

**DIN EN ISO 13849-1/A1**

ICS 13.110

Einsprüche bis 2013-11-13  
Vorgesehen als Änderung von  
DIN EN ISO 13849-1:2008-12**Entwurf**

**Sicherheit von Maschinen –  
Sicherheitsbezogene Teile von Steuerungen –  
Teil 1: Allgemeine Gestaltungsleitsätze – Änderung 1  
(ISO 13849-1:2006/DAM 1:2013);  
Deutsche Fassung EN ISO 13849-1:2006/prA1:2013**

Safety of machinery –  
Safety-related parts of control systems –  
Part 1: General principles for design – Amendment 1 (ISO 13849-1:2006/DAM 1:2013);  
German version EN ISO 13849-1:2006/prA1:2013

Sécurité des machines –  
Parties des systèmes de commande relatives à la sécurité –  
Partie 1: Principes généraux de conception – Amendement 1  
(ISO 13849-1:2006/DAM 1:2013);  
Version allemande EN ISO 13849-1:2006/prA1:2013

**Anwendungswarnvermerk**

Dieser Norm-Entwurf mit Erscheinungsdatum 2013-09-13 wird der Öffentlichkeit zur Prüfung und  
Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses  
Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter [www.entwuerfe.din.de](http://www.entwuerfe.din.de) bzw. für Norm-  
Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter [www.entwuerfe.normenbibliothek.de](http://www.entwuerfe.normenbibliothek.de),  
sofern dort wiedergegeben;
- oder als Datei per E-Mail an [nasg@din.de](mailto:nasg@din.de) möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle  
kann im Internet unter [www.din.de/stellungnahme](http://www.din.de/stellungnahme) oder für Stellungnahmen zu Norm-Entwürfen der DKE  
unter [www.dke.de/stellungnahme](http://www.dke.de/stellungnahme) abgerufen werden;
- oder in Papierform an den Normenausschuss Sicherheitstechnische Grundsätze (NASG) im DIN,  
10772 Berlin (Hausanschrift: Burggrafenstr. 6, 10787 Berlin).

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten  
Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 42 Seiten

Normenausschuss Sicherheitstechnische Grundsätze (NASG) im DIN  
Normenausschuss Maschinenbau (NAM) im DIN



## Nationales Vorwort

Dieser Änderungs-Entwurf enthält sicherheitstechnische Festlegungen.

Dieses Dokument enthält die Deutsche Fassung des vom Technischen Komitee ISO/TC 199 „Safety of machinery“ des Internationalen Komitees für Normung (ISO) in Zusammenarbeit mit dem Technischen Komitee CEN/TC 114 „Sicherheit von Maschinen“ des Europäischen Komitees für Normung (CEN) entsprechend der Vereinbarung zwischen dem CEN und ISO über die technische Zusammenarbeit (Wiener Vereinbarung) ausgearbeiteten Änderungs-Entwurfs A1:2013 zur EN ISO 13849-1:2008. Die Sekretariate beider Technischer Komitees werden vom DIN (Deutschland) gehalten.

Die nationalen Interessen bei der Erarbeitung dieses Dokuments wurden vom Gemeinschaftsarbeitsausschuss „Steuerungen“ (NA 095-01-03 GA) des Normenausschusses Sicherheitstechnische Grundsätze (NASG) mit dem NAM und der DKE im DIN wahrgenommen.

Es ist vorgesehen, diese Änderung bei der Veröffentlichung nicht separat, sondern als konsolidierte Fassung herauszugeben.

**Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen —  
Teil 1: Allgemeine Gestaltungsleitsätze – Änderung 1 (ISO 13849-  
1:2006/DAM 1:2013)**

*Sécurité des machines — Parties des systèmes de commande relatives à la sécurité — Partie 1 : Principes généraux de conception – Amendement 1 (ISO 13849-1:2006/DAM 1:2013)*

*Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design – Amendment 1 (ISO 13849-1:2006/DAM 1:2013)*

ICS:

Deskriptoren:

Dokument-Typ: Europäische Norm  
Dokument-Untertyp: Änderung  
Dokumentstufe: parallele Umfrage  
Dokumentsprache: D

STD Version 2.5a

## Inhalt

	Seite
Vorwort .....	3
1 Änderung zum Vorwort .....	4
2 Änderung zur Einleitung .....	4
3 Änderung zum Anwendungsbereich .....	4
4 Änderung zu Normative Verweisungen .....	4
5 Änderung zu Begriffe .....	5
6 Änderung zu 4 Gestaltungsaspekte .....	6
7 Änderung zu 5 Sicherheitsfunktionen .....	12
8 Änderung zu 6 Die Kategorien und deren Beziehung zur $MTTF_d$ jedes Kanals, $DC_{avg}$ und CCF .....	13
9 Änderung zu 7 Berücksichtigung von Fehlern, Fehlerausschluss .....	16
10 Änderung zu 9 Instandhaltung .....	16
11 Änderung zu 11 Benutzerinformation .....	16
12 Änderung zu Anhang A .....	17
13 Änderung zu Anhang C .....	19
14 Änderung zu Anhang D .....	24
15 Änderung zu Anhang E .....	25
16 Änderung zu Anhang F .....	25
17 Änderung zu Anhang G .....	27
18 Änderung zu Anhang I .....	27
Anhang I (informativ) Beispiele .....	28
Literaturhinweise .....	40

## Vorwort

Dieses Dokument (EN ISO 13849-1:2008/prA1:2013) wurde vom Technischen Komitee ISO/TC 199 „Safety of machinery“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 114 „Sicherheit von Maschinen“ erarbeitet, dessen Sekretariat vom DIN gehalten wird.

Dieses Dokument ist derzeit zur parallelen Umfrage vorgelegt.

Dieses Dokument wurde unter einem Mandat erarbeitet, das die Europäische Kommission und die Europäische Freihandelszone dem CEN erteilt haben, und unterstützt grundlegende Anforderungen der EU-Richtlinien.

Dieses Dokument ist als Änderung zu EN ISO 13849-1:2008 vorgesehen.

### Anerkennungsnotiz

Der Text von ISO 13849-1:2006/DAM 1:2013 wurde vom CEN als EN ISO 13849-1:2008/prA1:2013 ohne irgendeine Abänderung genehmigt.

## 1 Änderung zum Vorwort

Letzter Absatz:

*Die Verweisung „ISO 13849-100“ ist zu streichen, da der Teil 100 zurückgezogen wurde.*

## 2 Änderung zur Einleitung

Absatz nach der Auflistung:

*Die Verweisung „ISO 12100-1“ ist durch „ISO 12100“ zu ersetzen.*

Fünfter Absatz:

*Die Verweisung „Maschinenrichtlinie 98/37/EG, der Maschinen-Richtlinie“ ist durch „Richtlinie 2006/42/EG über Maschinen“ zu ersetzen.*

Tabelle 1 und der Absatz vor Tabelle 1:

*Tabelle 1 und der Absatz vor der Tabelle 1 sind durch folgenden Absatz zu ersetzen:*

„Die IEC 62061 und dieser Teil der ISO 13849 legen Anforderungen für den Entwurf und die Realisierung sicherheitsbezogener Steuerungen von Maschinen fest. Durch die Anwendung einer der beiden Internationalen Normen kann in Übereinstimmung mit deren Anwendungsbereichen angenommen werden, dass die relevanten und erforderlichen Sicherheitsanforderungen erfüllt sind. ISO/TR 23849 enthält Hinweise zur Anwendung von ISO 13849-1 und IEC 62061 bei der Gestaltung von sicherheitsbezogenen Steuerungen für Maschinen.“

*Der folgende neue Tabellentitel ist nach diesem neuen Absatz zu ergänzen, um eine neue Benummerung aller Tabellen und deren Verweise zu vermeiden:*

**„Tabelle 1 — gestrichen“**

## 3 Änderung zum Anwendungsbereich

*Die ANMERKUNG 5 ist durch folgende neue ANMERKUNG 5 zu ersetzen:*

„ANMERKUNG 5 ISO 13849-1 behandelt die Betriebsart mit hoher Anforderungsrate und die Betriebsart mit kontinuierlicher Anforderungsrate.“

## 4 Änderung zu Normative Verweisungen

*Folgende Verweisungen sind zu streichen:*

„ISO 12100-1:2003, *Safety of machinery — Basic concepts, general principles for design — Part 1: Basic terminology, methodology*“

ISO 12100-2:2003, *Safety of machinery — Basic concepts, general principles for design — Part 2: Technical principles*

ISO 14121, *Safety of machinery — Principles of risk assessment“*

*Folgende Verweisung ist zu ergänzen:*

„ISO 12100:2010, *Safety of machinery — General principles for design — Risk assessment and risk reduction“*

## 5 Änderung zu Begriffe

### 3.1 Begriffe

*Die Verweisung „ISO 12100-1“ ist durch „ISO 12100“ zu ersetzen.*

#### 3.1.6

*In der ANMERKUNG ist die Verweisung „(siehe ISO 12100-1:2003, 3.34)“ durch „(siehe ISO 12100:2010, 3.36)“ zu ersetzen.*

#### 3.1.10

*Die Quelle der Definition „[ISO 12100-1:2003, 3.5]“ ist durch „[ISO 12100:2010, 3.5]“ zu ersetzen.*

#### 3.1.11

*Die Quelle der Definition „[ISO 12100-1:2003, 3.6]“ ist durch „[ISO 12100:2010, 3.6, modifiziert]“ zu ersetzen.*

#### 3.1.12

*Die Quelle der Definition „[ISO 12100-1:2003, 3.9]“ ist durch „[ISO 12100:2010, 3.10]“ zu ersetzen.*

#### 3.1.13

*Die Quelle der Definition „[ISO 12100-1:2003, 3.11]“ ist durch „[ISO 12100:2010, 3.12]“ zu ersetzen.*

#### 3.1.14

*In der ANMERKUNG ist die Verweisung „ISO 12100-1:2003, Begriff 3.12“ durch „ISO 12100:2010, Begriff 3.13“ zu ersetzen.*

#### 3.1.15

*Die Quelle der Definition „[ISO 12100-1:2003, 3.13]“ ist durch „[ISO 12100:2010, 3.17]“ zu ersetzen.*

#### 3.1.16

*Die Quelle der Definition „[ISO 12100-1:2003, 3.14]“ ist durch „[ISO 12100:2010, 3.15]“ zu ersetzen.*

#### 3.1.17

*Die Quelle der Definition „[ISO 12100-1:2003, 3.16]“ ist durch „[ISO 12100:2010, 3.16]“ zu ersetzen.*

#### 3.1.18

*Die Quelle der Definition „[ISO 12100-1:2003, 3.22]“ ist durch „[ISO 12100:2010, 3.23]“ zu ersetzen.*

#### 3.1.19

*Die Quelle der Definition „[ISO 12100-1:2003, 3.23]“ ist durch „[ISO 12100:2010, 3.24]“ zu ersetzen.*

#### 3.1.20

*Die Quelle der Definition „[ISO 12100-1:2003, 3.28]“ ist durch „[ISO 12100:2010, 3.30]“ zu ersetzen.*

#### 3.1.27

*In der ANMERKUNG ist die Verweisung „ISO 12100-1:2003, Begriff 3.18“ durch „ISO 12100:2010, Begriff 3.19“ zu ersetzen.*

Folgender neuer **Begriff 3.1.38** ist zu ergänzen:

„3.1.38

**Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderungsrate**

Betriebsart, bei der die Häufigkeit der Anforderungen an SRP/CS mehr als einmal pro Jahr beträgt“

### 3.2 Formelzeichen und Abkürzungen

In Tabelle 2 ist Folgendes zu ergänzen:

PFH <sub>D</sub>	durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde	Tabelle 3
------------------	--	-----------

