

1- Einleitung

Zweck dieses Abschnittes ist es, dem Maschinenhersteller einen schnellen Überblick über einige Normen im Maschinensicherheitsbereich zu geben, einige Grundbegriffe zu klären und einige Anwendungsbeispiele anzuführen. Diese kurze Anleitung bezieht sich ausschließlich auf die sicherheitsrelevanten Aspekte der Maschine, beziehungsweise auf die Gesamtheit der getroffenen Maßnahmen, die die Bedienperson vor den Gefahren bei Maschinen in Betrieb schützen soll. Es werden keine Risiken behandelt, die von anderen Gefahrenquellen hervorgerufen werden könnten, wie zum Beispiel das Vorhandensein von Strom, Behälter unter Druck, explosive Atmosphären, usw. Diese müssen vom Maschinenhersteller eingeschätzt werden.

Die Firma Pizzato Elettrica hat an dieser Unterlage nach ihren besten Kenntnissen und mit Berücksichtigung der Normen, Interpretationen und der im Jahr 2011 bestehenden Technologien, gearbeitet. Da einige dieser behandelten Normen erst in diesen Monaten ihre tatsächliche Erstanwendung finden, ist es nicht auszuschließen, dass im Laufe der Zeit neue Normen oder Bewertungen seitens benannter Stellen die hier genannten Auswertungen abändern können. Die hier angeführten Beispiele müssen immer vom Endkunden in Bezug auf den neusten Stand der Technologie und Norm abgeschätzt werden und entbinden ihn nicht von seiner Verantwortung. Pizzato Elettrica übernimmt keine Verantwortung der hier angeführten Beispiele und schließt nicht aus, dass ungewollte Fehler oder Ungenauigkeiten bei den erteilten Daten auftreten können.

2- Entwerfen in Sicherheit. Die Europäische Normenstruktur.

Um innerhalb der Europäischen Gemeinschaft jede Art von Vorrichtung oder Maschine unbehindert zu vermarkten, müssen diese den Vorschriften der EU-Richtlinien entsprechen. Diese bestimmen allgemeine Grundsätze, um zu vermeiden, dass Hersteller Produkte auf den Markt bringen, welche für die Bedienpersonen gefährlich sein könnten. Die Gesamtheit der Produkte und der verschiedenen Gefahren ist sehr umfangreich und daher wurden im Laufe der Zeit mehrere Richtlinien erlassen. Wir nennen als Beispiel die Niederspannungsrichtlinie 2006/95/EC, Atex-Produktlinie 94/9/EC, Europäische EMV-Richtlinie, usw. Die Maschinenrichtlinie 2006/42/EC ersetzt und behandelt ableitbare Gefahren der sich in Betrieb befindenden Maschinen.

Die Konformität der Richtlinien wird durch die Konformitätserklärung des Herstellers und durch die Anbringung der CE-Kennzeichnung an der Maschine bescheinigt.

Zur Auswertung der Gefahren einer Maschine und zur Realisierung der Sicherheitssysteme haben CEN und CENELEC, europäische Normungsorganisationen, eine Reihe von Normen herausgegeben, die den Inhalt der Richtlinien in technische Hinweise übersetzen, um das Bedienpersonal vor Gefahren zu schützen. Die im EU-Amtsblatt veröffentlichten Normen sind harmonisch. Der Hersteller, der diese Normen zur Bescheinigung seiner Maschinen anwendet, hat das Konformitätsbewertungsverfahren bestanden.

Die Normen zur Sicherheit von Maschinen teilen sich in drei Typologien: A, B und C.

Typ A Normen: Normen, die Grundbegriffe und Entwurfsrichtlinien zur Herstellung aller Maschinen behandeln.

Typ B Normen: Normen, die eine oder mehrere Sicherheitsaspekte spezifisch behandeln und sich in folgende Normen unterteilen:

- B1: Normen in Bezug auf einige Sicherheitsaspekte (z.B.: Sicherheitsabstand, Temperatur, Lärm,...)
- B2: Normen in Bezug auf Sicherheitsvorrichtungen (z.B.: Zweihandüberwachung, gegenseitig verriegelte Vorrichtungen, Schutzvorrichtungen,...)

Typ C Normen: Normen, die die Sicherheitsvorschriften gewisser Maschinengruppen detailliert behandeln (z.B.: hydraulische Pressen, Spritzgießmaschinen,...)

Der Anlagen- oder Maschinenhersteller muß sich also zuerst erkundigen, ob das Produkt unter eine Typ C Norm einzustufen ist. Bei positiver Auswertung wird diese Norm die Sicherheitsvorschriften vorgeben, ansonsten werden die Typ B Normen für jeden einzelnen spezifischen Aspekt oder Vorrichtung des Produktes angewandt. Bei fehlender Spezifikation folgt der Hersteller den allgemeinen Grundsätzen der Typ A Normen.

TYP A NORMEN

zum Beispiel:

EN 12100-1 und -2:2010 (ersetzt EN 292-1 und EN 292-2).
Wesentliche Begriffe, allgemeine Entwurfsrichtlinien..
EN 61508. Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/ programmierbarer elektronischer Systeme
EN 14121:2007: Richtlinien zur Risikobeurteilung

TYP B1 NORMEN

zum Beispiel:

EN 62061:2005 Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/ programmierbarer elektronischer Systeme
EN ISO 13849-1:2006 e -2:2003 Teil der Sicherheitssteuerungssysteme

NORME DI TIPO B2

zum Beispiel:

EN 574:2008 Zweihandschaltungen
EN 13850:2006 (ersetzt EN 418:1992)
Not-Halt
EN 1088:2008 und ISO 14119 Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen
EN 60204-1:2006 Elektrische Ausrüstung von Maschinen
EN 60947-5-1:2009 Elektromechanische Steuergeräte

TYP C NORMEN

zum Beispiel:

EN 201:2007 Gummi- und Kunststoffmaschinen, Spritzgießmaschinen
EN 415-1...-7:2009 Sicherheit von Verpackungsmaschinen
EN 692:2009 Mechanische Pressen
EN 693:2009 Hydraulische Pressen
EN 848-1:2010 Sicherheit von Holzbearbeitungsmaschinen
Fräsmaschinen für einseitige Bearbeitung mit Drehendem Werkzeug – Teil 1: Senkrechte Einspindel-Tischfräsmaschinen (toupie)

3 – Sichere Maschinen entwerfen. Die Risikoeinschätzung.

Der erste Schritt zur Herstellung einer sicheren Maschine besteht darin, alle möglichen Gefährdungen, denen die Bedienpersonen einer Maschine ausgesetzt sind, zu ermitteln. Die Ermittlung und Klassifizierung der Gefährdungen erlaubt es, das Risiko für die Bedienperson oder die Wahrscheinlichkeit einer Gefährdung und des möglichen Schadens zu bestimmen.

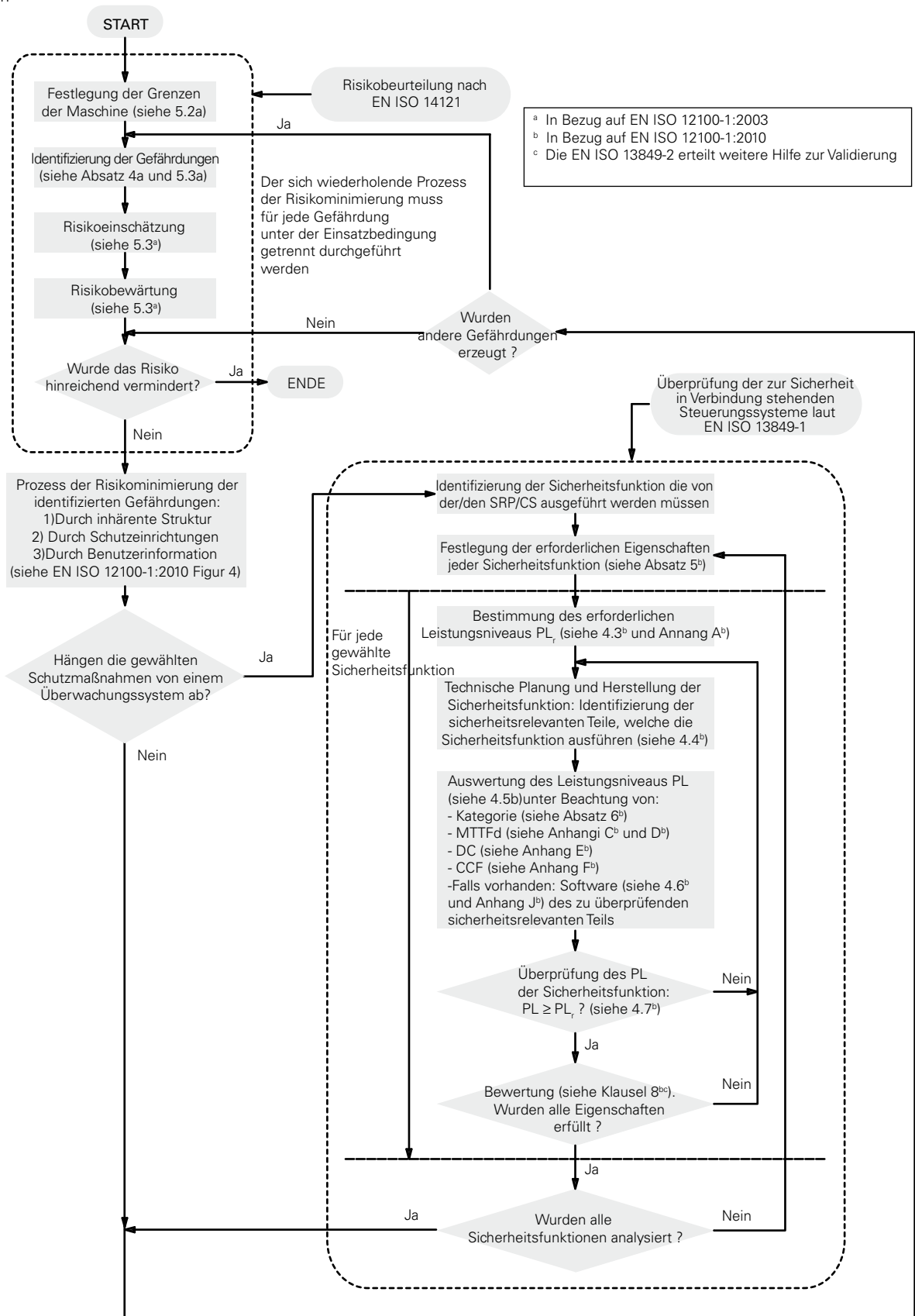
Die Methodologie der Risikoeinschätzung, deren Auswertung und Verminderung werden von den Normen EN 12100 und EN 14121 bestimmt. Diese Normen führen ein zyklisches Analysenmodell ein, bestimmt von den anfänglichen Zielsetzungen, der Risikoeinschätzung und der verschiedenen Möglichkeiten diese Risiken einzuschränken, werden diese wiederholt ausgewertet, bis diese der Ausgangszielsetzung nicht gerecht sind.

