzeinrichtungen

1 Sensor Eden
meldet das Öffnen einer Schutztür zum Auslösen von Sicherheitsfunktionen, um einen gefahrlosen Zustand in der Maschine herzustellen

2 Not-Halt-Taster Smile
zum schnellen Anhalten der Maschine bei Gefahr für Personen, drohenden Schäden an der Maschine oder an laufenden Arbeiten

3 Elektromagnetische Zuhaltung Magne
kann verwendet werden zum Zuhalten einer schweren Schutztür, damit diese nicht durch Erschütterungen oder unbedacht durch das Personal geöffnet wird und ein laufender Bearbeitungsvorgang unterbrochen wird

4 Zaunsystem Quick-Guard
ist eine trennende Schutzeinrichtung und verhindert den Zutritt zu den Gefahrbereichen in der Maschine und dient je nach Ausführung auch zur Lärmminderung

5 Elektromagnetische Zuhaltung Dalton
findet Verwendung an einer Schutztür oder Schutzklappe, damit diese nicht unbedacht geöffnet wird mit der unerwünschten Folge einer Unterbrechung eines maschinellen Arbeitsvorganges

6 Schaltleiste
meldet beim Schließen eines Rolltores ein Hindernis zum Auslösen einer Sicherheitsfunktion, die eine Bewegungsumkehr des Rolltores und somit eine Quetschung verhindert

7 Rolltor
ermöglicht kürzere Abstände zu Gefahrbereichen in der Maschine und dient auch zur Lärmminderung im geschlossenen Zustand

8 Sicherheitszuhaltung Knox
wird verwendet, damit eine Schutztür erst geöffnet werden kann, wenn innerhalb der Maschine sichergestellt ist, dass alle gefahrbringenden Bewegungen sicher zum Stillstand gekommen sind

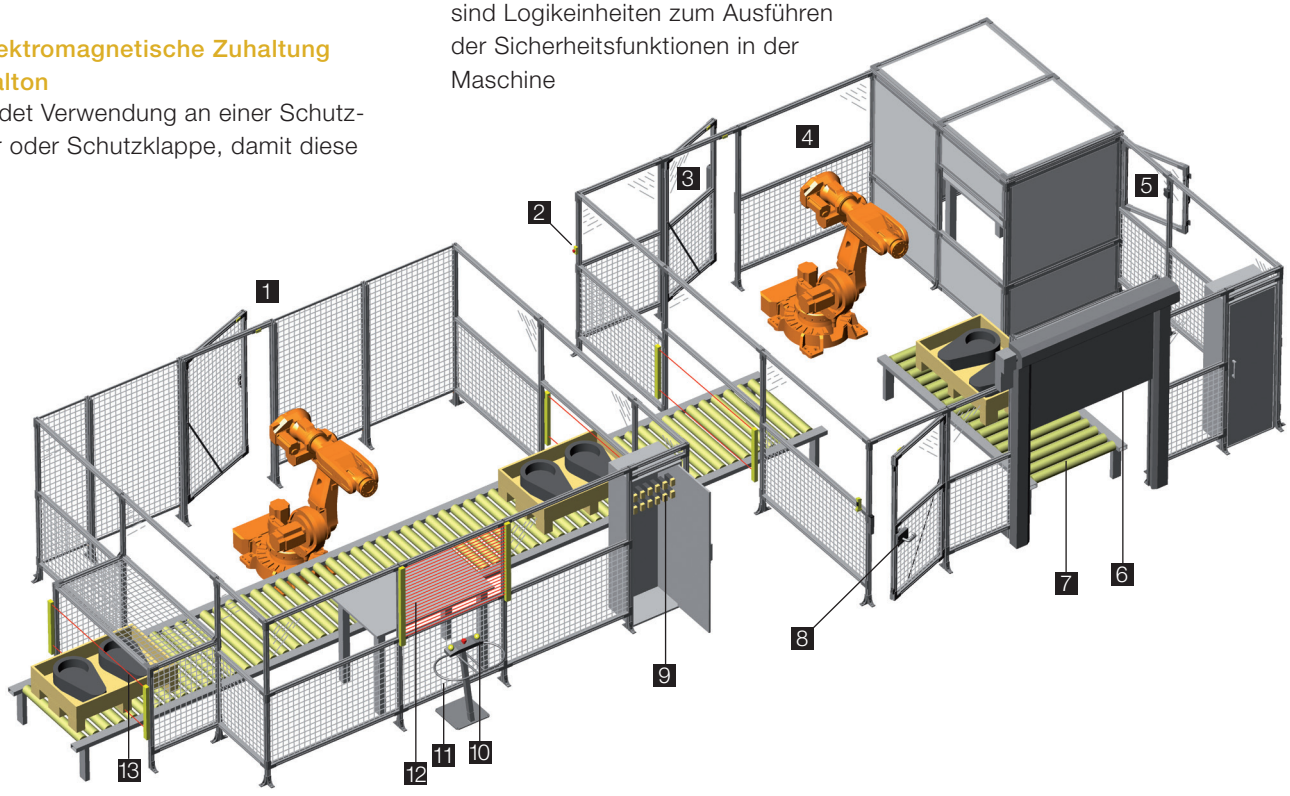
9 Sicherheits-SPS Pluto, Vital und Sicherheitsrelais
sind Logikeinheiten zum Ausführen der Sicherheitsfunktionen in der Maschine

10 Zweihandbedienung mit Safeballs
wird für sichere Zweihandschaltungen eingesetzt, und mit der ergonomischen Ausführung des Safeball wird ein ermüdungsarmes Bedienen erreicht

11 Nachlaufzeitmessgerät Smart
dient zum Messen der Zeit, die vom Öffnen einer Schutztür oder Betätigen eines Lichtvorhangs bis zum Stillstand gefahrbringender Bewegungen vergeht zum Beurteilen des erforderlichen Mindestabstandes

12 Lichtvorhang Focus
mit hoher Auflösung werden bereits Finger erfasst, so dass auch kleine Abstände zum Gefahrbereich realisiert werden können

13 Lichtschranke Focus
wenn anstatt der Kassette mit den zu bearbeitenden Teilen eine Person den Zugang zur Maschine versucht, so erfolgt eine Meldung zum Anhalten der Maschine durch eine Sicherheitsfunktion



Kontakt

ABB STOTZ-KONTAKT GmbH
Eppelheimer Str. 82
69123 Heidelberg, Deutschland
Telefon: +49 (0) 6221/701 - 0
Telefax: +49 (0) 6221/701 - 1325
E-Mail: info.desto@de.abb.com

www.abb.de/stotzkontakt

Vertrieb Jokab Safety
Max-Planck-Strasse 21
78549 Spaichingen, Deutschland
Telefon: +49 (0) 7424/95865 - 0
Telefax: +49 (0) 7424/95865 - 99
E-Mail: buero.spaichingen@de.abb.com

Hinweis:
Technische Änderungen der Produkte sowie Änderungen im Inhalt dieses Dokuments behalten wir uns jederzeit ohne Vorankündigung vor. Bei Bestellungen sind die jeweils vereinbarten Beschaffenheiten maßgebend. Die ABB AG übernimmt keinerlei Verantwortung für eventuelle Fehler oder Unvollständigkeiten in diesem Dokument.

Druckschrift Nummer 2CDC 001104B0101 - Gedruckt in Deutschland (03/12 - 2-ZVD)

Power and productivity
for a better world™