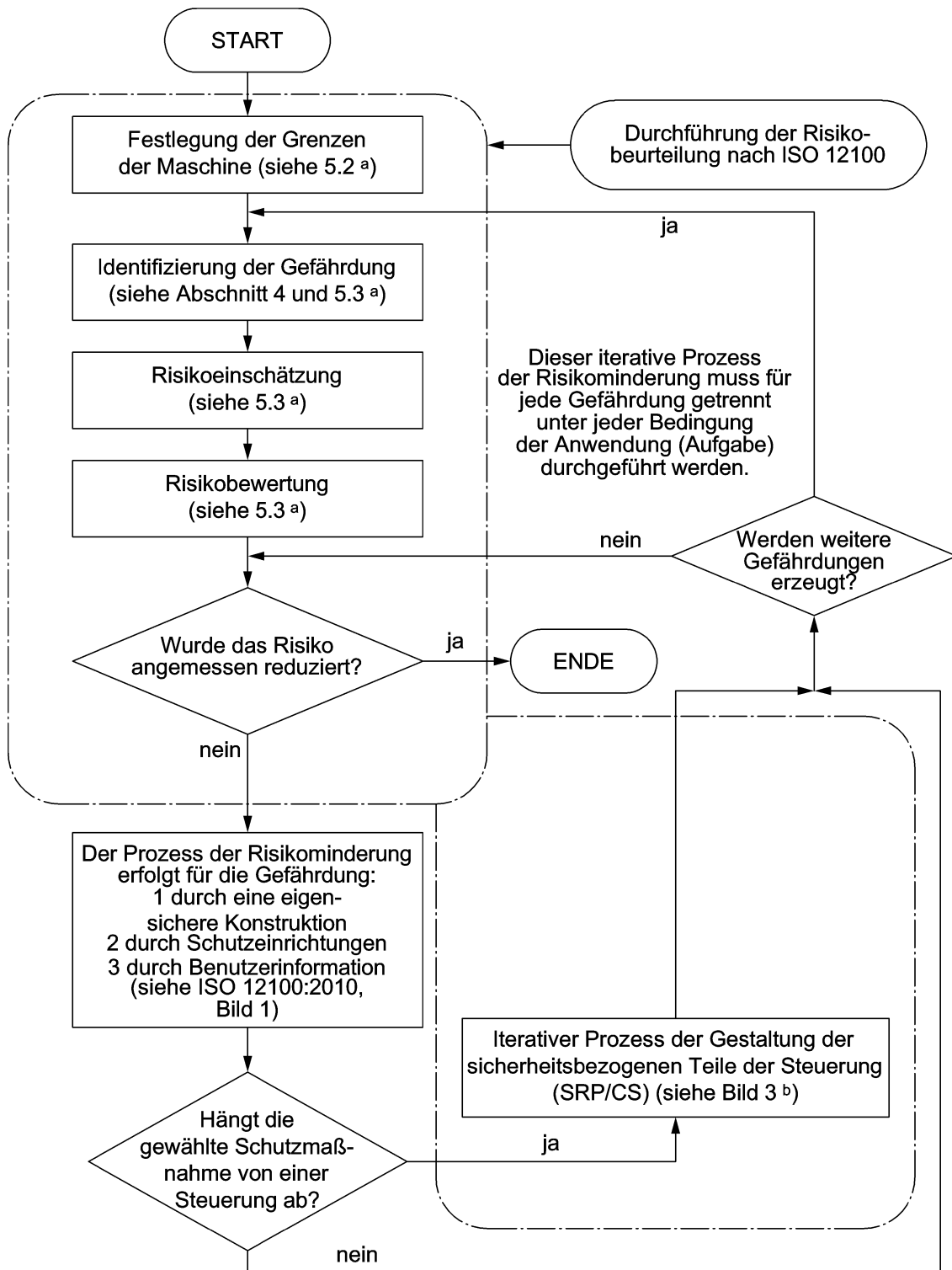
## 6 Änderung zu 4 Gestaltungsaspekte

### 4.1 Sicherheitsziele in der Gestaltung

Erster Absatz:

Die Verweisung „und ISO 14121“ im ersten Satz ist zu streichen.

Bild 1 ist durch folgendes Bild zu ersetzen (dieses neue Bild enthält keine fachlichen Änderungen sondern aktualisierte Verweisungen).



a Bezieht sich auf ISO 12100:2010.

b Bezieht sich auf diesen Teil der ISO 13849.

#### 4.2.1 Allgemeines

Erster Absatz:

*Um die Verweisungen zu aktualisieren, ist der erste Satz wie folgt zu ersetzen:*

„Die Strategie zur Risikominderung an einer Maschine wird in der ISO 12100:2010, Abschnitt 6, genannt.“

Zweiter Absatz:

*Um die Verweisungen zu aktualisieren, sind die drei Spiegelstriche wie folgt zu ersetzen:*

”

- Beseitigung von Gefährdungen oder Risikominderung durch den Entwurf (siehe ISO 12100:2010, 6.2);
- Risikominderung durch Schutzeinrichtungen und mögliche ergänzende Schutzmaßnahmen (siehe ISO 12100:2010, 6.3);
- Risikominderung durch Bereitstellung einer Benutzerinformation über das Restrisiko (siehe ISO 12100:2010, 6.4).

“

#### 4.2.2 Beitrag der Risikominderung durch das Steuerungssystem

Erster Absatz, vierter Satz:

*Das Wort „Schutzeinrichtung“ ist durch „verriegelte trennende Schutzeinrichtung“ zu ersetzen.*

Dritter Absatz, zweiter Satz:

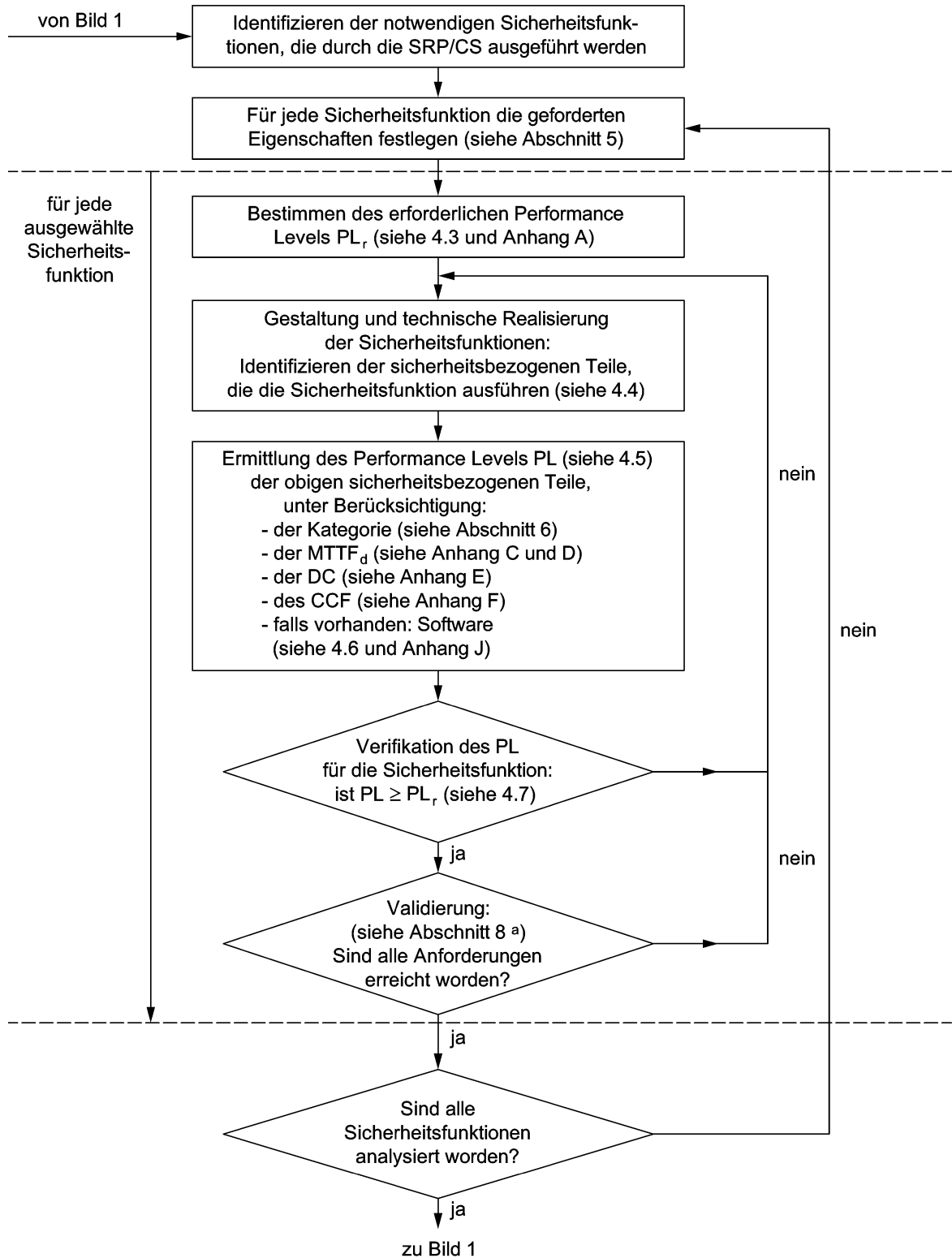
*Der Satz ist in folgenden zu ändern:* „Fünf Performance Level sind festgelegt, vom niedrigsten PL a bis zum höchsten PL e, mit definierten Bereichen der Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (siehe Tabelle 3).“

Vierter Absatz, nach Tabelle 3:

„(siehe ISO 14121)“ *ist durch* „(siehe ISO 12100)“ *zu ersetzen.*

Bild 3:

Die Verweisungen sind zu ändern, indem am Ende von Bild 3 „zu Bild 1 (ISO 12100)“ durch „zu Bild 1“ ersetzt wird.



<sup>a</sup> ISO 13849-2 enthält weitere Hilfe zur Validierung.

#### 4.5.1 Performance Level PL

*ANMERKUNG 2 ist durch folgende neue ANMERKUNG 2 zu ersetzen:*

„ANMERKUNG 2 Für den Entwurf komplexer Steuerungssysteme, wie PES zur Durchführung von Sicherheitsfunktionen, kann die Anwendung anderer einschlägiger Normen angemessen sein (z. B. IEC 61508 oder IEC 61496).“

*Folgender neuer Absatz ist nach Tabelle 4 zu ergänzen:*

„Obwohl es einen Zusammenhang zwischen den PLs der vorliegenden Norm und den SILs nach IEC 61508 und IEC 62061 gibt, ist es erlaubt, nur eine der beiden Normen anzuwenden; es ist jedoch nicht zulässig, die Anforderungen von ISO 13849-1 mit denen von IEC 61508/IEC 62061 (siehe auch ISO/TR 23849) bei der Auslegung von sicherheitsbezogenen Teilen von Steuerungen (SRP/CS) zu vermischen.“

#### 4.5.2 Mittlere Zeit bis zum gefahrbringenden Ausfall jedes Kanals (MTTF<sub>d</sub>)

Zweiter Absatz:

*Folgende neue ANMERKUNG ist zu ergänzen:*

„ANMERKUNG Für eine Kombination von mehr als drei Teilsystemen (SRP/CS) in Kategorie 4, wird der Höchstwert von MTTF<sub>d</sub> auf 2 500 Jahre für jedes Teilsystem (SRP/CS) erhöht. Dies ist darauf zurückzuführen, dass die anderen quantifizierbaren Aspekte, Struktur und DC, sich in Kategorie 4 auf ihrem Höchststand befinden, was in Kategorie 4 eine Kombination von mehr als drei Teilsystemen (SRP/CS) erlaubt und PL e nach 6.3 erreicht.“

#### 4.5.3 Diagnosedeckungsgrad (DC)

*Folgende neue ANMERKUNG ist nach Tabelle 6 zu ergänzen:*

„ANMERKUNG Beispiele der Abschätzung des Diagnosedeckungsgrades (DC) sind in Anhang E enthalten.“

#### 4.5.4 Vereinfachtes Verfahren zur Abschätzung eines PL

*Die Überschrift von 4.5.4 ist durch folgende zu ersetzen:*

„4.5.4 Vereinfachtes Verfahren zur Abschätzung der quantifizierbaren Aspekte des PL (PFH<sub>D</sub>)“

Fünfter Absatz:

*Die Verweisung „(siehe auch ISO 12100-1:2003, Anhang A)“ ist durch „(siehe ISO 12100:2010, Anhang A)“ zu ersetzen.*

*Der dritte Spiegelstrich (Seite 26) ist durch folgenden zu ersetzen:*

— für Kategorie 2, Anforderungsrate  $\leq 1/100$  der Testrate; oder die Prüfung erfolgt unmittelbar nach Anforderung der Sicherheitsfunktion und die Gesamtzeit zum Erkennen des Ausfalls und zur Überführung der Maschine in einen nicht gefahrbringenden Zustand (in der Regel wird die Maschine angehalten) ist kürzer als die Zeit zum Erreichen der Gefährdung (siehe auch ISO 13855);

*Der vierte Spiegelstrich (Seite 26) ist durch folgenden zu ersetzen:*

— für Kategorie 2, ist  $MTTF_{d,TE}$  größer als die Hälfte der  $MTTF_{d,L}$ .

Siebter Absatz auf Seite 26:

*Die Verweisung „(siehe auch ISO 12100-2:2003, Abschnitt 3 und IEC 60204-1:2000)“ ist durch „(siehe auch ISO 12100:2010, Abschnitt 3 und IEC 60204-1:2005)“ zu ersetzen.*

#### **4.6.2 Sicherheitsbezogene Embedded-Software (SRESW)**

*Die Auflistung auf Seite 29 (zweite Aufzählung in 4.6.2) ist zu ändern, indem im sechsten Spiegelstrich „Abgrenzung in nicht sicherheitsbezogene Software“ durch „Abgrenzung von nicht sicherheitsbezogener Software“ ersetzt wird.*

*Am Ende von 4.6.2, nach ANMERKUNG 2, ist folgender neuer Absatz zu ergänzen:*

„Bauteile, für die die SRESW-Anforderungen nicht erfüllt sind, z. B. nicht sicherheitsbezogene PLCs, dürfen unter folgenden alternativen Bedingungen verwendet werden:

- das SRP/CS ist auf PL a oder PL b begrenzt und verwendet Kategorie B, 2 oder 3;
- das SRP/CS ist auf PL c oder PL d begrenzt und verwendet zwei Bauteile für zwei Kanäle in Kategorie 2 oder 3 und die beiden Bauteile verwenden unterschiedliche Embedded-Software oder verschiedene Technologien und eine entsprechende sicherheitsbezogene Anwendungssoftware (siehe 4.6.3), damit die Fehlererkennung den erforderlichen DC erfüllt (z. B. Kreuzvergleich);
- das SRP/CS ist auf PL c oder PL d begrenzt und verwendet zwei Bauteile für zwei Kanäle in Kategorie 2 oder 3 und verwendet zwei verschiedene Anwendungssoftwarekanäle, damit die Fehlererkennung den erforderlichen DC erfüllt (z. B. Kreuzvergleich).“

#### **4.8 Ergonomische Aspekte der Gestaltung**

Erster Absatz:

*„ISO 12100-2“ ist durch „ISO 12100“ zu ersetzen und „IEC 60204-1:2000, Abschnitt 10“ ist durch „IEC 60204-1:2005, Abschnitt 10“ zu ersetzen.*