Das von diesen beiden Normen eingeführte Modell sieht vor, daß man nach einer Risikoeinschätzung gemäß EN 14121 wie folgt vorgeht, um dieses zu vermindern oder auszuschneiden:

- 1) Ausschließen der Risiken von Anfang an durch die Aufbaustruktur der Systeme und die Anwendung von wesentlich sicheren Entwurfsrichtlinien.
- 2) Risikominderung durch Schutz- und Überwachungssysteme.
- 3) Markierung der restlichen Risiken durch Meldung und Information an die Bedienpersonen.

Da jede Maschine Gefahren aufweist und es nicht möglich ist alle damit verbundenen möglichen Risiken auszuschließen, ist es das Ziel Restrisiken auf ein akzeptables Maß zu reduzieren.

Falls ein Risiko durch ein Überwachungssystem vermindert wird, tritt die Norm EN ISO 13849 ein, welche ein Auswertungsmodell der Güte dieses Systems liefert. Gibt man ein Risiko eines gewissen Niveaus an, ist es möglich eine Sicherheitsfunktion eines gleichen oder höheren Niveaus anzuwenden



Hinweis: Dieses Diagramm wurde durch Kombination 1 und 3 der Norm EN ISO 13849-1:2006 erstellt. Die angeführten Texte sind eine nicht offizielle Übersetzung der englischen Texte.

4 –Aktuelle Situation der Normen (Jahr 2011). Die Gründe der Veränderung, die neuen Normen und einige Überschneidungen

Die "traditionellen" Normen für die funktionelle Sicherheit, wie die Norm EN 954-1, heben sich dadurch hervor, da diese einige Grundsätze zur Analyse der Sicherheitsschaltungen nach bestimmten Grundsätzen formuliert haben. Das Thema programmierbarer elektronischer Vorrichtungen wird andererseits überhaupt nicht erwähnt und ist überholt. Um die programmierbaren elektronischen Vorrichtungen in die Analyse der Sicherheitsschaltungen einzuschließen, ist der Ansatz der neuen Normen hauptsächlich wahrscheinlichkeitstheoretisch und in diese werden daher neue statistische Variablen eingeführt.

Ansehnlich ist die Norm IEC 61508, „Mutter“ der Normen dieser Ansätze (in 8 Kapitel von circa 500 Seiten aufgeteilt); diese behandelt die Sicherheit der programmierbaren komplizierten elektronischen Systeme und kann zudem in sehr unterschiedlichen Bereichen (Prozessindustrie, Maschinenbau, Atomkraftwerke) eingesetzt werden und wird deshalb als Typ A Norm eingestuft. Diese Norm führt den Begriff SIL (Safety Integrity Level) ein, eine wahrscheinlichkeitstheoretische Angabe des Restrisikos eines Systems.

Auch die Norm EN ISO 13849, erstellt von CEN unter Schutz der ISO, basiert auf diesem wahrscheinlichkeitstheoretischem Ansatz, versucht aber dem Hersteller, gewöhnt an die Begriffe der Norm EN 954-1, den Übergang zu den neuen Begriffen weniger problematisch zu gestalten. Die Norm deckt elektromechanische, hydraulische, „unkomplizierte“ elektronische und einige programmierbare elektronische Vorrichtungen mit festgelegten Strukturen ab.

Die Norm EN ISO 13849 ist eine Typ B Norm und führt das Konzept PL (Performance Level) ein; wie bei SIL gibt dieses Konzept einen wahrscheinlichkeitstheoretische Angabe des Restrisikos einer Maschine. In dieser Norm wird auf eine Korrelation zwischen SIL und PL hingewiesen; es werden die durch Norm IEC 61508 abgewandelten Konzepte wie DC und CCF verwendet und eine Angabe mit den Sicherheitskategorien der Norm EN 654-1 hergestellt.

Drei Normen (Jahr 2011) haben aktuell im Bereich der funktionellen Sicherheit und zur Sicherheit der Steuerungen Gültigkeit:

- EN 954-1:1996. Typ B Norm, welche die Begriffe der Sicherheitskategorien eingeführt hat und in Kürze verfällt. Die aktuelle 954-1:1996 bleibt bis Dezember 2011 gültig und wird danach offiziell von der Norm EN ISO 13849 ersetzt. Durch die Verbreitung derselben in den letzten Jahren wird diese Norm jedenfalls noch lange als technische Unterlage dienen.
- EN ISO 13849:2006. Typ B1 Norm, welche das Konzept PL anwendet
- EN 62061:2005. Typ B1 Norm, welches das Konzept SIL anwendet.

Die beiden Normen EN 62061 und EN 13849 überschneiden sich ziemlich im Anwendungsbereich und sind sich unter einigen Aspekten sehr ähnlich; dies beweist auch die Ähnlichkeit der beiden

Abkürzungen (SIL und PL), die das Ergebnis der Analysen gemäß der beiden Normen festsetzen.

Die Empfehlungen des Anwendungsbereiches der beiden Normen werden in der Tabelle 1 der Norm EN 13849 erläutert und wie daraus ersichtlich ist, sind beide Normen bei vielen Typologien anwendbar.

PL EN ISO 13849-1	a	b	c	d	e	
SIL EN 62061 - IEC 61508	-	1	2	3	(4)	
PFHd	10 ⁻⁴	10 ⁻⁵	3x10 ⁻⁶	10 ⁻⁶	10 ⁻⁷	10 ⁻⁸
Ein gefährlicher Ausfall pro Jahre	~1	~10	~40	~100	~1000	~10000

Tabelle 1 –Empfohlene Anwendungen nach IEC 62061 und EN ISO 13849-1

Angewandte Technologie beim sicherheitsbezogenem Teil des Steuerungssystems	EN ISO 13849-1	IEC 62061
A Nicht elektrische, z.B.: hydraulische	X	Nicht behandelt
B Elektromechanische, z.B.: Relais und/oder unkomplizierte Elektroniken	Beschränkt auf die festgesetzte Bauweise und bis PL=e	Alle Bauweisen und bis SIL 3
C Komplizierte Elektroniken, z.B.: programmierbare	Beschränkt auf die festgesetzte Bauweise und bis PL=d	Alle Bauweisen und bis SIL 3
D A mit B kombiniert	Beschränkt auf die festgesetzte Bauweise und bis PL=e	X ^c
E C mit B kombiniert	Beschränkt auf die festgesetzte Bauweise (siehe Hinweis 1) und Bis PL=d	Alle Bauweisen und bis SIL 3
F C kombiniert mit A oder C kombiniert mit A oder B	X ^a	X ^c

X Diese Zeile wird von der internationalen Norm wie in der Überschrift geschrieben steht, behandelt

a. Die festgesetzten Bauweisen sind im Punkt 6.2 (EN ISO 13849-1) bestimmt, um den Ansatz bei der Bewertung des Performance Levels zu vereinfachen

b. Für komplizierte Elektroniken sollen die in diesem Teil der Norm EN ISO 13849-1 und bis PL=d festgesetzten Bauweisen verwendet werden oder jede andere Bauart in Übereinstimmung mit der Norm IEC 62061.

c. Für nicht elektrische Technologien sollen die Abschnitte des Untersystems in Übereinstimmung mit diesem Abschnitt der Norm EN ISO 13849-1 verwendet werden

Hinweis: Diese Tabelle ist eine nicht offizielle Übersetzung der Tabelle, die die Norm EN ISO 13849-1:2006 in englischer Sprache beinhaltet

Die Wahl der Norm bleibt dem Hersteller, in Funktion der angewandten Technologie, überlassen. Wir glauben, daß die Norm EN 13849 durch den mittelbaren Ansatz und die Wiederverwendung der schon bekannten Begriffe leichter zu interpretieren ist.

Hinweis: Das Deutsche Institut für Arbeitsschutz BGIA hat im Jahr 2008 einen Report (BGIA Report 2/2008) über die Anwendung der Norm EN 13849 eingeführt; in diesem werden erklärt, daß die Empfehlungen und Grenzen zur Anwendung der Norm 13849 als veraltet anzusehen sind und daher auch die Grenze bei der programmierbaren Elektronik (Beispiel C und E der obenstehenden Tabelle) wie PL_e zu betrachten sind.

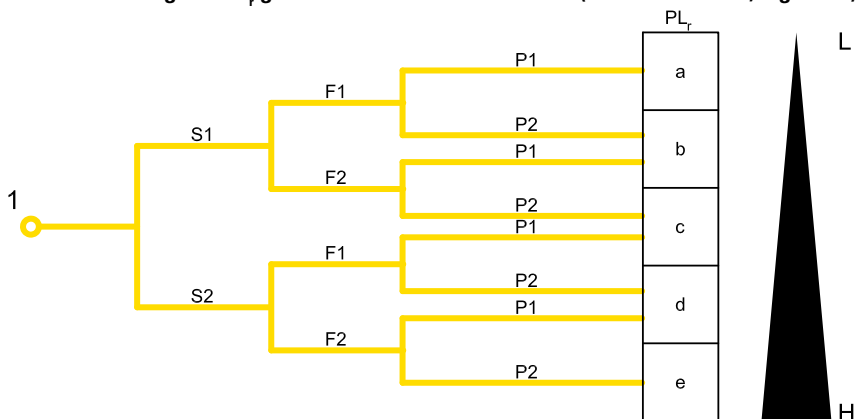
5- Die Norm EN ISO 13849 und die neuen Parameter: PL, MTTF_d, DC, CCF

Die Norm EN ISO 13849 liefert dem Hersteller eine Methode um abzuschätzen, ob Gefährdungen die von einer Maschine ausgehen, durch die Anwendung bestimmter Sicherheitsfunktionen auf ein annehmbares Restniveau beschränkt werden können. Die angewandte Methode sieht für jedes Risiko einen Zyklus von Hypothese-Analyse-Prüfung vor; am Ende desselben muss vorgewiesen werden können, dass jede gewählte Sicherheitsfunktion dem relativ zu prüfenden Risiko gerecht wird.

Der erste Schritt besteht in der Wahl des geforderten Leistungsniveaus, das von jeder Sicherheitsfunktion verlangt wird. Wie die Norm EN 654-1 verwendet auch die Norm EN 13849 einen Risikographen zur Risikoanalyse einer Maschinenfunktion (Figur A). Diese bestimmt in Funktion des Risikos anstatt einer Sicherheitskategorie ein gefordertes Leistungsniveau oder PL_r (Required Performance Level) zur Sicherheitsfunktion, die einen bestimmten Teil der Maschine schützen wird.

Der Maschinenhersteller, ausgehend von Punkt 1 der Zeichnung und auf die Fragen S, F und P antwortend, kann so den PL_r zur Sicherheitsfunktion ermitteln. Danach muss er ein System realisieren um die Bedienperson zu schützen und das ein Leistungsniveau dem PL_r gleich oder besser ist aufweist.