Dritter Absatz:

*Die Verweisung „ISO 12100-2:2003, 4.8“ ist durch „ISO 12100:2010, 6.2.8“ zu ersetzen.*

## 7 Änderung zu 5 Sicherheitsfunktionen

### 5.1 Spezifikation der Sicherheitsfunktionen

Die Verweisungen in Tabelle 8 sind zu aktualisieren, indem die Tabelle durch folgende ersetzt wird:

**Tabelle 8 — Einige Internationale Normen, die auf typische Sicherheitsfunktionen und einige ihrer Eigenschaften anwendbar sind**

Sicherheitsfunktion/ Eigenschaft	Anforderung(en)		Für weitere Informationen siehe :
	Dieser Teil der ISO 13849	ISO 12100:2010	
Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung <sup>a</sup>	5.2.1	3.28.8, 6.2.11.3	IEC 60204-1:2005, 9.2.2, 9.2.5.3, 9.2.5.5  ISO 14119  ISO 13855
Manuelle Rückstellfunktion	5.2.2	–	IEC 60204-1:2005, 9.2.5.3, 9.2.5.4
Start-/Wiederanlauf- funktion	5.2.3	6.2.11.3, 6.2.11.4	IEC 60204-1:2005, 9.2.1, 9.2.5.1, 9.2.5.2, 9.2.6
Lokale Steuerungs- funktion	5.2.4	6.2.11.8, 6.2.11.10	IEC 60204-1:2005, 10.1.5
Mutingfunktion	5.2.5	–	IEC/TS 62046:2008, 5.5
Einrichtung mit selbsttätiger Rückstellung (Tippschalter)		6.2.11.8 b)	IEC 60204-1:2005, 9.2.6.1
Zustimmfunktion		–	IEC 60204-1:2005, 9.2.6.3, 10.9
Verhindern des unerwarteten Anlaufs	–	6.2.11.4	ISO 14118 IEC 60204-1:2005, 5.4
Befreiung und Rettung eingeschlossener Personen	–	6.3.5.3	ISO 13850
Isolations- und Energieableitungs- funktion	–	6.3.5.4	ISO 14118 IEC 60204-1:2005, 5.3, 6.3.1
Steuerungsfunktion und Betriebsartenwahl	–	6.2.11.8, 6.2.11.10	IEC 60204-1: 2005, 9.2.3, 9.2.4
Beeinflussung zwischen verschie- denen sicherheits- bezogenen Teilen der Steuerungen	–	6.2.11.1 (letzter Satz)	IEC 60204-1:2005, 9.3.4
Überwachung der Parametrisierung der sicherheitsbezogenen Eingangswerte	4.6.4	–	–
Funktion zum Stillsetzen im Notfall <sup>b</sup>	–	6.3.5.2	ISO 13850 IEC 60204-1:2005, 9.2.5.4

<sup>a</sup> Einschließlich verriegelter trennender Schutzeinrichtungen und Grenzwertüberwachung (z. B. Höchstdrehzahl, Übertemperatur, Überdruck).

<sup>b</sup> Ergänzende Schutzmaßnahme, siehe ISO 12100:2010.

Die Verweisungen in Tabelle 9 sind zu aktualisieren, indem die Tabelle durch folgende ersetzt wird:

**Tabelle 9 — Einige Internationale Normen, die Anforderungen für bestimmte Sicherheitsfunktionen und sicherheitsbezogene Parameter geben**

Sicherheitsfunktion/ sicherheitsbezogener Parameter	Anforderung		Für weitere Informationen siehe:
	Dieser Teil der ISO 13849	ISO 12100:2010	
Ansprechzeit	5.2.6	–	ISO 13855:2010, 3.2, A.3, A.4
Sicherheitsbezogene Parameter, z. B. Geschwin- digkeit, Temperatur, Druck	5.2.7	6.2.11.8 e)	IEC 60204-1:2005, 7.1, 9.3.2, 9.3.4
Schwankungen, Verlust und Wiederkehr der Spannungs- versorgung	5.2.8	6.2.11.8 e)	IEC 60204-1:2005, 4.3, 7.1, 7.5
Anzeigen und Alarme	–	6.2.8	ISO 7731 ISO 11428 ISO 11429 IEC 61310-1 IEC 60204-1:2005, 10.3, 10.4 IEC 61131 IEC 62061

Nach dem Aufzählungspunkt e) ist ein neuer Aufzählungspunkt f) mit neuer ANMERKUNG zu ergänzen:

„f) das Verhalten der Maschine bei Energieverlust (siehe auch 5.2.8);

ANMERKUNG In einigen Fällen kann es notwendig sein, das Verhalten der Maschine bei Energieverlust zu berücksichtigen, wenn es beispielsweise notwendig ist, eine vertikale Achse einzuhalten. Das kann zwei getrennte Sicherheitsfunktionen erfordern: mit Energie verfügbar und ohne Energie verfügbar.“

Die Auflistungspunkte f) bis h) sind mit g) bis i) neu zu benummern.

### 5.2.3 Start-/Wiederaufnahmefunktion

Die Verweisung „ISO 12100-2:2003, 5.3.2.5“ im zweiten Absatz ist durch „ISO 12100:2010, 6.3.3.2.5“ zu ersetzen.

## 8 Änderung zu 6 Die Kategorien und deren Beziehung zur $MTTF_d$ jedes Kanals, $DC_{avg}$ und CCF

### 6.2.3 Kategorie B

Erster Absatz:

Der grammatikalische Fehler im ersten Satz ist zu berichtigen, indem der Satz durch folgenden ersetzt wird:

„Die SRP/CS müssen mindestens in Übereinstimmung mit den zutreffenden Normen gestaltet, gebaut, ausgewählt, zusammengestellt und kombiniert sein und die grundlegenden Sicherheitsprinzipien für die bestimmte Anwendung nutzen, um Folgendem standzuhalten:“

### 6.2.5 Kategorie 2

Vierter Absatz:

*Der letzte Satz ist wie folgt zu ersetzen:*

„Wenn das Einleiten eines sicheren Zustands nicht möglich ist (z. B. durch Verschweißen des Kontakts eines Schaltglieds), kann es ausreichen, wenn der Ausgang der Testeinrichtung, OTE, nur eine Warnung bis  $PL_r = c$  bereitstellt.“

Sechster Absatz:

*Der erste Satz ist durch folgenden zu ersetzen:*

„Der Diagnosedeckungsgrad ( $DC_{avg}$ ) des gesamten SRP/CS einschließlich der Fehlererkennung muss mindestens niedrig sein“

*Eine neue ANMERKUNG 4 ist nach ANMERKUNG 3 und vor Bild 10 zu ergänzen:*

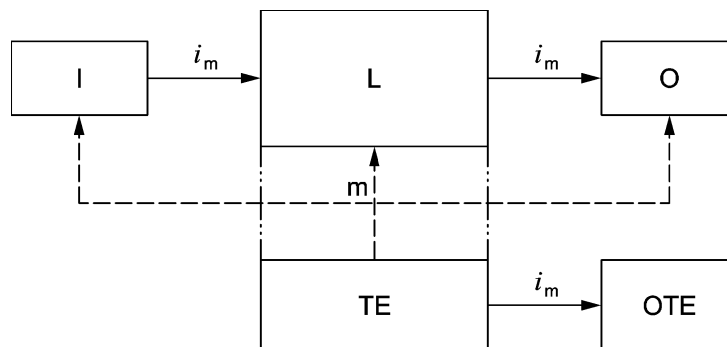
„ANMERKUNG 4 Zur Anwendung der vereinfachten Methode basierend auf den vorgesehenen Architekturen siehe Annahmen in 4.5.4.“

ANMERKUNG 2:

*Im ersten Satz ist „lässt zu, dass“ durch „ist dadurch gekennzeichnet, dass“ zu ersetzen.*

Bild 10:

*Bild 10 ist zu ändern, indem der auf den TE-Block gerichtete Pfeil gelöscht wird.*



### 6.2.6 Kategorie 3

Dritter Absatz:

*Der erste Satz ist durch folgenden zu ersetzen:*

„Der Diagnosedeckungsgrad ( $DC_{avg}$ ) des gesamten SRP/CS einschließlich der Fehlererkennung muss mindestens niedrig sein.“

ANMERKUNG 3:

*Im ersten Satz ist „lässt zu, dass“ durch „ist dadurch gekennzeichnet, dass“ zu ersetzen.*

### 6.2.7 Kategorie 4

ANMERKUNG 1:

*Im ersten Satz ist „lässt zu, dass“ durch „ist dadurch gekennzeichnet, dass“ zu ersetzen.*

Bild 12:

*Die Zeichnung, in der die vorgesehene Architektur für Kategorie 4 dargestellt ist, ist durch folgende zu ersetzen. Die folgende Zeichnung ersetzt auch Bild 12 von ISO 13849-1/Cor.1:2009. Es berichtigt die Pfeile, die mit „m“ beschriftet sind zwischen L1 und O1 und zwischen L2 und O2, und die Pfeile, die mit „c“ beschriftet sind zwischen L1 und L2, indem sie von gestrichelten Linien in durchgezogene Linien geändert werden, was einen höheren Diagnosedeckungsgrad darstellt.*

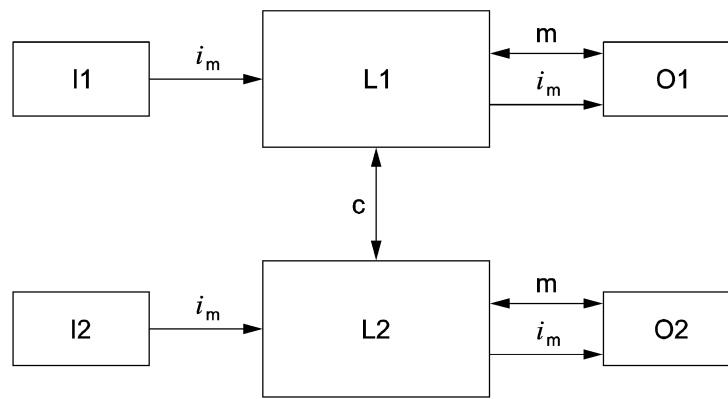


Tabelle 10 (Kategorie 2, Zusammenfassung der Anforderungen):

*Der Text ist wie folgt zu ändern:*

„Die Anforderungen von B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Die Sicherheitsfunktion muss in geeigneten Zeitabständen oder nach Anforderungen der Funktion durch die Maschinensteuerung getestet werden (siehe 4.5.4).“

### 6.3 Kombination von SRP/CS, um einen Gesamt-PL zu erreichen

Erster Absatz:

*Der vierte Satz ist durch folgenden zu ersetzen, in dem die Verweisung auf Tabelle 11 gestrichen wird:*

„Für die Gesamtkombination dieser SRP/CS kann ein Gesamt-PL nach den Verfahren dieses Abschnitts ermittelt werden.“

Dritter Absatz, vor Bild 13:

*Die Ausdrucksweise des dritten Absatzes ist zu verbessern, indem der Absatz wie folgt ersetzt wird:*

„Es werden  $N$  separate SRP/CS <sub>$i$</sub>  in einer Reihenschaltung angenommen, die zusammen eine Sicherheitsfunktion ausführen. Für jedes SRP/CS <sub>$i$</sub>  wurde bereits ein PL <sub>$i$</sub>  festgelegt. Diese Situation wird in Bild 13 dargestellt (siehe auch Bild 4 und Bild H.2).“

Folgender Absatz ist zu ergänzen, einschließlich der Auflistung und einer neuen ANMERKUNG:

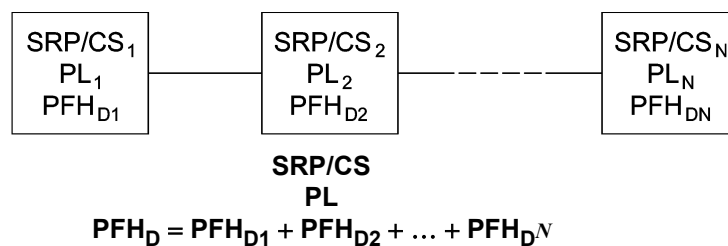
„Wenn die  $PFH_D$ -Werte aller  $SRP/CS_i$  bekannt sind, dann ist der  $PFH_D$  der kombinierten  $SRP/CS$  die Summe aller  $PFH_D$ -Werte der  $N$  einzelnen  $SRP/CS_i$ . Der PL der kombinierten  $SRP/CS$  wird beschränkt durch:

- den niedrigsten PL eines einzelnen  $SRP/CS_i$ , das an der Durchführung der Sicherheitsfunktion beteiligt ist, da der PL auch durch nicht quantifizierbare Aspekte bestimmt wird; und
- den PL, der dem  $PFH_D$  des kombinierten  $SRP/CS$  nach Tabelle 3 entspricht.