Risikograph zur Bestimmung des PL_r gemäß der Sicherheitsfunktion (EN ISO 13849-1, Figur A.1)



Auswertung

- 1** Ausgangspunkt zur Einschätzung der Risikominderung gegeben von den Sicherheitsfunktionen
- L** Niedriger Anteil zur Risikominderung
- H** Hoher Anteil zur Risikominderung
- PL_r** Gefordertes Leistungsniveau

Risikoparameter

S Schwere der Verletzung

- S1** Leicht (üblicherweise reversible Verletzung)
- S2** Ernst (üblicherweise irreversible Verletzung einschließlich Tod)

F Häufigkeit und/oder Dauer der Gefährdungsexposition

- F1** Selten bis weniger häufig und/oder die Dauer der Gefährdungsexposition ist kurz
- F2** Häufig bis dauernd und/oder Dauer der Gefährdungsexposition ist lang

P Möglichkeit zur Vermeidung der Gefährdung oder Begrenzung des Schadens

- P1** möglich unter bestimmten Bedingungen
- P2** kaum möglich

Für einen Maschinenhersteller könnte es von Interesse sein die Risikoanalyse der Maschine nicht wiederholen zu müssen, sondern zu versuchen die schon erprobte Risikoanalyse der Norm EN 954-1 wiederzuverwenden. Dies ist im allgemeinen nicht möglich, da sich mit der neuen Norm der Risikograph geändert hat (siehe Figur A.1) und daher können bei gleichbleibendem Risiko die geforderten Funktionsniveaus der Sicherheit geändert werden. Das Deutsche Institut BGIA empfiehlt im Report 2008/2 bezüglich der Norm EN ISO 13849 folgendes: bei Anwendung eines mit dem Kriterium ausgezeichneten „schlechtesten Falls“, kann man eine Umsetzung, wie aus der folgenden Tabelle zu ersehen ist, anwenden.

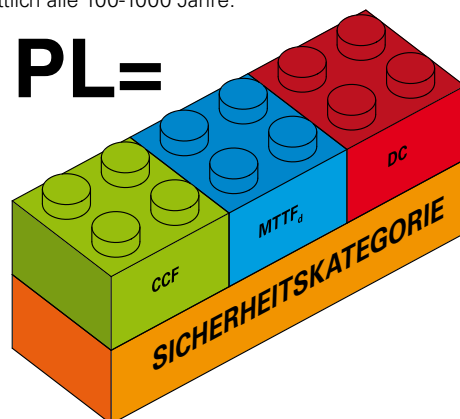
Erforderliche Kategorie nach EN 954-1:1996	Erforderlicher Performance Level (PL _r) und erforderliche Kategorie nach EN ISO 13849-1:2006
B	→ b
1	→ c
2	→ d, Kategorie 2
3	→ d, Kategorie 3
4	→ e, Kategorie 4

Der PL wird in fünf Niveaus nach der Risikosteigerung eingestuft von PL_a bis PL_e jedes dieser identifiziert einen numerischen Bereich der Wahrscheinlichkeit eines gefährlichen Schadens pro Stunde. Zum Beispiel weist PL_d drauf hin, daß die Möglichkeit gefährlicher Schäden pro Stunde im Durchschnitt zwischen 1×10^{-6} und 1×10^{-7} liegen. d.h. ungefähr 1 Ausfall durchschnittlich alle 100-1000 Jahre.

PL	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde PFHd (1/h)	
a	$\geq 10^{-5}$	$< 10^{-4}$
b	$\geq 3 \times 10^{-6}$	$< 10^{-5}$
c	$\geq 10^{-6}$	$< 3 \times 10^{-6}$
d	$\geq 10^{-7}$	$< 10^{-6}$
e	$\geq 10^{-8}$	$< 10^{-7}$

Zur Ermittlung des PL eines Steuerungssystems benötigt man mehrere Parameter:

1. Die Sicherheitskategorie des Systems abhängig von der Architektur(Struktur) des Steuerungssystems und des Verhaltens bei Schäden.
2. MTTF_d der Bauelemente
3. DC oder Diagnosedeckungsgrad des Systems.
4. CCF oder Ausfall infolge gemeinsamer Ursachen.





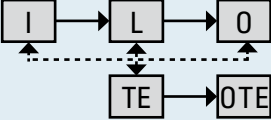
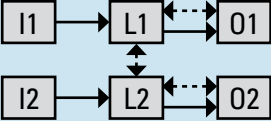
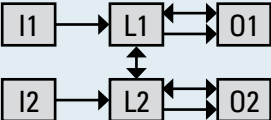
Sicherheitskategorie

Der Großteil der üblich angewandten Steuerungen werden durch eine logische Blockstruktur des Typs vertreten :

- Input oder Signaleingang
- Logik oder Signalverarbeitungslogik
- Output oder Ausgang des Überwachungssignals

untereinander verschieden verbunden gemäß der Steuerungsstruktur.

Die Norm EN ISO 13849 lässt fünf verschiedene grundlegende Steuerungsstrukturen zu; diese bezeichnet man als festgeschriebene Bauweise. Die Architekturen erstellt kombiniert mit den Anforderungen des Schadenverhaltens des Systems und der Minimalwerte von $MTTF_d$, DC und CCF die Sicherheitskategorie des Steuerungssystems wie aus der folgenden Tabelle zu ersehen ist. Die Sicherheitskategorien der Norm EN ISO 13849-1 sind also nicht gleichwertig sondern erweitern das Konzept der Sicherheitskategorie, das in der vorhergegangenen Norm EN 954-1 eingeführt wurde.

Kategorie	Aufstellung der Anforderungen	Verhalten des Systems	Richtlinien zur Sicherheit	$MTTF_d$ jedes Kanals	DC_{avg}	CCF
B	Die relevanten Teile, die zur Sicherheit der Überwachungssysteme und/oder deren Schutzeinrichtungen dienen, sowohl als auch deren Zubehör, müssen gemäß der zugehörigen Normen geplant, gebaut, ausgewählt und kombiniert werden um den vorgesehenen Einflüssen zu widerstehen. Es müssen grundlegende Sicherheitsprinzipien angewandt werden. Architektur: 	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen.	Hauptsächlich von der Auswahl der Teile charakterisiert	Niedrig bis mittel	Kein	Nicht beträchtlich
1	Es werden die Anforderungen der Kategorie B angewandt. Es müssen bewährte Teile und Sicherheitsprinzipien verwendet werden. Architektur: 	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen aber die Wahrscheinlichkeit des Auftretens eines Fehlers ist geringer als die der Kategorie B.	Hauptsächlich von der Auswahl der Teile charakterisiert	Hoch	Kein	Nicht beträchtlich
2	Es werden die Anforderungen der Kategorie B und die Anwendung der bewährten Sicherheitsprinzipien angewandt. Die Sicherheitsfunktion muß in geeigneten Zeittakten vom Steuerungssystem getestet werden. Architektur: 	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen. Der Verlust der Sicherheitsfunktion wird durch die Kontrolle erhoben.	Hauptsächlich von der Struktur charakterisiert	Niedrig bis hoch	Niedrig bis mittel	Siehe den Anhang F
3	Es werden die Anforderungen der Kategorie B und die Anwendung der bewährten Sicherheitsprinzipien angewandt. Die wichtigen Teile, die der Sicherheit dienen, müssen so geplant werden, daß -ein einzelner Fehler in einer dieser Teile nicht zum Verlust der Sicherheitsfunktion führt -wo möglich, jeder einzelne Fehler festgestellt wird Architektur: 	Wenn ein einzelner Fehler auftritt, wird die Sicherheitsfunktion immer ausgeführt. Nicht festgestellte Fehleranhäufungen können zum Verlust der Sicherheitsfunktion führen.	Hauptsächlich von der Struktur charakterisiert	Niedrig bis hoch	Niedrig bis mittel	Siehe den Anhang F
4	Es werden die Anforderungen der Kategorie B und die Anwendung der bewährten Sicherheitsprinzipien angewandt. Die wichtigen Teile, die der Sicherheit dienen, müssen so geplant werden, daß -ein einzelner Fehler einer dieser Teile nicht zum Verlust der Sicherheitsfunktion führt -ein einzelner Fehler im Monat oder vor der neuerlichen Nachfrage der Sicherheitsfunktion festgestellt wird. Falls dies nicht möglich ist, dürfen die Fehleranhäufungen nicht zum Verlust der Sicherheitsfunktion führen. Architektur: 	Wenn ein einzelner Fehler auftritt, wird die Sicherheitsfunktion immer ausgeführt. Die Erhebung der angehäuften Fehler vermindert die Möglichkeit des Verlusts der Sicherheitsfunktion (hoher DC). Die Fehler werden zeitlich erkannt, um den Verlust der Sicherheitsfunktion auszuschließen.	Hauptsächlich von der Struktur charakterisiert	Hoch	Hoch einschließlich der Fehleranhäufung	Siehe den Anhang F

MTTF_d ("Mean Time To Dangerous Failure", Mittlere Zeit bis zum gefahrbringendem Ausfall)

Dieser Parameter versucht die qualitative Güte der Teile des Systems zu bestimmen, mit dem Mittelwert ohne schadhafte Ausfall (kein allgemeiner Schaden) ausgedrückt in Jahren. Die Berechnung der MTTF_d basiert auf den Werten der Zahlen, die von den Herstellern von jedem

einzelnen Bauteil des Systems geliefert wird. Bei Fehlen dieser Daten liefert die Norm Werte in eigenen Inhalts-Tabellen (Anhang C der Norm EN ISO 13849-1). Die Auswertung führt zu einem numerischen Wert, aufgeteilt in drei Kategorien: Hoch, Mittel oder Niedrig.

Klassifikation	Werte
Nicht angemessen	MTTF _d < 3 Jahre
Niedrig	3 Jahre ≤ MTTF _d < 10 Jahre
Mittel	10 Jahre ≤ MTTF _d < 30 Jahre
Hoch	30 Jahre ≤ MTTF _d ≤ 100 Jahre

Bei stark verschleißbehafteten Bauteilen (typisch bei mechanischen oder hydraulischen Vorrichtungen) liefert der Hersteller anstatt der MTTF_d des Bauteils den Wert B10d des Bauteils, das heißt die Anzahl der Vorgänge des Bauteils innerhalb dessen 10% der Muster gefährlich beschädigt wurden.

Der Wert B10d des Bauteils muß vom Maschinenhersteller durch die folgende Formel in MTTF_d umgewandelt werden:

$$MTTF_d = \frac{B_{10d}}{0,1 \cdot n_{op}}$$

n_{op} = Anzahl der Vorgänge des Bauteils pro Jahr.

Durch die Hypothese der täglichen Anwendung und den täglichen Arbeitsstunden der Maschine n_{op} kann man wie folgt errechnen:

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600s/h}{t_{ciclo}}$$

d_{op} = Arbeitstage pro Jahr

h_{op} = Arbeitsstunden pro Tag

t_{ciclo} = Zyklusdauer (s)

Bei nicht verschleißfesten Bauteilen muß man also beachten, daß der Parameter MTTF_d nicht nur vom Bauteil selbst abhängig ist sondern auch von der Anwendung. Eine Vorrichtung mit niedriger Anwendungshäufigkeit, wie zum Beispiel ein Fernschalter, der nur für Notausschaltungen eingesetzt wird, wird eine hohe MTTF_d haben; falls dieselbe Vorrichtung auch für normale Vorgangszyklen angewandt wird könnte die MTTF_d desselben Fernschalters mit einer niedrigen Zyklusdauer, sehr stark sinken.