ANMERKUNG Ein Beispiel dieses Verfahrens ist in Anhang H und ISO/TR 23849, 8.2.6, enthalten.“

Bild 13:

Bild 13 ist durch folgendes Bild zu ersetzen:



Vor der Auflistung auf Seite 49:

Der erste Satz ist wie folgt zu ersetzen:

„Wenn die  $PFH_D$ -Werte aller einzelnen  $SRP/CS_i$  nicht bekannt sind, dann kann der PL des gesamten kombinierten  $SRP/CS$ , das die Sicherheitsfunktion ausführt, als Worst-case-Alternative zu dem vorstehenden Verfahren mithilfe von Tabelle 11 wie folgt berechnet werden.“

## 9 Änderung zu 7 Berücksichtigung von Fehlern, Fehlerausschluss

### 7.2 Fehlerbetrachtung

Erster Absatz:

Im zweiten Satz ist das Wort „abschließend“ durch „vollständig“ zu ersetzen. Der neue zweite Satz lautet dementsprechend wie folgt:

„Die Fehlerlisten sind nicht vollständig, und wenn notwendig, müssen weitere Fehler berücksichtigt und aufgezählt werden.“

## 10 Änderung zu 9 Instandhaltung

Zweiter Absatz:

Die Verweisung „ISO 12100-2:2003, 4.7“ im zweiten Absatz ist durch „ISO 12100:2010, 6.2.7“ zu ersetzen und „ISO 12100-2:2003, 6.5.1 e)“ ist durch „ISO 12100:2010, 6.4.5.1 e)“ zu ersetzen.

## 11 Änderung zu 11 Benutzerinformation

Erster Absatz:

Die Verweisung „ISO 12100-2:2003, 6.5.2“ im ersten Absatz ist durch „ISO 12100:2010, 6.4.5.2“ zu ersetzen.

## 12 Änderung zu Anhang A

### A.1 Auswahl des $PL_r$

Eine neue ANMERKUNG ist nach dem ersten Absatz zu ergänzen:

„ANMERKUNG Diese Vorgehensweise zur Abschätzung des  $PL_r$  ist nicht verbindlich. Sie stellt eine allgemeine Herangehensweise dar, bei der eine Eintrittswahrscheinlichkeit eines Gefährdungsereignisses im ungünstigsten Fall angenommen wird. Andere geeignete Verfahren zur Risikoabschätzung für die Abschätzung eines  $PL_r$  können ebenfalls angewendet werden. In Typ-C-Normen kann der sich daraus ergebende  $PL_r$  somit aufgrund maschinenspezifischer Bedingungen und Erfahrungen von dem der allgemeinen Herangehensweise abweichen.“

### A.2.3 Möglichkeit zur Vermeidung der Gefährdung P1 und P2

Letzter Absatz:

Der Absatz ist unter das Bild A.1 zu verschieben und die Verweisung im letzten Satz ist zu aktualisieren, indem der Satz wie folgt ersetzt wird:

„Das Verfahren der Risikobeurteilung basiert auf ISO 12100.“

Folgendes ist zu ersetzen:

### „A.2.3 Möglichkeit zur Vermeidung der Gefährdung P1 und P2

Es ist wichtig zu wissen, ob eine Gefährdungssituation erkannt oder vermieden werden kann, bevor sie zu einem Unfall führt. Eine wichtige Überlegung ist z. B., ob die Gefährdung direkt durch ihre physikalischen Eigenschaften identifiziert werden kann, oder nur durch technische Mittel erkannt werden kann, z. B. durch Anzeigen. Andere wichtige Aspekte, die die Auswahl des Parameters P beeinflussen, sind z. B.:

- Betrieb mit oder ohne Beaufsichtigung;
- Betrieb durch Fachleute oder Laien;
- Geschwindigkeit, mit der die Gefährdung auftritt (z. B. schnell oder langsam);
- Möglichkeit zur Vermeidung der Gefährdung, (z. B. durch Flucht);
- praktische Erfahrungen mit der Sicherheit in Bezug zum Prozess.

Wenn eine Gefährdungssituation auftritt, sollte P1 nur dann gewählt werden, wenn eine realistische Chance besteht, den Unfall zu vermeiden oder dessen Auswirkung maßgeblich zu reduzieren; P2 sollte gewählt werden, wenn fast keine Chance besteht, die Gefährdung zu vermeiden.“

ist zu ersetzen durch:

### „A.2.3 Eintrittswahrscheinlichkeit und Möglichkeit zur Vermeidung der Gefährdungsereignisse P1 und P2

Die Wahrscheinlichkeit, mit der die Gefährdung vermieden wird und die Wahrscheinlichkeit des Eintretens eines Gefährdungsereignisses sind beide im Parameter P miteinander kombiniert. Wenn eine Gefährdungssituation eintritt, sollte P1 nur dann ausgewählt werden, wenn eine realistische Chance besteht, dass eine Gefährdung vermieden wird oder dass deren Auswirkung deutlich verringert wird; ansonsten sollte P2 ausgewählt werden.

Wenn die Eintrittswahrscheinlichkeit eines Gefährdungsereignisses vernünftigerweise abgeschätzt werden kann, darf der  $PL_r$  um ein Level verringert werden.

### A.2.3.1 Möglichkeit zur Vermeidung der Gefährdung

Es ist wichtig zu wissen, ob eine Gefährdungssituation erkannt und vermieden werden kann, bevor sie zu einem Unfall führt. Eine wichtige Überlegung ist z. B., ob die Gefährdung direkt durch ihre physikalischen Eigenschaften identifiziert werden kann, oder nur durch technische Mittel erkannt werden kann, z. B. durch Anzeigen. Andere wichtige Aspekte, die die Auswahl des Parameters P beeinflussen, sind z. B.:

- Betrieb mit oder ohne Beaufsichtigung;
- Betrieb durch Fachleute oder Laien;
- Geschwindigkeit, mit der die Gefährdung auftritt (z. B. schnell oder langsam);
- Möglichkeit zur Vermeidung der Gefährdung, (z. B. durch Flucht);
- praktische Erfahrungen mit der Sicherheit in Bezug zum Prozess.

### A.2.3.2 Eintrittswahrscheinlichkeit eines Gefährdungsereignisses

Die Wahrscheinlichkeit des Eintritts eines Gefährdungsereignisses hängt entweder vom menschlichen Verhalten oder vom technischen Versagen ab. In den meisten Fällen sind die entsprechenden Wahrscheinlichkeiten nicht bekannt oder schwer zu bestimmen. Die Abschätzung der Eintrittswahrscheinlichkeit eines Gefährdungsereignisses sollte auf Faktoren beruhen, zu denen folgende zählen:

- Zuverlässigkeitsdaten;
- Unfallgeschichte an vergleichbaren Maschinen.

Wenn vergleichbare Maschinen

- dieselben Risiken umfassen, die die maßgebliche Sicherheitsfunktion verringern soll,
- dieselbe Betätigung durch die Bedienungsperson erfordern,

sind die gleichen Techniken anzuwenden, die die Gefährdung verursachen.“

*Ein neuer Abschnitt A.3 ist zu ergänzen:*

## „A.3 Gefährdungen durch Überlappen

Bei Anwendung von ISO 13849-1 werden alle Gefährdungen als spezifische Gefährdungen oder Gefährdungssituationen betrachtet. Zur Quantifizierung des Risikos kann deshalb jede Gefährdung getrennt bewertet werden.

BEISPIEL 1 Schweißroboter, die verschiedene spezifische Gefährdungssituationen erzeugen können, wie z. B. Quetschen durch Bewegen und Verbrennen durch den Schweißvorgang.

Die an der spezifischen Gefährdungssituation beteiligten Stellteile können zusammengefasst werden oder getrennt behandelt werden, je nach deren Auswirkung (z. B. kinematische Kette).

BEISPIEL 2 In einer Roboterzelle, in der einzelne Roboter arbeiten, wird jeder Roboter einzeln betrachtet.

BEISPIEL 3 Infolge der Risikobeurteilung kann es ausreichend sein, am runden Tisch jede Klemmvorrichtung einzeln zu betrachten.“

## 13 Änderung zu Anhang C

### C.2 Verfahren guter ingenieurmäßiger Praxis

*Punkt b) ist wie folgt zu ersetzen:*

„b) Der Hersteller des Bauteils beschreibt die geeignete Anwendung und Betriebsbedingungen für den SRP/CS-Hersteller.“

### C.3 Hydraulische Bauteile

*Der erste Satz von Punkt b) ist wie folgt zu ersetzen:*

„b) Der Hersteller des hydraulischen Bauteils legt die geeignete Anwendung und Betriebsbedingungen für den SRP/CS-Hersteller fest.“

*Der zweite Absatz von C.3 (nach Punkt b)) ist wie folgt zu ersetzen:*

„Wenn die in C.4 dargestellten Kriterien erfüllt sind, kann der  $MTTF_d$ -Wert für ein einzelnes hydraulisches Bauteil, z. B. Ventil, mit 150 Jahren abgeschätzt werden. Wenn die mittlere Anzahl der jährlichen Betätigungen ( $n_{op}$ ) unter 1 000 000 beträgt, kann der  $MTTF_d$ -Wert höher als in Tabelle C.1 angegeben abgeschätzt werden.

Wenn aber weder a) noch b) erreicht werden kann, muss der  $MTTF_d$ -Wert für das einzelne hydraulische Bauteil vom Hersteller angegeben werden. Anstatt einen festen Wert für  $MTTF_d$  zu verwenden, wie vorstehend beschrieben, ist es zulässig, den  $B_{10d}$ -Wert für  $MTTF_d$  von pneumatischen, mechanischen und elektromechanischen Bauteilen und auch für hydraulische Bauteile zu verwenden, wenn der Hersteller die Daten liefern kann.“

Tabelle C.1:

*Tabelle C.1 ist durch folgende Tabelle zu ersetzen:*

Tabelle C.1 — Internationale Normen, die sich mit  $MTTF_d$ - oder  $B_{10d}$ -Werten für Bauteile befassen

	Grundlegende und bewährte Sicherheitsprinzipien nach ISO 13849-2:2012	Relevante Normen	Typische Werte: $MTTF_d$ (Jahre) $B_{10d}$ (Zyklen)
<b>Mechanische Bauteile</b>	Tabellen A.1 und A.2	–	$MTTF_d = 150$
<b>Hydraulische Bauteile mit <math>n_{op} \geq 1\,000\,000</math></b>	Tabellen C.1 und C.2	ISO 4413	$MTTF_d = 150$
<b>Hydraulische Bauteile mit <math>1\,000\,000 &gt; n_{op} \geq 500\,000</math></b>	Tabellen C.1 und C.2	ISO 4413	$MTTF_d = 300$
<b>Hydraulische Bauteile mit <math>500\,000 &gt; n_{op} \geq 250\,000</math></b>	Tabellen C.1 und C.2	ISO 4413	$MTTF_d = 600$
<b>Hydraulische Bauteile mit <math>250\,000 \geq n_{op}</math></b>	Tabellen C.1 und C.2	ISO 4413	$MTTF_d = 1\,200$
<b>Pneumatische Bauteile</b>	Tabellen B.1 und B.2	ISO 4414	$B_{10d} = 20\,000\,000$
<b>Relais und Hilfsschütze mit geringer Last</b>	Tabellen D.1 und D.2	EN 50205 IEC 61810 IEC 60947	$B_{10d} = 20\,000\,000$
<b>Relais und Hilfsschütze mit nominaler Last</b>	Tabellen D.1 und D.2	EN 50205 IEC 61810 IEC 60947	$B_{10d} = 400\,000$
<b>Näherungsschalter mit geringer Last</b>	Tabellen D.1 und D.2	IEC 60947 ISO 14119	$B_{10d} = 20\,000\,000$
<b>Näherungsschalter mit nominaler Last</b>	Tabellen D.1 und D.2	IEC 60947 ISO 14119	$B_{10d} = 400\,000$
<b>Schütze mit geringer Last</b>	Tabellen D.1 und D.2	IEC 60947	$B_{10d} = 20\,000\,000$
<b>Schütze mit nominaler Last</b>	Tabellen D.1 und D.2	IEC 60947	$B_{10d} = 1\,300\,000$
<b>Positionsschalter<sup>a</sup></b>	Tabellen D.1 und D.2	IEC 60947 ISO 14119	$B_{10d} = 20\,000\,000$
<b>Positionsschalter (mit separatem Betätiger, Zuhaltung)<sup>a</sup></b>	Tabellen D.1 und D.2	IEC 60947 ISO 14119	$B_{10d} = 2\,000\,000$
<b>Not-Aus-Einrichtungen<sup>a</sup></b>	Tabellen D.1 und D.2	IEC 60947 ISO 13850	$B_{10d} = 100\,000$
<b>Druck-Taster (z. B. Zustimmungsschalter)<sup>a</sup></b>	Tabellen D.1 und D.2	IEC 60947	$B_{10d} = 100\,000$

Für die Definition und Verwendung von  $B_{10d}$ , siehe C.4.

ANMERKUNG 1  $B_{10d}$  wird abgeschätzt als zweimal  $B_{10}$  (50 % gefährlicher Ausfall), wenn keine anderen Angaben vorliegen (z. B. Produktnorm).

ANMERKUNG 2 „Nominale Last“ oder „geringe Last“ sollten die Sicherheitsprinzipien berücksichtigen, die in ISO 13849-2 beschrieben sind, wie Überdimensionierung des Strom-Nennwerts. „Geringe Last“ bedeutet z. B. 20 %.

ANMERKUNG 3 Not-Aus-Einrichtungen nach IEC 60947-5-5 und ISO 13850 sowie Zustimmungsschalter nach IEC 60947-5-8 können als Teilsystem der Kategorie 1 oder Kategorie 3/4 abgeschätzt werden, je nach Anzahl der elektrischen Fernmeldekontakte und der Fehlererkennung im Teilsystem SRP/CS. Jedes Kontaktelement (einschließlich der mechanischen Betätigung) kann als ein Kanal mit entsprechendem  $B_{10d}$ -Wert betrachtet werden. Für Zustimmungsschalter nach IEC 60947-5-8 umfasst dies die Öffnungsfunktion durch Durchdrücken oder Loslassen. In einigen Fällen kann es möglich sein, dass der Maschinenhersteller einen Fehlerausschluss nach ISO 13849-2, Tabelle D.8, unter Berücksichtigung der jeweiligen Anwendungs- und Umgebungsbedingungen des Gerätes anwenden kann.

<sup>a</sup> Falls Fehlerausschluss für Zwangsöffnung möglich ist.

#### C.4.1 Allgemeines

*Der erste Satz von Punkt c) ist wie folgt zu ersetzen:*

„c) Der Hersteller des Bauteils legt die geeignete Anwendung und Betriebsbedingungen für den SRP/CS-Hersteller fest.“

#### C.4.2 Berechnung der $MTTF_d$ für Bauteile aus $B_{10d}$

Gleichung (C.2):

*Die Erklärung für „ $t_{\text{Zyklus}}$ “ ist wie folgt zu ersetzen:*

„ $t_{\text{Zyklus}}$  die mittlere Betriebszeit zwischen dem Beginn zweier aufeinander folgender Zyklen des Bauteils (z. B. Schalten eines Ventils) in Sekunden je Zyklus.“

*Folgende neue ANMERKUNG ist nach Gleichung (C.7) zu ergänzen:*

„ANMERKUNG Alle Variablen, die in den Gleichungen verwendet werden, sind physikalische Mengen, angegeben als Produkt aus numerischem Wert und Maßeinheit. Die ordnungsgemäße Anwendung, z. B. der Gleichungen (C.5), (C.6) und  $MTTF_d = 1/\lambda_d$  kann die Umwandlung von „Jahren“ in „Stunden“ erfordern, wobei für 1 Jahr = 8 760 Stunden verwendet werden.“

#### C.5.1 Allgemeines

Erster Absatz:

*Der grammatikalische Fehler im letzten Satz ist zu berichtigen, indem der Satz wie folgt ersetzt wird:*

„Wenn der Konstrukteur eines SRP/CS andere verlässliche spezifische Daten der verwendeten Bauteile hat, dann wird die Verwendung dieser speziellen Daten anstelle der anderen Daten dringend empfohlen.“

Dritter Absatz:

*Der letzte Satz ist zu streichen:*

„Für die Anwendung in Zweifelsfällen ist für die Bauteile eine ungünstigste  $MTTF_d$  in der Spalte „ungünstigster Fall“ angegeben, wobei der Sicherheitsfaktor 10 beträgt.“

#### C.5.2 Halbleiter

*C.5.2 ist durch folgenden Abschnitt zu ersetzen:*

**C.5.2 Halbleiter**

Siehe Tabellen C.2 und C.3.

**Tabelle C.2 — Transistoren (verwendet als Schalter)**

Transistor	Beispiel	MTTF für Bauteile Jahre	MTTF <sub>d</sub> für Bauteile Jahre Typisch	Bemerkungen
Bipolar	TO18, TO92, SOT23	34 247	68 493	50 % gefahrbringende Ausfälle
Bipolar, niedrige Leistung	TO5, TO39	5 708	11 416	50 % gefahrbringende Ausfälle
Bipolar, Leistung	TO3, TO220, D-Pack	1 941	3 881	50 % gefahrbringende Ausfälle
FET	Junction MOS	22 831	45 662	50 % gefahrbringende Ausfälle
MOS, Leistung	TO3, TO220, D-Pack	1 142	2 283	50 % gefahrbringende Ausfälle

**Tabelle C.3 — Dioden, Leistungshalbleiter und integrierte Schaltungen**

Diode	Beispiel	MTTF für Bauteile Jahre	MTTF <sub>d</sub> für Bauteile Jahre Typisch	Bemerkungen
Allgemeine Anwendung	–	114 155	228 311	50 % gefahrbringende Ausfälle
Entstörgerät	–	15 981	31 963	50 % gefahrbringende Ausfälle
Zenerdiode $P_{tot} < 1$ W	–	114 155	228 311	50 % gefahrbringende Ausfälle
Gleichrichterioden	–	57 078	114 155	50 % gefahrbringende Ausfälle
Gleichrichterbrücken	–	11 415	22 831	50 % gefahrbringende Ausfälle
Thyristoren	–	2 283	4 566	50 % gefahrbringende Ausfälle
Triacs, Diacs	–	1 484	2 968	50 % gefahrbringende Ausfälle
Integrierte Schaltungen (programmierbar und nicht programmierbar)	Herstellerdaten verwenden			50 % gefahrbringende Ausfälle

## C.6 Passive Bauteile

C.6 ist durch folgenden Abschnitt zu ersetzen:

## C.6 Passive Bauteile

Siehe Tabellen C.4 bis C.7.

**Tabelle C.4 — Kondensatoren**

Kondensator	Beispiel	MTTF für Bauteile Jahre	MTTF <sub>d</sub> für Bauteile Jahre Typisch	Bemerkungen
Standard, keine Leistung	KS, KP, KC, KT, MKT, MKC, MKP, MKU, MP, MKV	57 078	114 155	50 % gefahrbringende Ausfälle
Keramik	–	22 831	45 662	50 % gefahrbringende Ausfälle
Aluminiumelektrolyt	flüssiges Elektrolyt	22 831	45 662	50 % gefahrbringende Ausfälle
Aluminiumelektrolyt	festes Elektrolyt	37 671	75 342	50 % gefahrbringende Ausfälle
Tantalelektrolyt	flüssiges Elektrolyt	11 415	22 831	50 % gefahrbringende Ausfälle
Tantalelektrolyt	festes Elektrolyt	114 155	228 311	50 % gefahrbringende Ausfälle

**Tabelle C.5 — Widerstände**

Widerstand	Beispiel	MTTF für Bauteile Jahre	MTTF <sub>d</sub> für Bauteile Jahre Typisch	Bemerkungen
Kohleschicht	–	114 155	228 311	50 % gefahrbringende Ausfälle
Metallfilm	–	570 776	1 141 552	50 % gefahrbringende Ausfälle
Metalloxid und gewendelt	–	22 831	45 662	50 % gefahrbringende Ausfälle
Variabel	–	3 767	7 534	50 % gefahrbringende Ausfälle

**Tabelle C.6 — Induktivitäten**

Induktivität	Beispiel	MTTF für Bauteile Jahre	MTTF <sub>d</sub> für Bauteile Jahre Typisch	Bemerkungen
Für MC-Anwendung	–	37 671	75 342	50 % gefahrbringende Ausfälle
Niederfrequenz-Induktivitäten und Transformatoren	–	22 831	45 662	50 % gefahrbringende Ausfälle
Leistungstransformatoren und Transformatoren für Schaltanwendungen und Netzteile	–	11 415	22 831	50 % gefahrbringende Ausfälle

Tabelle C.7 — Optokoppler

Optokoppler	Beispiel	MTTF für Bauteile Jahre	MTTF <sub>d</sub> für Bauteile Jahre Typisch	Bemerkungen
Bipolar Ausgang	SFH 610	7 648	15 296	50 % gefahrbringende Ausfälle
FET Ausgang	LH 1056	2 854	5 708	50 % gefahrbringende Ausfälle

## 14 Änderung zu Anhang D

### D.1 „Parts-Count“-Verfahren

Tabelle D.1 ist durch folgende zu ersetzen:

Tabelle D.1 — Beispiel der Teilleiste auf einer Platine

<i>j</i>	Bauteil	Anzahl <i>n<sub>j</sub></i>	MTTF <sub>dj</sub> ungünstigster Fall Jahre	1/MTTF <sub>dj</sub> ungünstigster Fall 1/Jahr	<i>n<sub>j</sub></i> /MTTF <sub>dj</sub> ungünstigster Fall 1/Jahr
1	Transistoren, Bipolar, Kleinleistung (siehe Tabelle C.2)	2	11 420	0,000 087 6	0,000 175 2
2	Widerstand, Kohlefilm (siehe Tabelle C.5)	5	228 310	0,000 004 4	0,000 021 9
3	Kondensator, Standard, keine Leistung (siehe Tabelle C.4)	4	114 160	0,000 008 8	0,000 035 0
4	Relais, vom Hersteller angegebener Wert ( <i>B</i> <sub>10d</sub> = 20 000 000 Zyklen, <i>n</i> <sub>op</sub> = 633 600)	4	3 156,6	0,000 316 8	0,001 267 2
5	Schütz, vom Hersteller angegebener Wert ( <i>B</i> <sub>10d</sub> = 2 000 000 Zyklen, <i>n</i> <sub>op</sub> = 633 600)	1	315,7	0,003 167 6	0,003 167 6
Σ( <i>n<sub>j</sub></i> /MTTF <sub>dj</sub> )					0,004 666 9
MTTF <sub>d</sub> = 1/Σ( <i>n<sub>j</sub></i> /MTTF <sub>dj</sub> ) [Jahre]		214,3			

ANMERKUNG 1 ist durch folgende zu ersetzen:

„ANMERKUNG 1 Dieses Verfahren basiert auf der Annahme, dass ein gefährlicher Ausfall irgendeines Bauteils (Abschätzung des ungünstigsten Falls) im Kanal zu einem gefährlichen Ausfall des Kanals führt. Die MTTF<sub>d</sub>-Berechnung der Tabelle D.1 basiert auf dieser Annahme.“

### D.2 Die MTTF<sub>d</sub> für unterschiedliche Kanäle, Symmetrisierung der MTTF<sub>d</sub> für jeden Kanal

Satz nach Gleichung (D.2):

Der Satz ist wie folgt zu ersetzen:

„wobei MTTF<sub>dC1</sub> und MTTF<sub>dC2</sub> die Werte für zwei unterschiedliche redundante Kanäle sind, die jeweils auf einen Höchstwert von 100 Jahren (Kategorien B, 1, 2 und 3) oder 2 500 Jahren (Kategorie 4) begrenzt sind, bevor Gleichung (D.2) angewendet wird.“

## 15 Änderung zu Anhang E

### E.1 Beispiele für den Diagnosedeckungsgrad (DC)

*Eine zusätzliche ANMERKUNG 3 ist am Ende von Tabelle E.1 zu ergänzen:*

„ANMERKUNG 3 Für Maßnahmen, für die ein Bereich des Diagnosedeckungsgrades angegeben ist (z. B. Fehlererkennung durch den Prozess), kann der richtige DC-Wert durch Betrachten aller gefahrbringenden Ausfälle bestimmt werden und anschließend die Entscheidung getroffen werden, welcher von ihnen durch die DC-Maßnahme erkannt wird. Im Zweifelsfall sollte eine FMEA die Grundlage für die Abschätzung des DC darstellen.“

## 16 Änderung zu Anhang F

### F.1 Anforderungen an CCF

*Der zweite Satz ist wie folgt zu ersetzen (Streichen von „-bereich“):*

„Nicht alle Maßnahmen, die darin gegeben werden, sind für Maschinen geeignet.“

### F.2 Abschätzung der Auswirkung des CCF

*Tabelle F.1 ist durch folgende zu ersetzen:*

Tabelle F.1 — Verfahren zur Punktevergabe und Quantifizierung für Maßnahmen gegen CCF

Nr	Maßnahme gegen CCF	Punktezahl
<b>1</b>	<b>Trennung/Abtrennung</b>	
	Physikalische Trennung zwischen den Signalpfaden: — Trennung der Verdrahtung/Verrohrung, Erkennen von Kurschlüssen und offenen Stromkreisen in Kabeln durch dynamische Prüfung, getrennte Abschirmung des Signalpfads jedes Kanals und/oder — ausreichende Luft- und Kriechstrecken auf gedruckten Schaltungen.	<b>15</b>
<b>2</b>	<b>Diversität</b>	
	Unterschiedliche Technologien/Gestaltung oder physikalische Prinzipien werden verwendet, z. B.: — der erste Kanal elektronisch oder programmierbar elektronisch und der zweite Kanal elektromechanisch fest verdrahtet, — unterschiedliche Initiierung der Sicherheitsfunktion für jeden Kanal (z. B. Position, Druck, Temperatur), und/oder digitale und analoge Messung von Variablen (z. B. Abstand, Druck oder Temperatur) und/oder Bauteile von unterschiedlichen Herstellern.	<b>20</b>
<b>3</b>	<b>Entwurf/Anwendung/Erfahrung</b>	
3.1	Schutz gegen Überspannung, Überdruck, Überstrom, Übertemperatur, usw.	<b>15</b>
3.2	Verwendung bewährter Bauteile.	<b>5</b>
<b>4</b>	<b>Beurteilung/Analyse</b>	
	Für jedes Teil von sicherheitsbezogenen Teilen eines Steuerungssystems wurde eine Fehlermöglichkeits- und Einflussanalyse durchgeführt und deren Ergebnisse berücksichtigt, um Ausfälle infolge gemeinsamer Ursache bei der Gestaltung zu vermeiden.	<b>5</b>
<b>5</b>	<b>Kompetenz/Ausbildung</b>	
	Ausbildung der Konstrukteure, damit sie die Gründe und Auswirkungen von Ausfällen infolge gemeinsamer Ursache erkennen.	<b>5</b>
<b>6</b>	<b>Umgebung</b>	
6.1	Für elektrische/elektronische Systeme, Verhindern vor Verunreinigung und elektromagnetischen Störungen (EMV) zum Schutz vor Ausfällen infolge gemeinsamer Ursache entsprechend den einschlägigen Normen (z. B. IEC 61326-3-1) Fluidische Systeme: Filtrierung des Druckmediums, Verhinderung von Schmutzeintrag, Entwässerung von Druckluft, z. B. in Übereinstimmung mit den Anforderungen des Herstellers für die Reinheit des Druckmediums ANMERKUNG Bei kombinierten fluidischen und elektrischen Systemen sollten beide Aspekte berücksichtigt werden.	<b>25</b>
6.2	Andere Einflüsse Berücksichtigung der Anforderungen hinsichtlich Unempfindlichkeit gegenüber allen relevanten Umgebungsbedingungen wie Temperatur, Schock, Vibration, Feuchte (z. B. wie in den zutreffenden Normen festgelegt).	<b>10</b>
	<b>Gesamt</b>	<b>[max. erreichbar 100]</b>
<b>Gesamtpunktezahl</b>		<b>Maßnahmen, um CCF<sup>a</sup> zu vermeiden</b>
65 oder besser		Anforderungen erreicht
Kleiner als 65		Verfahren gescheitert ⇒ Auswahl zusätzlicher Maßnahmen
<sup>a</sup> Wenn technische Maßnahmen nicht relevant sind, können die Punkte der rechten Spalte bei der ausführlichen Berechnung berücksichtigt werden.		