Zur Berechnung der MTTF_d der Steuerungen tragen alle Elemente, in Funktion seiner Struktur, der jeweiligen Schaltung bei. In Steuerungen mit einkanaliger Architektur (wie in den Fällen der Kategorie B, 1 und 2) ist der Beitrag jedes Teils linear und die Berechnung der MTTF_d des Kanals entsteht wie folgt

$$\frac{1}{MTTF_d} = \sum_{i=1}^N \frac{1}{MTTF_{di}}$$

Um zu optimistische Auslegungen zu vermeiden ist der maximale Wert der MTTF_d jedes Kanals auf 100 Jahre beschränkt. Kanäle mit einer MTTF_d von weniger als 3 Jahren sind nicht erlaubt.

Bei zweikanaligen Systemen (Kategorie 3 und 4) berechnet man den MTTF_d der Schaltung durch die Symmetrien der MTTF_d der beiden Kanäle mit der Formel:

$$MTTF_d = \frac{2}{3} \left[MTTF_{dc1} + MTTF_{dc2} - \frac{1}{\frac{1}{MTTF_{dc1}} + \frac{1}{MTTF_{dc2}}} \right]$$

DC ("Diagnostic Coverage", Diagnosedeckungsgrad).

Dieser Parameter versucht zu zeigen, wo das System eine eventuelle eigene Fehlfunktion selbst überwachen kann. Anhand des Prozentsatzes der erhobenen gefährlichen Schäden, wird man eine mehr oder weniger gute Deckungsdiagnostik haben. Der numerische Parameter DC ist ein Prozentwert, der durch die in der Tabelle (Anhang E der Norm EN ISO 13849-1) gegebenen Werte, in Funktion der angewandten Maßnahmen des Herstellers zur Erhebung der Unregelmäßigkeiten der Schaltung, errechnet wird. Da normalerweise in derselben Schaltung mehrere Maßnahmen getroffen werden um verschiedene Unregelmäßigkeiten zu erheben, wird man am Ende einen Mittelwert oder eine DC_{avg} berechnen, die vier Bereichen zugeordnet werden kann:

Hoch DC_{avg} ≥ 99%

Mittel 90% ≤ DC_{avg} < 99%

Niedrig 60% ≤ DC_{avg} < 90%

Null 60% < DC_{avg}

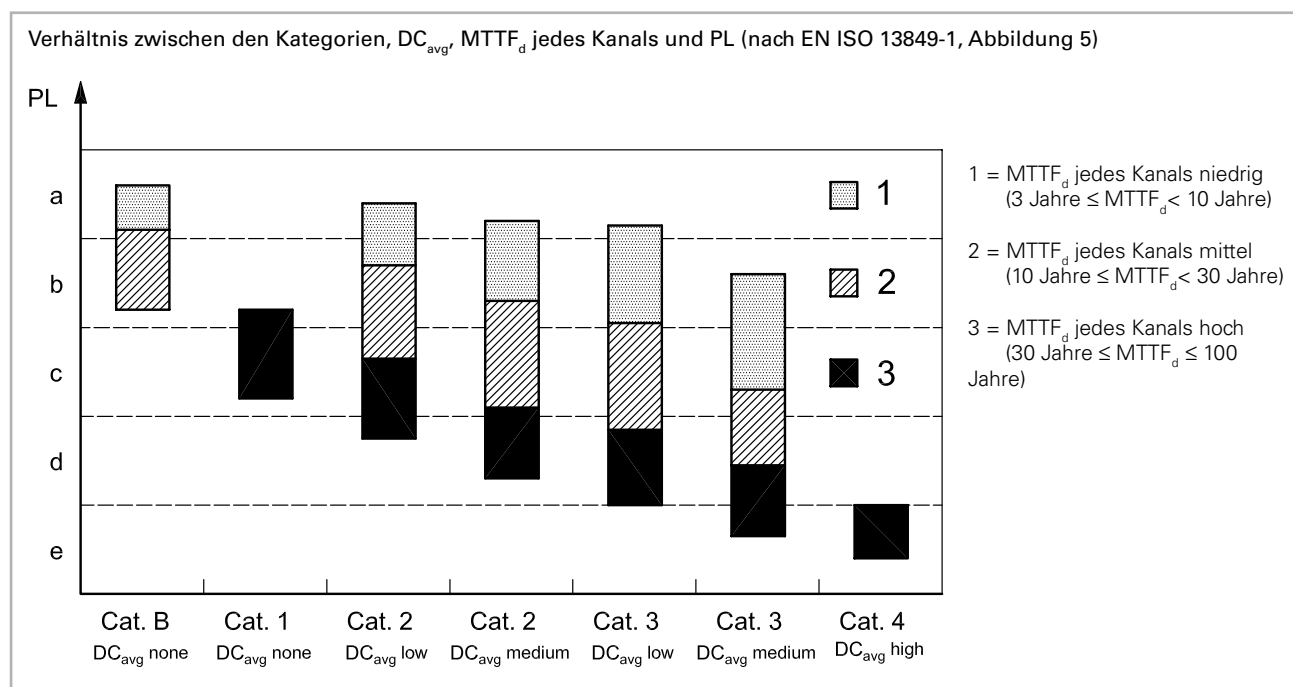
Der Diagnosedeckungsgrad Null ist nur für die Systeme der Kategorie B oder 1 gestattet.

CCF ("Common Cause Failures", Ausfall infolge gemeinsamer Ursachen).

Nur bei Systemen in Kategorie 2,3, oder 4 ist zur Berechnung des PL ist auch die Bewertung eventueller allgemeiner Schadenursachen oder CCF nötig, welche die Redundanz der Systeme für ungültig erklären können. Die Bewertung wird durch eine Check-List (Anhang F der Norm EN ISO 13849-1) durchgeführt; diese erteilt eine Wertung von 0 bis 100 je nach den angewandten Maßnahmen gegen übliche Schäden. Der minimale zugelassene Wert für die Kategorien 2,3 und 4 sind 65 Punkte.

PL ("Performance Level")

Nach Bekanntsein dieser Daten, liefert die Norm EN ISO 13849-1 den PL des Systems mit einer Zuordnungstabelle (Anhang K der Norm EN ISO 13849-1) oder mit einer vereinfachten, grafischen Darstellung (Punkt 4.5 der Norm EN ISO 13849-1), wie aus der folgenden Abbildung zu ersehen ist.



Diese Abbildung ist sehr nützlich, da sie mehrere Lesemöglichkeiten bietet. Bei einem gewissen PL_r hebt sie alle möglichen Lösungen hervor, die dieses Niveau des PL_r bietet, das heißt, die möglichen Schaltungsstrukturen die denselben PL_r liefern.

Bei näherer Betrachtung der Abbildung kann man feststellen, daß es zur Erreichung eines Systems mit PL_r gleich "c" folgende Möglichkeiten gibt:

1. System in Kategorie 3 mit nicht sehr zuverlässigen Teilen ($MTTF_d$ =niedrig) und DC mittel.
2. System in Kategorie 3 mit zuverlässigen Teilen ($MTTF_d$ =mittel) und DC niedrig.
3. System in Kategorie 2 mit zuverlässigen Teilen ($MTTF_d$ =mittel) und DC mittel.
4. System in Kategorie 2 mit zuverlässigen Teilen ($MTTF_d$ =mittel) und DC niedrig.
5. System in Kategorie 1 mit sehr zuverlässigen Teilen ($MTTF_d$ =hoch).

Nach der Wahl der Schaltungsstruktur erlaubt die Abbildung sofort die maximal zu erreichenden Werte zu erkennen, in Funktion der mittleren Deckungsdiagnostik und der $MTTF_d$ der Teile.

Der Hersteller kann also vorab einige Stromkreisstrukturen ausschließen, da diese nicht dem geforderten PL_r entsprechen.

Normalerweise bezieht man sich nicht auf die Abbildung um den PL_r zu ermitteln, da sich in vielen Fällen die Grafikbereiche mit den Grenzl意思en der verschiedenen PL_r überschneiden. Man verwendet anstatt die Tabelle des Anhangs K der Norm EN ISO 13849-1 für eine genaue Festsetzung des PL_r des Stromkreises.

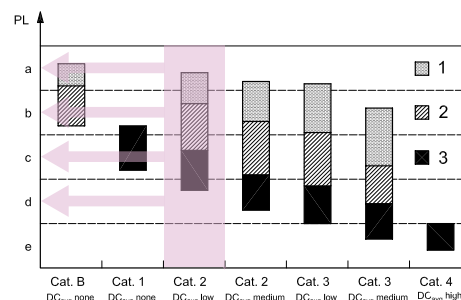
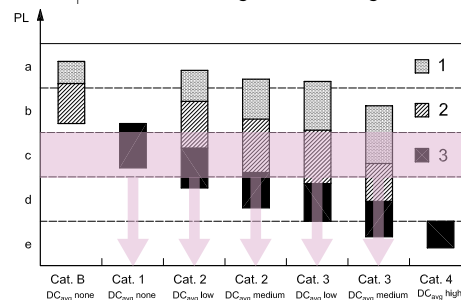


Tabelle der Sicherheitsparameter (2011)

Die in der Tabelle angeführten Daten B10 und B10d beziehen sich auf das Schaltspiel der sicheren Kontakte (Ö mit Zwangsöffnung) der Vorrichtungen unter normalen Umwelteinflüssen. Mission time (für alle hier unten aufgeführten Artikel): 20 Jahr.

Serie	Artikelbeschreibung	B10	B10 _d	B10/ B10 _d
F•••••	Positionsschalter	20.000.000	40.000.000	50%
F•••93 F•••92 F•••99 F•••R2	Sicherheitsschalter mit getrenntem Betätiger	1.000.000	2.000.000	50%
FS, FG	Sicherheitsschalter mit getrenntem Betätiger mit Verriegelung	1.000.000	5.000.000	20%
F•••96 F•••95	Sicherheitsschalter für Scharniere	1.000.000	5.000.000	20%
F•••C•	Schalter mit Schwenkhebel für Schutztüren	1.000.000	2.000.000	50%
F•••••	Seilzugschalter zur Notausschaltung	1.000.000	2.000.000	50%
HP	Sicherheitsscharniere	1.000.000	5.000.000	20%
SR	Magnetische Sicherheitssensoren (Anwendung mit Sicherheitsmodulen Pizzato)	10.000.000	20.000.000	50%
SR	Magnetische Sicherheitssensoren (max. Spannung: 24V 250mA)	5.000.000	10.000.000	50%
PX, PA	Fußschalter	20.000.000	40.000.000	50%
MK	Mikroschalter	10.000.000	20.000.000	50%
NA, NB, NF	Modulare vorverkabelte Schalter	20.000.000	40.000.000	50%
E2 1PE••••••	Not-Aus-Drucktasten	300.000	600.000	50%
E2 C•••••••	Kontakteinheiten	20.000.000	40.000.000	50%