## 17 Änderung zu Anhang G

### G.2 Maßnahmen zur Beherrschung systematischer Ausfälle

Letzter Absatz:

„Siehe auch ISO 13849-2:2002, D.3.“ *ist durch* „Siehe auch ISO 13849-2:2012, D.3.“ *zu ersetzen*.

### G.3 Maßnahmen zur Vermeidung systematischer Ausfälle

Absatz nach dem vierten Spiegelstrich:

*Folgende ANMERKUNG ist nach dem Satz zu ergänzen:*

„ANMERKUNG 1 Bauteile, wie z. B. hydraulische oder pneumatische Ventile, können zyklisches Schalten erfordern, um Ausfälle durch Nicht-Schalten oder durch unzulässig häufiges Schalten zu vermeiden. In diesem Fall ist eine wiederkehrende Prüfung notwendig.“

Absatz nach dem fünften Spiegelstrich:

„(siehe ISO 13849-2:2002, D.2)“ *ist durch* „(siehe ISO 13849-2:2012, D.2)“ *zu ersetzen*.

Nach dem letzten Spiegelstrich:

*Folgende ANMERKUNG ist zu ergänzen:*

„ANMERKUNG 2 IEC 61508-2:2011, Anhang F, legt Techniken und Maßnahmen zur Vermeidung systematischer Ausfälle während des Entwurfs und der Entwicklung von anwendungsspezifischen integrierten Schaltungen (ASIC), feldprogrammierbaren Gate-Arrays (FPGA), programmierbaren Logikbausteinen usw. fest.“

## 18 Änderung zu Anhang I

### Anhang I Beispiele

*Anhang I ist durch folgenden Anhang I zu ersetzen:*

## Anhang I (informativ)

### Beispiele

#### I.1 Allgemeines

Dieser Anhang stellt die Verwendung der in den Anhängen A bis H angegebenen Verfahren zur Ermittlung der Sicherheitsfunktionen und Bestimmung des PL vor. Es wird die Quantifizierung zweier weit verbreiteter Steuerstromkreise gezeigt. Für das schrittweise Vorgehen siehe Bild 3.

Zwei Beispiele (A und B) von Steuerstromkreisen von unterschiedlichen Maschinen werden betrachtet, siehe Bilder I.1 und I.3. Beide zeigen die Leistungsfähigkeit der gleichen Sicherheitsfunktion der Verriegelung der trennenden Schutzeinrichtung, haben aber unterschiedliche  $PL_r$  aufgrund der Unterschiede bei der Anwendung. Das erste Beispiel besteht aus einem Kanal aus elektromechanischen Bauteilen mit mittleren und hohen  $MTTF_d$ -Werten, während das zweite Beispiel aus zwei Kanälen besteht — einem elektromechanischen und einem programmierbar elektronischen — mit Bauteilen mit mittleren und hohen  $MTTF_d$ -Werten und mit entsprechender diagnostischer Prüfung.

#### I.2 Sicherheitsfunktion und erforderlicher Performance Level ( $PL_r$ )

Für beide Beispiele können die Anforderungen der Sicherheitsfunktion in Verbindung mit der Verriegelung der trennenden Schutzeinrichtung wie folgt festgelegt werden.

Die gefahrbringende Bewegung hält an, wenn die trennende Schutzeinrichtung geöffnet ist (durch Abbremsen oder Abschalten des Elektromotors).

**ANMERKUNG** Für das Beispiel B hat die Risikobeurteilung festgestellt, dass ein Verlust des kontrollierten Abbremsens des Motors infolge einer Fehlfunktion (B2, CC oder PLC) annehmbar war.

Der Mindestabstand zwischen der verriegelten trennenden Schutzeinrichtung und den beweglichen Teilen der Maschine wurde nach ISO 13855 ermittelt, basierend auf dem Anhaltevermögen der Maschine.

Für Beispiel A sehen die Risikoparameter entsprechend dem Verfahren mit Risikographen (siehe Bild A.1) wie folgt aus:

- Schwere der Verletzung, S = S2, sehr ernst;
- Häufigkeit und/oder Dauer der Gefährdungsexposition, F = F1, selten bis weniger häufig und/oder die Gefährdungsexpositionszeit ist kurz;
- Möglichkeit zur Vermeidung der Gefährdung, P = P1, möglich unter bestimmten Voraussetzungen.

Diese Auswahl an Risikoparametern führt zu einem erforderlichen Performance Level  $PL_r$  von „c“.

Bestimmung der bevorzugten Kategorie: ein Performance Level von „c“ kann üblicherweise durch hochzuverlässige einkanalige Systeme (Kategorie 1) oder durch redundante Architekturen (Kategorie 2 oder 3) erreicht werden (siehe Bild 5 und Abschnitt 6).

Für Beispiel B sind die Risikoparameter S2 und P1 die gleichen aber bei der Häufigkeit und/oder Gefährdungsexpositionszeit ist F = F2, häufig oder dauernd und/oder die Gefährdungsexpositionszeit ist von langer Dauer.

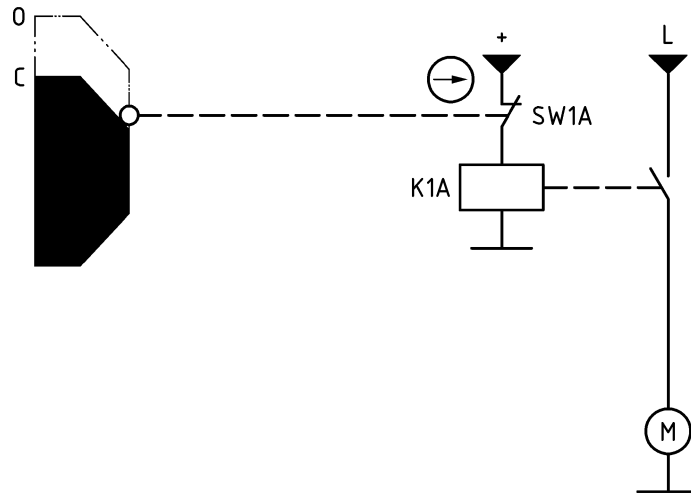
Diese Entscheidungen führen zu einem erforderlichen Performance Level  $PL_r$  von „d“.

Bestimmung der bevorzugten Kategorie: ein Performance Level von „d“ kann in der Regel durch redundante Architekturen erreicht werden (Kategorie 2 oder 3) (siehe Bild 5 und Abschnitt 6).

### I.3 Beispiel A, einkanaliges System

#### I.3.1 Identifikation der sicherheitsbezogenen Teile

Alle Bauteile, die zur Sicherheitsfunktion mit verriegelter trennender Schutzeinrichtung beitragen, sind in Bild I.1 dargestellt. Andere Bauteile, die nicht zur Sicherheitsfunktion beitragen (z. B. Start- und Stoppschalter) sind aus Gründen der Einfachheit weggelassen worden.



#### Legende

o	offen
c	geschlossen
M	Motor
K1A	Hilfsschütz
SW1A	Positionsschalter (NC)

**Bild I.1 — Schaltplan A zur Ausführung der Sicherheitsfunktion**

In diesem Beispiel wird ein Positionsschalter SW1A mit Zwangsöffnung und zwangsläufiger Betätigung verwendet, jedoch ohne begründeten Fehlerausschluss. Der Positionsschalter ist mit einem Hilfskontakt K1A verbunden, der in der Lage ist, die Energiezufuhr zum Motor auszuschalten. Die wesentlichen Merkmale dieser sicherheitsbezogenen Teile sind daher:

- ein Kanal aus elektromechanischen Bauteilen;
- Positionsschalter SW1A (NC) hat zwangsöffnende Kontakte und hohen  $B_{10d}$ ;
- Hilfskontakt K1A hat hohen  $B_{10d}$ .

Der Positionsschalter und der Hilfskontakt in diesem Beispiel gelten beide als bewährte Bauteile, wenn sie nach ISO 13849-2 angewendet werden.

Die sicherheitsbezogenen Teile können in einem sicherheitsbezogenen Blockdiagramm dargestellt werden, wie in Bild I.2 gezeigt.



#### Legende

K1A	Hilfsschütz
SW1A	Positionsschalter

**Bild I.2 — Sicherheitsbezogenes Blockdiagramm, das die sicherheitsbezogenen Teile von Beispiel A zeigt**

### I.3.2 Quantifizierung von $MTTF_d$ , $DC_{avg}$ , Ausfall infolge gemeinsamer Ursache, Kategorie, PL

Es wird angenommen, dass die Werte für  $MTTF_d$ ,  $DC_{avg}$  und der Ausfall infolge gemeinsamer Ursache nach den Anhängen C, D, E und F abgeschätzt oder durch den Hersteller angegeben werden. Die Kategorien werden nach 6.2 ermittelt.

#### — $MTTF_d$

Der Positionsschalter SW1A und der Hilfsschütz K1A tragen zur  $MTTF_d$  des einen Kanals bei. Es wird angenommen, dass die Werte von  $B_{10d,SW1A} = 20\,000\,000$  Zyklen (Positionsschalter unabhängig von der Last) und  $B_{10d,K1A} = 400\,000$  Zyklen (Hilfsschütz mit maximaler Last) vom Hersteller zur Verfügung gestellt werden. Durch Anwendung des Verfahrens von C.4.2 mit 220 Arbeitstagen pro Jahr, 8 Arbeitsstunden je Tag und einer Zyklusdauer von 60 Minuten ergibt sich  $MTTF_{d,SW1A} = 113\,636$  Jahre und  $MTTF_{d,K1A} = 2\,273$  Jahre. Anschließend wird mithilfe des Parts-Count-Verfahrens nach D.1 der  $MTTF_d$  eines Kanals mit folgender Gleichung berechnet:

$$\frac{1}{MTTF_d} = \frac{1}{MTTF_{d,SW1A}} + \frac{1}{MTTF_{d,K1A}} = \frac{1}{113\,636 \text{ Jahre}} + \frac{1}{2\,273 \text{ Jahre}} = \frac{0,000\,45}{\text{Jahre}} \quad (I.1)$$

woraus sich  $MTTF_d = 2\,222$  Jahre (begrenzt auf 100 Jahre) für den Kanal ergibt, der „hoch“ nach 4.5.2, Tabelle 5, ist.

ANMERKUNG Wenn keine Informationen zu SW1A oder K1A zur Verfügung stehen, könnte eine Annahme für den ungünstigsten Fall nach C.2 oder C.4 gemacht werden.

#### — $T_{10d}$

Das in C.4.2 angegebene Verfahren ergibt  $T_{10d,SW1A}$  mit 11 364 Jahren und  $T_{10d,K1A}$  mit 227 Jahren, die beide die Gebrauchsdauer von 20 Jahren überschreiten und aus diesem Grund die Notwendigkeit eines vorbeugenden Austauschs ausschließen.

#### — DC

Da keine diagnostische Prüfung im Steuerstromkreis A erfolgt, ist der  $DC = 0$  oder „kein“ nach 4.5.3, Tabelle 6.

#### — CCF

Da nur ein Kanal verwendet wird, sind Maßnahmen gegen CCF nicht relevant.

#### — Kategorie

Die Eigenschaften von Kategorie 1 (grundlegende und bewährte Sicherheitsprinzipien, bewährte Bauteile) sind erfüllt, einschließlich der Anforderung, dass der  $MTTF_d$  des Kanals „hoch“ sein muss.

Eingangsdaten für Bild 5:  $MTTF_d$  des Kanals ist „hoch“ (100 Jahre),  $DC_{avg}$  ist „kein“ und Kategorie ist 1.

Mithilfe von Bild 5 wird dies als Performance Level c gewertet.

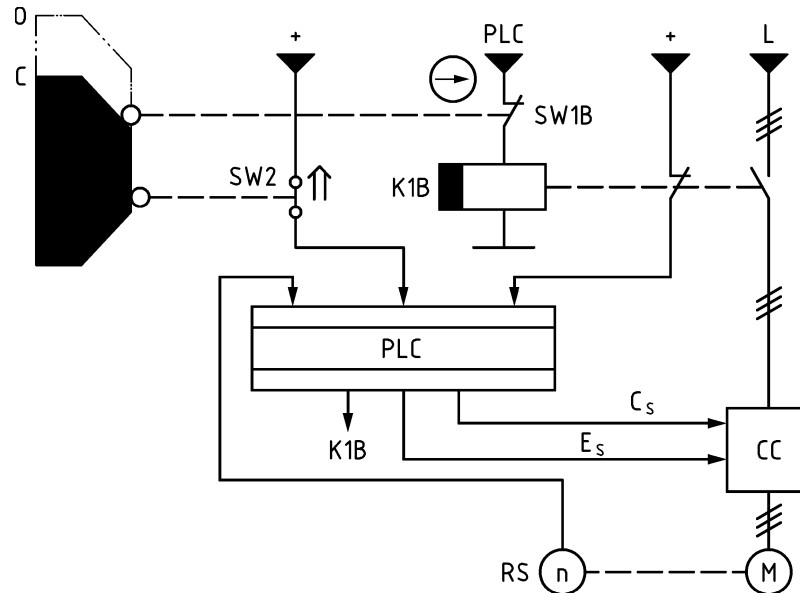
Die Anwendung von Anhang K ergibt eine mittlere Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde ( $PFH_D$ ) von  $1,14 \times 10^{-6}/h$  und PL c.