Code	Artikelbeschreibung	MTTF _d	DC	PFH _d	SIL CL	PL	Cat
CS AM-01	Sicherheitsmodul zur Feststellung Motorstillstand	145	M	1.94E-09	2	d	3
CS AR-01	Sicherheitsmodul zur Schutztürüberwachung und Notausschaltung	147	H	6.38E-10	3	e	4
CS AR-02	Sicherheitsmodul zur Schutztürüberwachung und Notausschaltung	147	H	6.38E-10	3	e	4
CS AR-04	Sicherheitsmodul zur Schutztürüberwachung und Notausschaltung	147	H	6.38E-10	3	e	4
CSAR-04V024	Sicherheitsmodul zur Schutztürüberwachung und Notausschaltung	218	H	4,58E-10	3	e	4
CS AR-05	Sicherheitsmodul zur Schutztürüberwachung und Notausschaltung und Lichtgitter	147	H	6.61E-10	3	e	4
CSAR-05V024	Sicherheitsmodul zur Schutztürüberwachung und Notausschaltung und Lichtgitter	218	H	4,58E-10	3	e	4
CS AR-06	Sicherheitsmodul zur Schutztürüberwachung und Notausschaltung und Lichtgitter	147	H	6.61E-10	3	e	4
CSAR-06V024	Sicherheitsmodul zur Schutztürüberwachung und Notausschaltung und Lichtgitter	218	H	4,58E-10	3	e	4
CS AR-07	Sicherheitsmodul zur Schutztürüberwachung und Notausschaltung	111	H	7.56E-10	3	e	4
CS AR-08	Sicherheitsmodul zur Schutztürüberwachung und Notausschaltung und Lichtgitter	218	H	4.58E-10	3	e	4
CS AR-20	Sicherheitsmodul zur Schutztürüberwachung und Notausschaltung	358	M	8.71E-09	3	e	3
CS AR-21	Sicherheitsmodul zur Schutztürüberwachung und Notausschaltung	358	M	8.71E-09	3	e	3
CS AR-22	Sicherheitsmodul zur Schutztürüberwachung und Notausschaltung	201	H	8.87E-09	3	e	3
CS AR-23	Sicherheitsmodul zur Schutztürüberwachung und Notausschaltung	201	H	8.87E-09	3	e	3
CS AR-24	Sicherheitsmodul zur Schutztürüberwachung und Notausschaltung	111	H	1.18E-09	3	e	3
CS AR-25	Sicherheitsmodul zur Schutztürüberwachung und Notausschaltung	111	H	1.18E-09	3	e	3
CS AR-40	Sicherheitsmodul zur Schutztürüberwachung und Notausschaltung	356	M	1.08E-08	2	d	2
CS AR-41	Sicherheitsmodul zur Schutztürüberwachung und Notausschaltung	356	M	1.08E-08	2	d	2
CS AR-46	Sicherheitsmodul zur Schutztürüberwachung und Notausschaltung	435	-	3.32E-08	1	c	1
CS AR-51	Sicherheitsmodul zur Schaltmatten und Schaltleisten	209	H	9.43E-09	3	e	4
CS AR-90	Sicherheitsmodul zur Kontrolle Etageeinfahren	382	H	5.03E-10	3	e	4
CS AR-94	Sicherheitsmodul zur Kontrolle Etageeinfahren	213	H	5.62E-09	3	e	4
CS AR-95	Sicherheitsmodul zur Kontrolle Etageeinfahren	213	H	5,42E-09	3	e	4
CS AT-0x	Schaltschützmodul zur Schutztürüberwachung und Notausschaltung	84	H	9.01E-09	3	e	4
CS AT-1x	Schaltschützmodul zur Schutztürüberwachung und Notausschaltung	84	H	9.01E-09	3	e	4
CS AT-3x	Schaltschützmodul zur Schutztürüberwachung und Notausschaltung	74	H	4.05E-09	3	e	4
CS DM-01	Sicherheitsmodul zur Kontrolle Zweihandschaltung	142	H	2.99E-08	3	e	4
CS DM-02	Sicherheitsmodul zur Kontrolle Zweihandschaltung	206	H	2.98E-08	3	e	4
CS FS-10	Schaltschützmodul	146	H	1.62E-09	3	e	4
CS FS-20	Schaltschützmodul	205	M	1.10E-08	2	d	3
CS FS-30	Schaltschützmodul	205	M	1.10E-08	2	d	3
CS FS-50	Schaltschützmodul	349	M	1.17E-08	2	d	3
CS ME-01	Schaltschützmodul	76	H	6.38E-10	3	e	4
CS ME-02	Schaltschützmodul	113	H	2.84E-09	3	e	4
CS ME-03	Schaltschützmodul	208	M	2,45 E-08	2	d	3
CS ME-20	Schaltschützmodul	113	H	3.07E-09	3	e	4
CS ME-30	Schaltschützmodul	112	H	2.77E-09	3	e	4
CS ME-31	Schaltschützmodul	112	H	2.77E-09	3	e	4

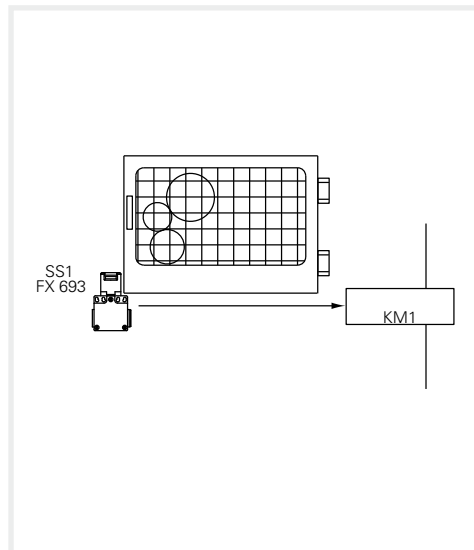
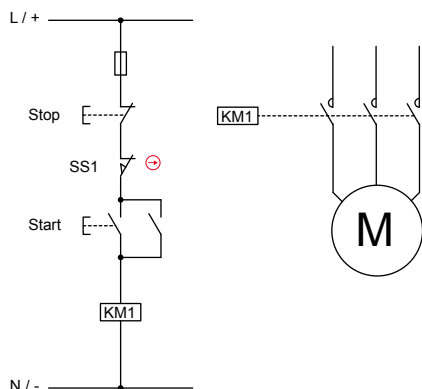
B10_d: Anzahl der Vorgänge innerhalb dessen 10% der Bauteile gefährlich beschädigt werden
 B10: Anzahl der Vorgänge innerhalb dessen 10% der Bauteile beschädigt werden
 B10/B10_d: Verhältnis zwischen gefährlichen und totalen Beschädigungen
 MTTF_d: Mean Time To Failure Dangerous (Mittlere Zeit bis zum gefahrbringenden Ausfall)
 DC: Diagnostic coverage (Diagnosedeckungsgrad)

PFH_d: Probability of Dangerous Failure per hour (Durchschnittliche Wahrscheinlichkeit eines Ausfalls je Stunde)
 SIL CL: Safety Integrity Level Claim Limit. Maximal zu erreichbarer SIL nach EN 62061
 PL: Performance Level. PL nach EN ISO 13849-1

BEISPIEL 1**Anwendung: Schutztürüberwachung**

In Bezug auf Norm EN ISO 13849-1:2006

Sicherheitskategorie	1
Performance Level	PL c



Die Steuerung in der Abbildung dient zur Überwachung der Schutztür. Bei geöffneter Schutztür darf der Motor nicht anlaufen. Die Gefährdungsanalyse hat herausgestellt, dass das System mit keinem Nachlauf ausgestattet ist, das heißt, dass der Motor nach Entnahme der Betriebsspannung in geringerer Zeit stillsteht als sich die Schutztür öffnet. Aus der Gefährdungsanalyse geht daraus hervor vor, dass das geforderte Ziel PL_r dem PL_c entspricht. Man möchte überprüfen ob die vorgesehene Steuerung mit einkanaliger Struktur, einen PL höher oder gleich wie PL_r hat.

Beschreibung der Sicherheitsfunktion

Die Schutztürposition wird vom Schalter mit getrenntem Betätiger SS, der direkt auf den Schaltschütz einwirkt, erhoben. Der Schaltschütz KM1, der die Elemente in Bewegung überwacht, wird normalerweise von den Knöpfen Start und Stop ausgelöst; die Analyse des Betriebszyklus hat aber bewiesen, dass auch die Schutztür bei jedem Schaltspiel geöffnet wird. Daraus geht hervor, dass man die Anzahl der Arbeitsgänge des Fernschalters und des Sicherheitsschalters als gleich betrachten kann.

Eine Schaltungsstruktur bezeichnet man als einkanalig ohne Überwachung (Kategorie B oder 1), wo nur das Element des Input (Schalter) und Output (Schaltschütz) vorhanden ist.

Die Sicherheitsfunktion bleibt bei einem Schaden an einer der beiden Vorrichtungen nicht erhalten.

Es wurden keine Maßnahmen zur Fehlerfeststellung getroffen.

Daten der Vorrichtungen

- SS1 ist ein Schalter mit Zwangsöffnung (Anhang K der Norm EN 60947-5-1). Der Schalter ist eine absolut geprüfte Vorrichtung laut der Tabelle D.4 der Norm EN ISO 13849-2. Der Wert B10_d der Vorrichtung wird vom Hersteller zur Verfügung gestellt (siehe Seite 7/32) und ist gleich 2.000.000 Schaltspielen.
- KM1 ist ein Schaltschütz mit Nennlast und ein absolut geprüftes Element laut der Tabelle D.4 der Norm EN ISO 13849-2. Der Wert B10_d ist gleich 2.000.000 von Schaltspielen; dieser Wert wurde von den Tabellen der Norm entnommen (siehe Tabelle C.1 der Norm EN ISO 13849-1).

Annahme der Anwendungshäufigkeit

- Man nimmt an, dass die Maschine maximal 365 Tage pro Jahr eingesetzt wird, in drei Reihenfolgen von 8 Stunden und mit einer Zeit von 600 Sekunden pro Schaltspiel. Die Anzahl der Schaltspiele pro Jahr sind für den Schalter gleich dem $n_{op} = (365 \times 24 \times 3600) / 600 = 52560$.
- Man nimmt an, dass die Maschine maximal 365 Tage pro Jahr eingesetzt wird, in drei Reihenfolgen von 8 Stunden und mit einer Zeit von 600 Sekunden pro Schaltspiel. Die Anzahl der Schaltspiele pro Jahr sind für den Schalter gleich dem $n_{op}/\text{Jahr} = 105120$
- Der Schaltschütz KM1 wird sowohl bei normalem Start-Stop als auch beim Wiederanlauf in Folge einer Öffnung der Schutzvorrichtung betätigt. $n_{op}/\text{Jahr} = 52560 + 105120 = 157680$

MTTF_d Ermittlung

MTTF_d des Schalters SS1 ist gleich: $MTTF_d = B10_d / (0,1 \times n_{op}) = 2000000 / (0,1 \times 52560) = 381$ Jahre

MTTF_d des Schalters KM1 ist gleich: $MTTF_d = B10_d / (0,1 \times n_{op}) = 2000000 / (0,1 \times 157680) = 127$ Jahre

Daraus ergibt sich eine MTTF_d des einkanaligen Stromkreises gleich: $1 / (1/381 + 1/127) = 95$ Jahre

Diagnosedeckungsgrad DC_{avg}

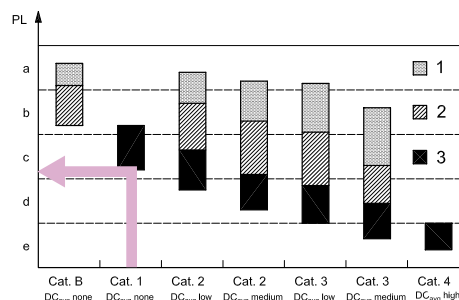
Es werden keine Maßnahmen zur Überprüfung der Schäden implementiert und daher ist der Diagnosedeckungsgrad Null, erlaubte Bedingung für die Schaltung in Kategorie 1 unter Prüfung.

Ausfall infolge gemeinsamer Ursache CCF

Die Auswertung des CCF ist für eine Schaltung in Kategorie 1 nicht nötig.

PL-Ermittlung

Mit der Tabelle oder der Abbildung 5 überprüft man, daß das Ergebnis für eine Schaltung in Kategorie 1 mit einer MTTF_d=95 Jahre, der PL der Steuerung gleich c ist und daher erfüllt wurde.



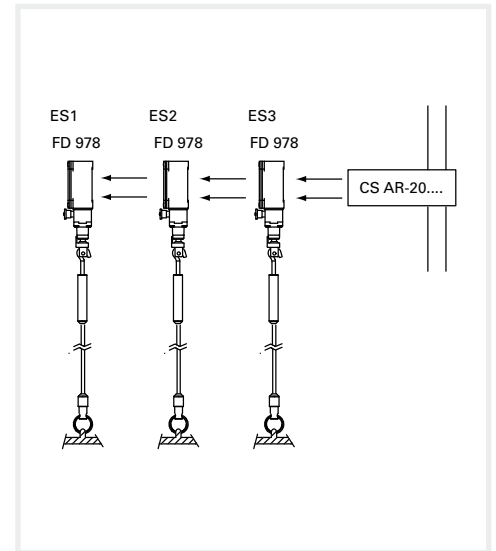
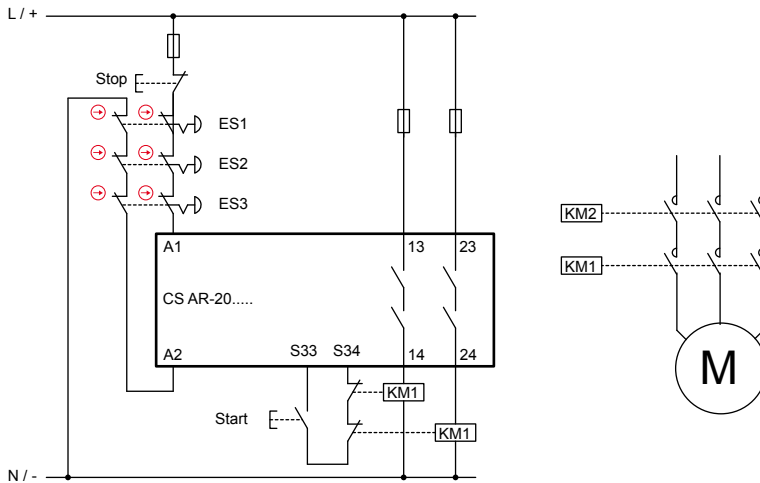
BEISPIEL 2**Anwendung: Schutzüberwachung**

In Bezug auf Norm EN ISO 13849-1:2006

Sicherheitskategorie

3

Performance Level

PL e**Beschreibung der Sicherheitsfunktion**

Die Betätigung einer der Sicherheitsvorrichtungen löst den Eingriff des Sicherheitsmodus und der Schalschütze KM1 und KM2 aus. Das Signal der Vorrichtungen ES1, ES2, ES3 wird vom Sicherheitsmodul CS redundant gelesen. Auch die Schaltschütze KM1 und KM2 (mit zwangsgeführten Kontakten) werden vom CS durch die Rückwirkungsschaltung überwacht.

Daten der Vorrichtungen

- ES1, ES2, ES3 (FD 978) sind Seilzugschalter für Not-Aus-Schaltungen mit Zwangsöffnung. Der Wert $B10_d$ ist gleich 2000000 (siehe Seite 7/32)
- KM1, KM2 sind Schaltschütze mit Nennlast. Der Wert $B10_d$ ist gleich 2000000 (siehe Tabelle C.1 der Norm EN ISO 13849-1)
- CS ist ein Sicherheitsmodul (CS AR-20) mit $MTTF_d = 358$ Jahre (siehe Seite 7/32) und DC= Mittel
- Die Bauweise der Schaltung ist doppelkanalig in Kategorie 3

Annahme der Anwendungshäufigkeit

- 2 Mal im Monat $n_{op}/\text{Jahr} = 24$
- Betätigung des Starknopfs: 4 Mal am Tag
- Bei Annahme von 365 Arbeitstagen, werden die Kontakte $4 \times 365 + 24 = 1484$ Mal/Jahr schalten
- Die Schalter werden mit derselben Frequenz betätigt
- Es ist nicht vorgesehen, daß mehrere Knöpfe gleichzeitig gedrückt werden

MTTFd Ermittlung

- $MTTF_{d,ES1,ES2,ES3} = 833333$ Jahre
- $MTTF_{d,KM1,KM2} = 13477$ Jahre
- $MTTF_{d,CS} = 358$ Jahre
- $MTTF_{d,CH1} = 349$ Jahre. Der Wertw ist auf 100 Jahre begrenzt. Die Kanäle sind parallel geschaltet, daher $MTTF_d = 100$ Jahre (Hoch)

Diagnosedeckungsgrad DC_{avg}

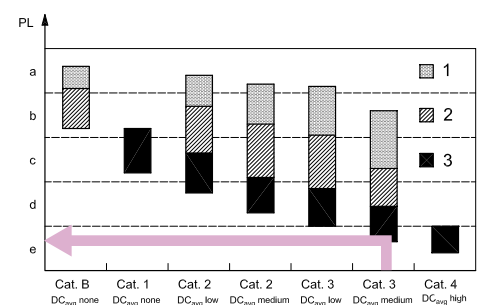
- Die Kontakte KM1 und KM2 werden vom CS durch die Rückwirkungsschaltung überwacht. $DC = 99\%$ (Hoch)
- Das Sicherheitsmodul CS AR-20 hat einen Diagnosedeckungsgrad Mittel
- Nicht alle Schäden können bei den Serien der Sicherheitsvorrichtungen festgestellt werden. Der Diagnosedeckungsgrad ist 90% (Mittel.)

Ausfall infolge gemeinsamer Ursache CCF

Bei Anahme einer Auswertung > 65 (Basierend auf Anhang F der Norm EN ISO 13849-1).

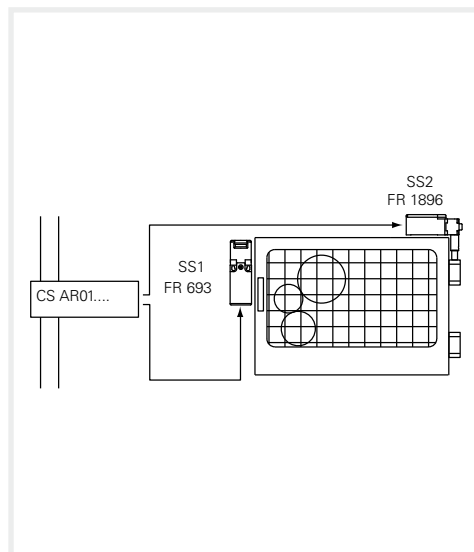
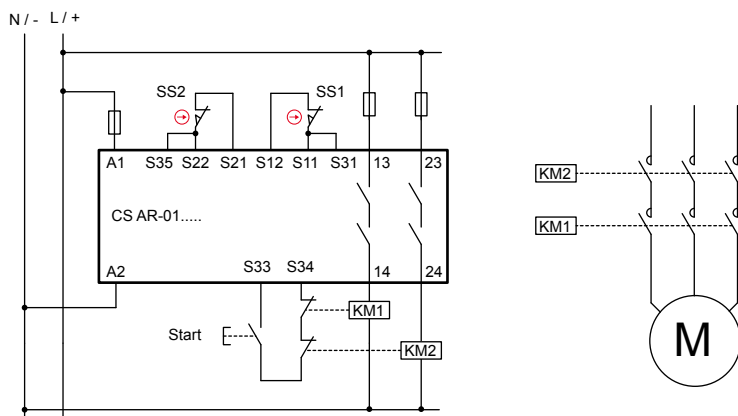
PL-Ermittlung

Eine Schaltung in Kategorie 3 mit $MTTF_d = 100$ Jahre und DC_{avg} entspricht einem PL e



BEISPIEL 3**Anwendung: Schutztürüberwachung**

In Bezug auf Norm EN ISO 13849-1:2006

Sicherheitskategorie **4**
Performance Level **PL e****Beschreibung der Sicherheitsfunktion**

Die Öffnung der Schutztür löst den Eingriff der Schalter SS1 und SS2 bzw. des Sicherheitsmoduls und der beiden Schaltschütze KM1 und KM2 aus.

Das Signal der Vorrichtungen SS1, SS2 wird vom Sicherheitsmodul Cs redundant gelesen.

Die Schalter haben verschiedene Arbeitsweiseprinzipien.

Auch die Schaltschütze KM1 und KM2 (mit zwangsgeführten Kontakten) werden vom CS durch die Rückwirkungsschaltung überwacht.