Das Ergebnis entspricht dem erforderlichen Performance Level c nach I.2. Der Steuerstromkreis A erfüllt somit die Anforderungen an die Risikominderung für das Anwendungsbeispiel A nach I.2, mit S2, F1, P1 und  $PL_r$  c.

## I.4 Beispiel B, redundantes System

### I.4.1 Identifikation der sicherheitsbezogenen Teile

Alle Bauteile, die zur Sicherheitsfunktion der verriegelten trennenden Schutzeinrichtung beitragen, sind in Bild I.3 dargestellt. Andere Bauteile, die nicht zur Sicherheitsfunktion beitragen (z. B. Start- und Stoppschalter oder die Abfallverzögerung von K1B) wurden aus Gründen der Einfachheit weggelassen.



#### Legende

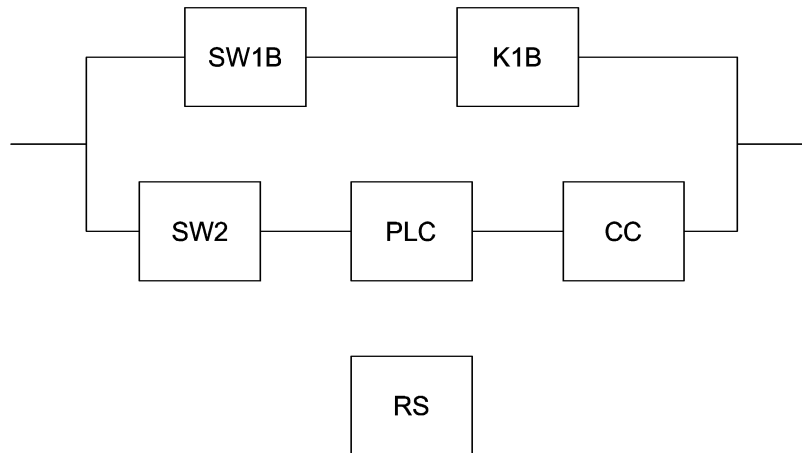
PLC	speicherprogrammierbare Steuerung	<b>C<sub>s</sub></b>	<b>Stopp-Signal (normal)</b>
CC	Stromrichter	E <sub>s</sub>	Einschalten (normal)
M	Motor	K1B	Hilfsschütz
RS	Drehgeber	SW1B	Positionsschalter (NC)
o	offen	SW2	Positionsschalter (NO)
c	geschlossen		

**Bild I.3 — Schaltplan B zur Ausführung der Sicherheitsfunktion**

In diesem zweiten Beispiel wird eine Architektur mit zwei Kanälen verwendet, um die Redundanz bereitzustellen. Wie in Beispiel A umfasst der erste Kanal einen Positionsschalter SW1B mit zwangsöffnenden Kontakten in zwangsläufiger Betätigung. Dieser Positionsschalter ist mit einem Hilfschütz K1B verbunden, der in der Lage ist, die Energiezufuhr zum Motor abzuschalten. Im zweiten Kanal, der (speicherprogrammierbare) elektronische Bauteile enthält, ist ein zweiter Positionsschalter SW2 an eine speicherprogrammierbare Steuerung PLC angeschlossen, der den Stromrichter CC ansteuern kann, um die Energiezufuhr zum Motor auszuschalten. Die wesentlichen Merkmale dieser sicherheitsbezogenen Teile sind daher:

- redundante Kanäle, ein elektromechanischer und ein programmierbar elektronischer;
- nur der Positionsschalter SW1B (NC) verfügt über zwangsöffnende Kontakte, aber beide Positionsschalter SW1B und SW2 haben einen hohen  $B_{10d}$ ;
- die  $MTTF_d$  des Hilfschützes K1B ist hoch;
- die  $MTTF_d$  der elektronischen Bauteile PLC und CC sind mittel.

Die sicherheitsbezogenen Teile und ihre Aufteilung in Kanäle kann in einem sicherheitsbezogenen Blockdiagramm, wie in Bild I.4 gezeigt, dargestellt werden.



Der erste Kanal besteht somit aus SW1B und K1B und der zweite Kanal besteht aus SW2, PLC und CC, während RS nur zur Prüfung des Stromrichters verwendet wird.

**Legende**

- SW1B Positionsschalter
- K1B Hilfsschütz
- SW2 Positionsschalter
- PLC speicherprogrammierbare Steuerung
- CC Stromrichter
- RS Drehgeber

**Bild I.4 — Blockdiagramme, die die sicherheitsbezogenen Teile aus Beispiel B kennzeichnen**

**I.4.2 Quantifizierung der  $MTTF_d$  für jeden Kanal,  $DC_{avg}$ , Ausfall infolge gemeinsamer Ursache, Kategorie und PL**

Es wird angenommen, dass die Werte für  $MTTF_d$  für jeden Kanal,  $DC_{avg}$  und Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache nach den Anhängen C, D, E und F bewertet werden oder durch den Hersteller angegeben werden. Die Kategorien werden nach 6.2 ermittelt.

Der Positionsschalter SW1B verfügt über Zwangsöffnung mit zwangsläufiger Betätigung, jedoch wird kein Fehlerausschluss für die mechanischen Teile begründet.

—  **$MTTF_d$**

Der Positionsschalter SW1B und der Hilfsschütz K1B tragen zur  $MTTF_{d,C1}$  des ersten Kanals bei. Es wird angenommen, dass die Werte von  $B_{10d,SW1B} = 20\,000\,000$  Zyklen (Positionsschalter unabhängig von der Last) und  $B_{10d,K1B} = 400\,000$  Zyklen (Hilfsschütz mit maximaler Last) vom Hersteller zur Verfügung gestellt werden. Durch Anwendung von Verfahren C.4.2 mit 300 Arbeitstagen pro Jahr, 16 Arbeitsstunden je Tag und einer Zyklusdauer von 4 Minuten ergibt sich  $MTTF_{d,SW1B} = 2\,778$  Jahre und  $MTTF_{d,K1B} = 56$  Jahre. Anschließend wird mithilfe des Parts-Count-Verfahrens nach D.1 der  $MTTF_{d,C1}$  des ersten Kanals mit folgender Gleichung berechnet:

$$\frac{1}{MTTF_{d,C1}} = \frac{1}{MTTF_{d,SW1B}} + \frac{1}{MTTF_{d,K1B}} = \frac{1}{2\,778 \text{ Jahre}} + \frac{1}{56 \text{ Jahre}} = \frac{0,018}{\text{Jahre}} \tag{I.2}$$

woraus sich  $MTTF_d = 56$  Jahre für den Kanal ergibt, der „hoch“ nach 4.5.2, Tabelle 5 ist.

Im zweiten Kanal tragen SW2, PLC und CC zur  $MTTF_{d,C2}$  bei. Von  $B_{10d,SW2}$  von 1 000 000 Zyklen wird angenommen, dass er vom Hersteller zur Verfügung gestellt wird. Die Anwendung des Verfahrens von C.4.2, wie für den ersten Kanal, ergibt eine  $MTTF_{d,SW2}$  von 139 Jahren. Für PLC und CC wird angenommen, dass eine  $MTTF_d$  von 20 Jahren vom Hersteller angegeben wird. Anschließend wird mithilfe des Parts-Count-Verfahrens nach D.1 der  $MTTF_{d,C2}$  des zweiten Kanals mit folgender Gleichung berechnet:

$$\frac{1}{MTTF_{d,C2}} = \frac{1}{MTTF_{d,SW2}} + \frac{1}{MTTF_{d,PLC}} + \frac{1}{MTTF_{d,CC}} = \frac{1}{139 \text{ Jahre}} + \frac{1}{20 \text{ Jahre}} + \frac{1}{20 \text{ Jahre}} = \frac{0,11}{\text{Jahre}} \quad (I.3)$$

woraus sich  $MTTF_d = 9,1$  Jahre für den Kanal ergibt, der „niedrig“ nach 4.5.2 ist.

ANMERKUNG Wenn keine Informationen für SW1B, SW2 oder K1B bezüglich der  $MTTF_d$  zur Verfügung stehen, könnte eine Annahme für den ungünstigsten Fall nach C.2 oder C.4 gemacht werden.

Da beide Kanäle unterschiedliche Werte für  $MTTF_d$  besitzen, kann Gleichung (D.2) verwendet werden, um äquivalente identische Werte für  $MTTF_d$  für ein symmetrisches Zwei-Kanal-System zu berechnen. Durch Anwendung dieser Gleichung ergibt sich  $MTTF_d = 37$  Jahre für jeden Kanal, der „hoch“ nach 4.5.2, Tabelle 5 ist.

#### — $T_{10d}$

Das in C.4.2 angegebene Verfahren ergibt  $T_{10d,SW1B}$  mit 278 Jahren und  $T_{10d,K1B}$  mit 5,6 Jahren und  $T_{10d,SW2}$  mit 13,9 Jahren, wobei die letzten beiden kürzer sind als die Gebrauchsdauer von 20 Jahren. Die Abschätzung von PL und PFH ist somit nur gültig, wenn K1B und SW2 früher als nach 5,6 Jahren und 13,9 Jahren Betriebszeit ausgetauscht werden.

#### — DC

Im Steuerstromkreis B werden fünf der sicherheitsbezogenen Teile durch die PLC geprüft. Diese Prüfung besteht aus SW1B, SW2 und K1B, die durch die PLC zurückgelesen werden, CC wird durch PLC über RS zurückgelesen und PLC führt Selbstprüfungen durch. Die zugehörigen DC-Werte zu jedem dieser geprüften Teile sind:

- 1)  $DC_{SW1B} = DC_{SW2} = 99 \%$ , „hoch“ aufgrund Plausibilitätsprüfung, siehe Tabelle E.1 (zweite Zeile der Eingabeeinheit);
- 2)  $DC_{K1B} = 99 \%$ , „hoch“, aufgrund der zwangsgeführten Öffner-/Schließer-Kombination, siehe Tabelle E.1 (zweite Zeile der Eingabeeinheit);
- 3)  $DC_{PLC} = 30 \%$ , „kein“ aufgrund der niedrigen Wirksamkeit der Selbsttests (der Hersteller des PLC gibt den Wert auf Grundlage einer Berechnung durch beispielsweise FMEA an); und
- 4)  $DC_{CC} = 90 \%$ , „mittel“, aufgrund indirekter Überwachung der Antriebselemente durch die Steuerung, siehe Tabelle E.1 (sechste Zeile der Eingabeeinheit) — wenn die PLC einen Ausfall des CC bemerkt, ist es möglich die Bewegung mit dem Einschalter (Standard) anzuhalten und den Hilfsschutz K1B abzuschalten (zusätzlicher Abschaltpfad).

Für eine Abschätzung des PL wird als Eingabe für Bild 5 ein mittlerer DC-Wert ( $DC_{avg}$ ) benötigt.

$$DC_{avg} = \frac{\frac{DC_{SW1B}}{MTTF_{d,SW1B}} + \frac{DC_{K1B}}{MTTF_{d,K1B}} + \frac{DC_{SW2}}{MTTF_{d,SW2}} + \frac{DC_{PLC}}{MTTF_{d,PLC}} + \frac{DC_{CC}}{MTTF_{d,CC}}}{\frac{1}{MTTF_{d,SW1B}} + \frac{1}{MTTF_{d,K1B}} + \frac{1}{MTTF_{d,SW2}} + \frac{1}{MTTF_{d,PLC}} + \frac{1}{MTTF_{d,CC}}}$$

$$= \frac{\frac{0,99}{2\,778 \text{ Jahre}} + \frac{0,99}{56 \text{ Jahre}} + \frac{0,99}{139 \text{ Jahre}} + \frac{0,3}{20 \text{ Jahre}} + \frac{0,9}{20 \text{ Jahre}}}{\frac{1}{2\,778 \text{ Jahre}} + \frac{1}{56 \text{ Jahre}} + \frac{1}{139 \text{ Jahre}} + \frac{1}{20 \text{ Jahre}} + \frac{1}{20 \text{ Jahre}}} = \frac{0,09}{0,13} = 67,9 \% \quad (I.4)$$

Demnach ist der sich daraus ergebende  $DC_{avg}$  „niedrig“ nach 4.5.3 und Tabelle 6.

— CCF

Für eine Abschätzung der Maßnahmen gegen CCF nach F.2 sind die Ergebnisse für Steuerstromkreis B in Tabelle I.1 angegeben.