Daten der Vorrichtungen

- SS1 (FR 693) ist ein Schalter mit Zwangsöffnung. Der Wert $B10_d$ ist gleich 2000000 (siehe Seite 7/32)
- SS2 (FR 1896) ist ein Schalter für Scharniere mit Zwangsöffnung. $B10_d = 5000000$ (siehe Seite 7/32)
- KM1, KM2 sind Schaltschütze mit Nennlast. $B10_d = 2000000$ (siehe Tabelle C.1 der Norm EN ISO 13849-1)
- CS sind Sicherheitsmodule (CS AR-01) mit $MTTF_d = 147$ Jahre und $DC = 99\%$ (Hoch)

Annahme der Anwendungshäufigkeit

365 Tage/Jahr, 16 h/Tag, 1 Eingriff alle 4 Minuten (240 s). $n_{op}/\text{Jahr} = 87600$

MTTFd Ermittlung

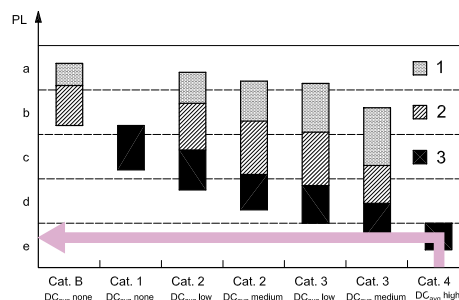
- $MTTF_{d, SS1} = 228$ Jahre
- $MTTF_{d, SS2} = 571$ Jahre
- $MTTF_{d, KM1, KM2} = 228$ Jahre
- $MTTF_{d, CS} = 147$ Jahre
- $MTTF_{d, CH1} = 64$ Jahre (SS1, CS, KM1)
- $MTTF_{d, CH2} = 77$ Jahre (SS2, CS, KM2)
- $MTTF_d$: bei Paralleler Schaltung der beiden Kanäle 70,5 Jahre (Hoch)

Diagnosedeckungsgrad DC_{avg}

- SS1, SS2 haben $DC = 99\%$, da die Kontakte SS1 und SS2 vom CS überwacht werden und verschiedene Arbeitsweiseprinzipien haben.
- Die Kontakte KM1 und KM2 werden vom CS durch die Rückwirkungsschaltung überwacht. $DC = 99\%$ (High)
- CS AR-01 besitzt eine selbstüberprüfende redundante Schaltung. $DC = 99\%$ (High)
- $DC_{avg} = 99\%$ (Hoch)

PL-Ermittlung

Eine Schaltung in Kategorie 4 mit $MTTF_d = 70,5$ Jahre und $DC_{avg} = \text{Hoch}$ entspricht einem PL e



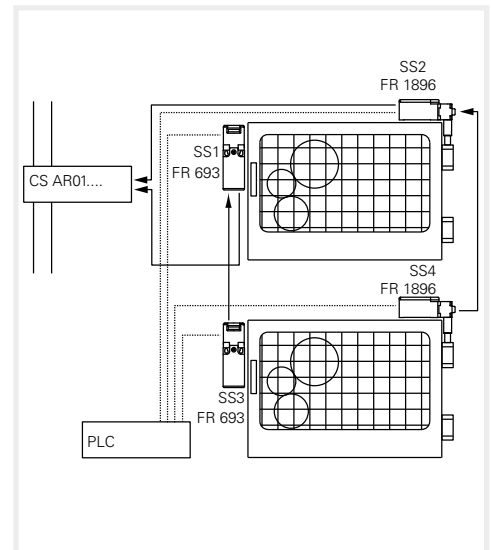
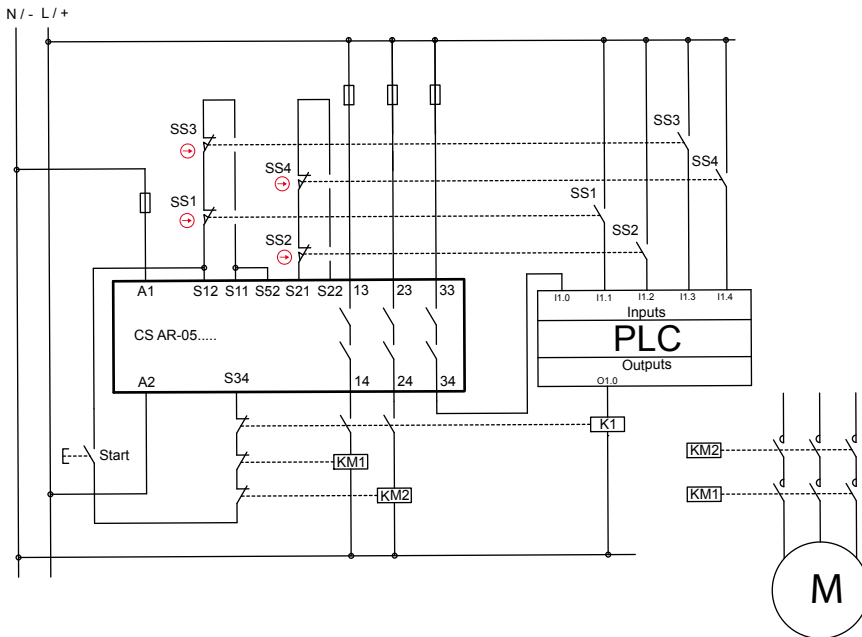
BEISPIEL 4**Anwendung: Schutzüberwachung**

In Bezug auf Norm EN ISO 13849-1:2006

Sicherheitskategorie

4

Performance Level

PL e**Beschreibung der Sicherheitsfunktion**

Die Öffnung einer Schutztür löst den Eingriff der Schalter SS1, SS2 auf den ersten Schutz und SS3, SS4 auf den zweiten Schutz aus, die Schalter schalten das Sicherheitsmodul und die beiden Schaltschütze KM1 und KM2 ein.

Das Signal der Vorrichtungen SS1, SS2 und SS3, SS4 wird vom Sicherheitsmodul CS redundant überwacht, weiterhin wird ein Hilfskontakt der Schalter vom PLC überwacht.

Die Schalter haben verschiedene Arbeitsweiseprinzipien.

Auch die Schaltschütze KM1 und KM2 (mit zwangsgeführten Kontakten) werden vom CS durch die Rückwirkungsschaltung überwacht.

Daten der Vorrichtungen

- SS1 (FR 693) ist ein Schalter mit Zwangsöffnung. Der Wert $B10_d$ ist gleich 2000000 (siehe Seite 7/32)
- SS2 (FR 1896) ist ein Schalter für Scharniere mit Zwangsöffnung. $B10_d = 5000000$ (siehe Seite 7/32)
- KM1, KM2 sind Schaltschütze mit Nennlast. $B10_d = 2000000$ (siehe Tabelle C.1 der Norm EN ISO 13849-1)
- CS sind Sicherheitsmodule (CS AR-01) mit $MTTF_d = 147$ Jahre und $DC = 99\%$

Annahme der Anwendungshäufigkeit

- 4 mal pro Stunde für 24 Stunden/Tag für 365 Tage/Jahr gleich $n_{op}/\text{Jahr} = 35040$
- Die Schaltschütze schalten sich um das Doppelte der Vorgänge ein = 70080

MTTFd Ermittlung

- $MTTF_d SS1, SS3 = 571$ Jahre; $MTTF_d SS2, SS4 = 1427$ Jahre
- $MTTF_d KM1, KM2 = 285$ Jahre
- $MTTF_d CS = 147$ Jahre
- $MTTF_d Ch1 = 72$ Jahre (SS1, SS3, CS, KM1)
- $MTTF_d Ch2 = 85$ Jahre (SS2, SS4, CS, KM2)
- $MTTF_d$: Bei paralleler Schaltung der beiden Kanäle ergibt sich $MTTF_d = 79$ Jahre (Hoch)

Diagnosedeckungsgrad DC_{avg}

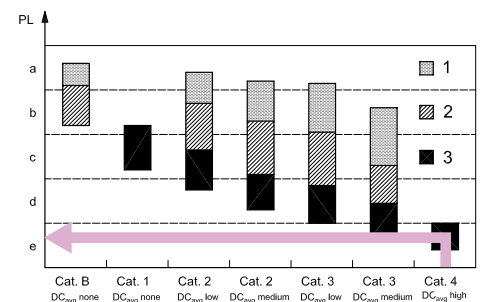
- Die Kontakte KM1 und KM2 werden vom CS durch die Rückwirkungsschaltung überwacht. $DC = 99\%$
- Die Hilfskontakte der Schalter sind vom PLC überwacht. $DC = 99\%$
- Das Modul CS AR-05 hat einen $DC = 99\%$ (siehe Seite 7/32)
- Der Deckungsgrad beider Kanäle ist 99% (High)

Ausfall infolge gemeinsamer Ursache CCF

- Bei Annahme einer Auswertung > 65 (Basis Addendum F der Norm EN ISO 13849-1)

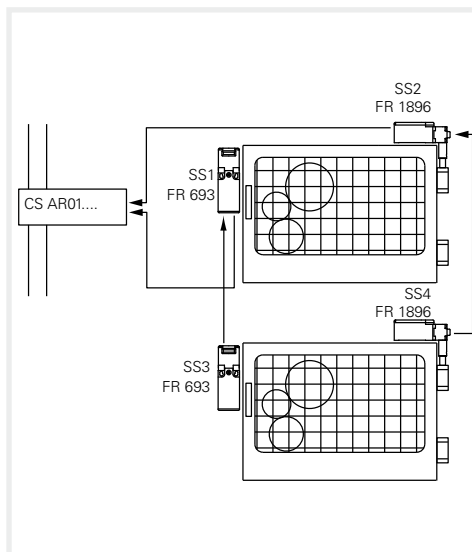
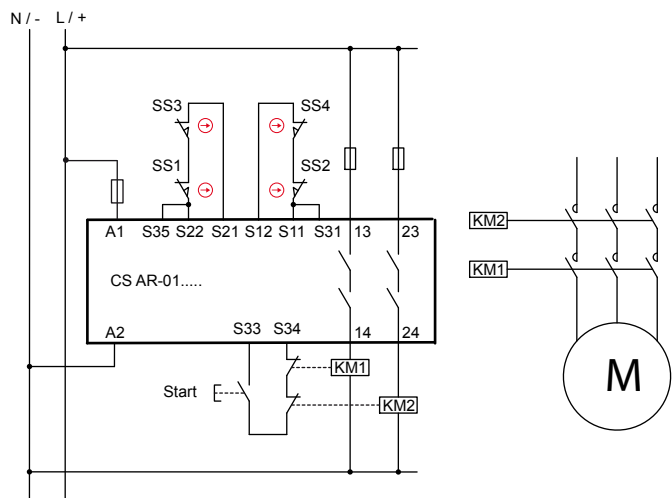
PL-Ermittlung

- Eine Schaltung in Kategorie 4 mit $MTTF_d = 79$ Jahre (Hoch) und $DC_{avg} = \text{Hoch}$ entspricht einem PL e



BEISPIEL 5**Anwendung: Schutztürüberwachung**

In Bezug auf Norm EN ISO 13849-1:2006

Sicherheitskategorie **3**
Performance Level **PL e****Beschreibung der Sicherheitsfunktion**

Die Öffnung einer Schutztür löst den Eingriff der Schalter SS1, SS2 auf den ersten Schutz und SS3, SS4 auf den zweiten Schutz aus, die Schalter schalten das Sicherheitsmodul und die beiden Schaltschütze KM1 und KM2 ein.

Das Signal der Vorrichtungen SS1, SS2 und SS3, SS4 wird vom Sicherheitsmodul CS redundant überwacht, weiterhin wird ein Hilfskontakt der Schalter vom PLC überwacht.

Die Schalter haben verschiedene Arbeitsweiseprinzipien.

Auch die Schaltschütze KM1 und KM2 (mit zwangsgeführten Kontakten) werden vom CS durch die Rückwirkungsschaltung überwacht.

Daten der Vorrichtungen

- SS1 (FR 693) ist ein Schalter mit Zwangsöffnung. Der Wert $B10_d$ ist gleich 2.000.000 (siehe Seite 7/32)
- SS2 (FR 1896) ist ein Schalter für Scharniere mit Zwangsöffnung. $B10_d = 5.000.000$ (siehe Seite 7/32)
- KM1, KM2 sind Schaltschütze mit Nennlast. $B10_d = 2.000.000$ (siehe Tabelle C.1 der Norm EN ISO 13849-1)
- CS sind Sicherheitsmodule (CS AR-01) mit $MTTF_d = 147$ Jahre und $DC = 99\%$

Annahme der Anwendungshäufigkeit

- 2 mal pro Stunde für 16 Stunden/Tag für 365 Tage/Jahr gleich $n_{op}/\text{Jahr} = 11680$
- Die Schaltschütze schalten sich um das Doppelte der Vorgänge = 23360

MTTfd Ermittlung

- $MTTF_{d, SS1, SS3} = 1712$ Jahre
- $MTTF_{d, SS2, SS4} = 4281$ Jahre
- $MTTF_{d, KM1, KM2} = 856$ Jahre
- $MTTF_{d, CS} = 147$ Jahre
- $MTTF_{d, CH1} = 109$ Jahre (SS1, SS3, CS, KM1)
- $MTTF_{d, CH2} = 118$ Jahre (SS2, SS4, CS, KM2)
- $MTTF_d =$ Wert begrenzt auf 100 Jahre

Diagnosedeckungsgrad DC_{avg}

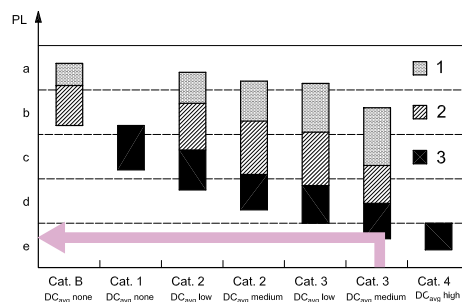
- Die Kontakte KM1 werden vom CS durch die Rückwirkungsschaltung überwacht. $DC = 99\%$
- Nicht alle Schäden können an den Schalterserien festgestellt werden. $DC = 60\%$
- Das Modul CS AR-01 hat einen $DC = 99\%$
- Der Deckungsgrad ist 92% (Mittel)

Ausfall infolge gemeinsamer Ursache CCF

- Bei Annahme einer Asuwertung > 65 (Basis Addendum F der Norm EN ISO 13849-1)

PL-Ermittlung

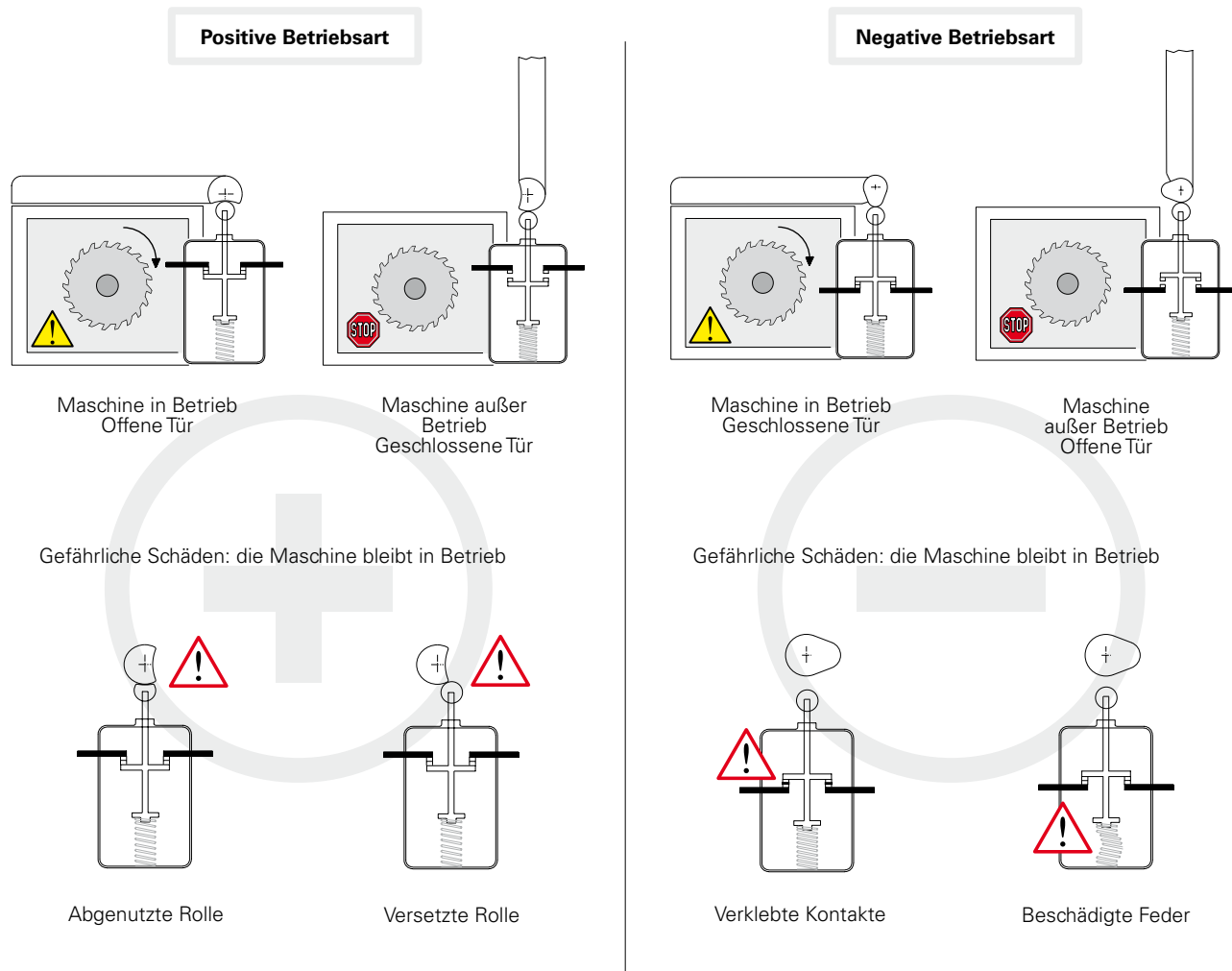
- Eine Schaltung in Kategorie 3 mit $MTTF_d = 100$ Jahre und $DC_{avg} =$ Mittel entspricht einem PL e



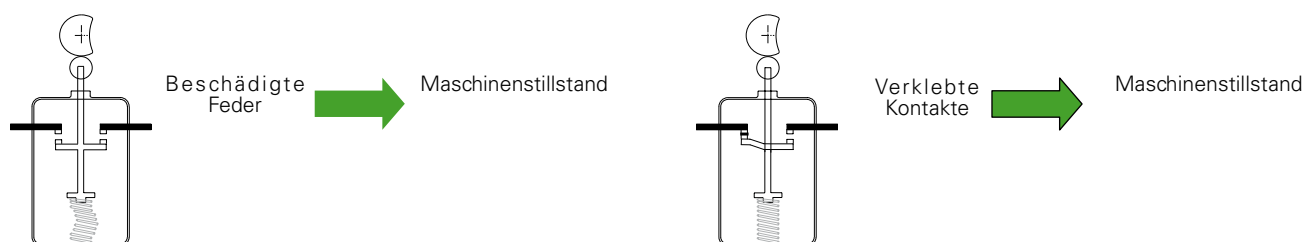
6 - Zwangsöffnung, Redundanz, Diversifikation und Selbstprüfung

Positive und negative Betriebsart


Nach der Norm EN 292-2 Punkt 3.5 sind Teile in positiver Betriebsart, wenn ein in Bewegung stehender mechanischer Teil durch direkten Kontakt oder durch Festteile einen anderen Teil mitnimmt. Man spricht dagegen von negativer Betriebsart, wenn die Versetzung eines mechanischen Teils einem zweiten Teil erlaubt, sich frei zu bewegen (z.B.: Schwerkraft, Feder, ...)

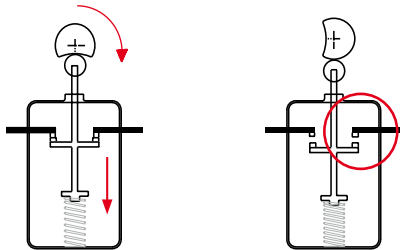


Die positive Betriebsart gibt die Möglichkeit die oben dargestellten gefährlichen Schäden durch eine vorbeugende Wartung zu umgehen. Mit der negativen Betriebsart sind die Schäden im Inneren des Schalters und daher sehr schwer behebbar. Die positive Betriebsart erlaubt die Öffnung der Kontakte auch bei inneren Schäden (verklebte Kontakte oder beschädigte Feder) und daher den Maschinenstillstand.



Einsatz der Schalter bei Sicherheitsanwendungen

Wenn nur ein Schalter bei einer Sicherheitsanwendung verwendet wird, muß derselbe in positiver Betriebsart betätigt werden. Für die Sicherheitsanwendungen wird der Öffnungskontakt (Ö) verwendet, der vom Typ "Zwangsöffnung" sein muß; alle Schalter mit dem Symbol  verfügen über Kontakte Ö mit Zwangsöffnung.



Keine elastische Verbindung zwischen den beweglichen Kontakten und dem Betätiger auf welchem die Betätigungskraft ausgeübt wird.

Wenn zwei oder mehrere Schalter vorhanden sind, sollten diese in gegengesetzter Weise arbeiten :

- Der Erste mit einem normalerweise geschlossenen Kontakt (Öffnungskontakt) und von der Schutztür in positiver Betriebsart betätigt .
 - Der Andere mit einem normalerweise geöffneten Kontakt (Schließkontakt) und von der Schutztür in nicht positiver Betriebsart betätigt.
- Dies ist ein übliches Verfahren, welches aber den Gebrauch von zwei, in positiver Betriebsart betätigten Schaltern nicht ausschließt. (siehe Diversifikation)

Diversifikation

Die Sicherheit in redundanten Systemen wird durch die Diversifikation erhöht. Diese erhält man , indem man zwei Schalter verschiedener Herstellung und/oder Technologie anwendet, um Schäden, die durch die gleichen Ursachen ausgelöst werden, zu verhindern. Beispiele einer Diversifikation sind: die Verwendung eines Schalters mit positiver Wirkung verbunden mit einem Schalter mit nicht positiver Wirkung, die Verwendung eines Schalters mit mechanischer und einer nicht mechanischen Betätigung (z.B.: elektronischer Sensor) oder die Verwendung von zwei Schaltern mit mechanischer Betätigung mit positiver Wirkung aber verschiedenen Antriebsprinzipien (z.B.: ein Schalter mit Betätiger FR 693 und ein Schalter mit Bolzen FR 1896).

Ridundanz

Die Ridundanz ist die Anwendung von mehr als einer Vorrichtung oder einem System; im Fall eines Schadens in einem der Teile, vollzieht diese Vorrichtung die Sicherheitsfunktion. Falls der erste Schaden nicht erhoben wird, könnte der zweite zum Verlust der Sicherheitsfunktion führen.

Selbstkontrolle

Die Selbstkontrolle besteht darin, den Betrieb aller Vorrichtungen, die bei der Maschine eingreifen, automatisch zu prüfen. So kann der folgende Zyklus entweder verboten oder genehmigt werden.

Ridundanz und Selbstkontrolle

Die Kombination von Ridundanz und Selbstkontrolle garantieren, daß ein Erstscha den bei Sicherheitsschaltungen nicht zum Verlust der Sicherheitsfunktionen führt. Dieser Erstscha den wird bei der Wiederü betriebsnahme festgestellt, oder auf jeden Fall vor einem zweiten Scha den, der zum Verlust der Sicherheitsfunktionen führen könnte.