**Tabelle I.1 — Abschätzung der Maßnahmen gegen CCF für das Beispiel B**

Nr	Betrachtungseinheit	Punktezahl für den Steuerstromkreis	Maximal mögliches Ergebnis
<b>1</b>	<b>Trennung/Abtrennung</b>		
	Physikalische Trennung zwischen den Signalwegen	15	15
<b>2</b>	<b>Diversität</b>		
	Unterschiedliche Technologien/Gestaltung oder physikalische Prinzipien werden verwendet	20	20
<b>3</b>	<b>Gestaltung/Anwendung/Erfahrung</b>		
3.1	Schutz gegen Überspannung, Überdruck, Überstrom usw.	15	15
3.2	Verwendung bewährter Bauteile	kein (nur teilweise erfüllt, siehe F.2)	5
<b>4</b>	<b>Beurteilung/Analyse</b>		
	Sind die Ergebnisse einer Ausfallart und Effektanalyse berücksichtigt worden, um Ausfälle aufgrund gemeinsamer Ursache in der Entwicklung zu vermeiden?	Kein	5
<b>5</b>	<b>Kompetenz/Ausbildung</b>		
	Sind Konstrukteure geschult worden, um die Gründe und Auswirkungen von Ausfällen infolge gemeinsamer Ursache zu verstehen?	Kein	5
<b>6</b>	<b>Umgebung</b>		
6.1	Schutz vor Verunreinigung und elektromagnetischer Beeinflussung (EMV) gegen CCF in Übereinstimmung mit den einschlägigen Normen	25	25
6.2	<b>Andere Einflüsse</b> Wurden alle Anforderungen hinsichtlich Unempfindlichkeit gegenüber allen relevanten Umgebungsbedingungen wie Temperatur, Schock, Vibration, Feuchte (z. B. wie in den maßgeblichen Normen festgelegt) berücksichtigt?	10	10
	<b>Gesamt</b>	85	Max. 100

Ausreichende Maßnahmen gegen CCF erfordern eine Mindestpunktezahl von mindestens 65; somit ist im Beispiel B eine Punktezahl von 85 ausreichend, um die Anforderungen gegen CCF zu erfüllen.

Die Eigenschaften von Kategorie 3 wurden erfüllt, da ein einzelner Fehler in irgendeinem Teil nicht zum Verlust der Sicherheitsfunktion führt; wenn immer in angemessener Weise durchführbar, wird der einzelne Fehler vor der nächsten Anforderung der Sicherheitsfunktion erkannt; der Diagnosedeckungsgrad ( $DC_{avg}$ ) ist im Bereich 60 % bis 90 %; die Maßnahmen gegen CCF sind ausreichend und der äquivalente  $MTTF_d$  für jeden Kanal ist „hoch“.

Eingangsdaten für Bild 5:  $MTTF_d$  für den Kanal ist „hoch“ (37 Jahre),  $DC_{avg}$  ist „niedrig“ und die Kategorie ist 3.

Durch Anwendung von Bild 5 kann dies als Performance Level d gewertet werden.

Die Anwendung von Anhang K ergibt eine mittlere Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde ( $PFH_D$ ) von  $5,16 \times 10^{-7}/h$  und PL d.

Dieses Ergebnis entspricht dem erforderlichen Performance Level d von I.2. Somit erfüllt ein Steuerstromkreis B die Anforderungen zur Risikominderung der Beispielanwendung B von I.2 mit S2, F2, P1 und PL<sub>r</sub> d.

## 19 Änderung zu Anhang K

### Anhang K Numerische Darstellung von Bild 5

*Tabelle K.1 ist durch folgende neue Tabelle zu ersetzen:*

Tabelle K.1 — Numerische Darstellung von Bild 5

MTTF <sub>d</sub> für jeden Kanal Jahre	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (1/h) und der zugehörige Performance Level (PL)													
	Kat. B		Kat. 1		Kat. 2		Kat. 2		Kat. 3		Kat. 3		Kat. 4	
	PL	DC <sub>avg</sub> = kein	PL	DC <sub>avg</sub> = kein	PL	DC <sub>avg</sub> = niedrig	PL	DC <sub>avg</sub> = mittel	PL	DC <sub>avg</sub> = niedrig	PL	DC <sub>avg</sub> = mittel	PL	DC <sub>avg</sub> = hoch
3	a	$3,80 \times 10^{-5}$			a	$2,58 \times 10^{-5}$	a	$1,99 \times 10^{-5}$	a	$1,26 \times 10^{-5}$	a	$6,09 \times 10^{-6}$	b	
3,3	a	$3,46 \times 10^{-5}$			a	$2,33 \times 10^{-5}$	a	$1,79 \times 10^{-5}$	a	$1,13 \times 10^{-5}$	a	$5,41 \times 10^{-6}$	b	
3,6	a	$3,17 \times 10^{-5}$			a	$2,13 \times 10^{-5}$	a	$1,62 \times 10^{-5}$	a	$1,03 \times 10^{-5}$	a	$4,86 \times 10^{-6}$	b	
3,9	a	$2,93 \times 10^{-5}$			a	$1,95 \times 10^{-5}$	a	$1,48 \times 10^{-5}$	a	$9,37 \times 10^{-6}$	b	$4,40 \times 10^{-6}$	b	
4,3	a	$2,65 \times 10^{-5}$			a	$1,76 \times 10^{-5}$	a	$1,33 \times 10^{-5}$	a	$8,39 \times 10^{-6}$	b	$3,89 \times 10^{-6}$	b	
4,7	a	$2,43 \times 10^{-5}$			a	$1,60 \times 10^{-5}$	a	$1,20 \times 10^{-5}$	a	$7,58 \times 10^{-6}$	b	$3,48 \times 10^{-6}$	b	
5,1	a	$2,24 \times 10^{-5}$			a	$1,47 \times 10^{-5}$	a	$1,10 \times 10^{-5}$	a	$6,91 \times 10^{-6}$	b	$3,15 \times 10^{-6}$	b	
5,6	a	$2,04 \times 10^{-5}$			a	$1,33 \times 10^{-5}$	a	$9,87 \times 10^{-6}$	b	$6,21 \times 10^{-6}$	b	$2,80 \times 10^{-6}$	c	
6,2	a	$1,84 \times 10^{-5}$			a	$1,19 \times 10^{-5}$	a	$8,80 \times 10^{-6}$	b	$5,53 \times 10^{-6}$	b	$2,47 \times 10^{-6}$	c	
6,8	a	$1,68 \times 10^{-5}$			a	$1,08 \times 10^{-5}$	a	$7,93 \times 10^{-6}$	b	$4,98 \times 10^{-6}$	b	$2,20 \times 10^{-6}$	c	
7,5	a	$1,52 \times 10^{-5}$			a	$9,75 \times 10^{-6}$	b	$7,10 \times 10^{-6}$	b	$4,45 \times 10^{-6}$	b	$1,95 \times 10^{-6}$	c	
8,2	a	$1,39 \times 10^{-5}$			a	$8,87 \times 10^{-6}$	b	$6,43 \times 10^{-6}$	b	$4,02 \times 10^{-6}$	b	$1,74 \times 10^{-6}$	c	
9,1	a	$1,25 \times 10^{-5}$			a	$7,94 \times 10^{-6}$	b	$5,71 \times 10^{-6}$	b	$3,57 \times 10^{-6}$	b	$1,53 \times 10^{-6}$	c	
10	a	$1,14 \times 10^{-5}$			a	$7,18 \times 10^{-6}$	b	$5,14 \times 10^{-6}$	b	$3,21 \times 10^{-6}$	b	$1,36 \times 10^{-6}$	c	
11	a	$1,04 \times 10^{-5}$			a	$6,44 \times 10^{-6}$	b	$4,53 \times 10^{-6}$	b	$2,81 \times 10^{-6}$	c	$1,18 \times 10^{-6}$	c	
12	b	$9,51 \times 10^{-6}$			b	$5,84 \times 10^{-6}$	b	$4,04 \times 10^{-6}$	b	$2,49 \times 10^{-6}$	c	$1,04 \times 10^{-6}$	c	
13	b	$8,78 \times 10^{-6}$			b	$5,33 \times 10^{-6}$	b	$3,64 \times 10^{-6}$	b	$2,23 \times 10^{-6}$	c	$9,21 \times 10^{-7}$	d	

Tabelle K.1 (fortgesetzt)

MTTF <sub>d</sub> für jeden Kanal Jahre	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (1/h) und der zugehörige Performance Level (PL)													
	Kat. B	PL	Kat. 1	PL	Kat. 2	PL	Kat. 2	PL	Kat. 3	PL	Kat. 3	PL	Kat. 4	PL
	DC <sub>avg</sub> = kein		DC <sub>avg</sub> = kein		DC <sub>avg</sub> = niedrig		DC <sub>avg</sub> = mittel		DC <sub>avg</sub> = niedrig		DC <sub>avg</sub> = mittel		DC <sub>avg</sub> = hoch	
15	7,61 × 10 <sup>-6</sup>	b			4,53 × 10 <sup>-6</sup>	b	3,01 × 10 <sup>-6</sup>	b	1,82 × 10 <sup>-6</sup>	c	7,44 × 10 <sup>-7</sup>	d		
16	7,13 × 10 <sup>-6</sup>	b			4,21 × 10 <sup>-6</sup>	b	2,77 × 10 <sup>-6</sup>	c	1,67 × 10 <sup>-6</sup>	c	6,76 × 10 <sup>-7</sup>	d		
18	6,34 × 10 <sup>-6</sup>	b			3,68 × 10 <sup>-6</sup>	b	2,37 × 10 <sup>-6</sup>	c	1,41 × 10 <sup>-6</sup>	c	5,67 × 10 <sup>-7</sup>	d		
20	5,71 × 10 <sup>-6</sup>	b			3,26 × 10 <sup>-6</sup>	b	2,06 × 10 <sup>-6</sup>	c	1,22 × 10 <sup>-6</sup>	c	4,85 × 10 <sup>-7</sup>	d		
22	5,19 × 10 <sup>-6</sup>	b			2,93 × 10 <sup>-6</sup>	c	1,82 × 10 <sup>-6</sup>	c	1,07 × 10 <sup>-6</sup>	c	4,21 × 10 <sup>-7</sup>	d		
24	4,76 × 10 <sup>-6</sup>	b			2,65 × 10 <sup>-6</sup>	c	1,62 × 10 <sup>-6</sup>	c	9,47 × 10 <sup>-7</sup>	d	3,70 × 10 <sup>-7</sup>	d		
27	4,23 × 10 <sup>-6</sup>	b			2,32 × 10 <sup>-6</sup>	c	1,39 × 10 <sup>-6</sup>	c	8,04 × 10 <sup>-7</sup>	d	3,10 × 10 <sup>-7</sup>	d		
30			3,80 × 10 <sup>-6</sup>	b	2,06 × 10 <sup>-6</sup>	c	1,21 × 10 <sup>-6</sup>	c	6,94 × 10 <sup>-7</sup>	d	2,65 × 10 <sup>-7</sup>	d	9,54 × 10 <sup>-8</sup>	e
33			3,46 × 10 <sup>-6</sup>	b	1,85 × 10 <sup>-6</sup>	c	1,06 × 10 <sup>-6</sup>	c	5,94 × 10 <sup>-7</sup>	d	2,30 × 10 <sup>-7</sup>	d	8,57 × 10 <sup>-8</sup>	e
36			3,17 × 10 <sup>-6</sup>	b	1,67 × 10 <sup>-6</sup>	c	9,39 × 10 <sup>-7</sup>	d	5,16 × 10 <sup>-7</sup>	d	2,01 × 10 <sup>-7</sup>	d	7,77 × 10 <sup>-8</sup>	e
39			2,93 × 10 <sup>-6</sup>	c	1,53 × 10 <sup>-6</sup>	c	8,40 × 10 <sup>-7</sup>	d	4,53 × 10 <sup>-7</sup>	d	1,78 × 10 <sup>-7</sup>	d	7,11 × 10 <sup>-8</sup>	e
43			2,65 × 10 <sup>-6</sup>	c	1,37 × 10 <sup>-6</sup>	c	7,34 × 10 <sup>-7</sup>	d	3,87 × 10 <sup>-7</sup>	d	1,54 × 10 <sup>-7</sup>	d	6,37 × 10 <sup>-8</sup>	e
47			2,43 × 10 <sup>-6</sup>	c	1,24 × 10 <sup>-6</sup>	c	6,49 × 10 <sup>-7</sup>	d	3,35 × 10 <sup>-7</sup>	d	1,34 × 10 <sup>-7</sup>	d	5,76 × 10 <sup>-8</sup>	e
51			2,24 × 10 <sup>-6</sup>	c	1,13 × 10 <sup>-6</sup>	c	5,80 × 10 <sup>-7</sup>	d	2,93 × 10 <sup>-7</sup>	d	1,19 × 10 <sup>-7</sup>	d	5,26 × 10 <sup>-8</sup>	e
56			2,04 × 10 <sup>-6</sup>	c	1,02 × 10 <sup>-6</sup>	c	5,10 × 10 <sup>-7</sup>	d	2,52 × 10 <sup>-7</sup>	d	1,03 × 10 <sup>-7</sup>	d	4,73 × 10 <sup>-8</sup>	e
62			1,84 × 10 <sup>-6</sup>	c	9,06 × 10 <sup>-7</sup>	d	4,43 × 10 <sup>-7</sup>	d	2,13 × 10 <sup>-7</sup>	d	8,84 × 10 <sup>-8</sup>	e	4,22 × 10 <sup>-8</sup>	e
68			1,68 × 10 <sup>-6</sup>	c	8,17 × 10 <sup>-7</sup>	d	3,90 × 10 <sup>-7</sup>	d	1,84 × 10 <sup>-7</sup>	d	7,68 × 10 <sup>-8</sup>	e	3,80 × 10 <sup>-8</sup>	e
75			1,52 × 10 <sup>-6</sup>	c	7,31 × 10 <sup>-7</sup>	d	3,40 × 10 <sup>-7</sup>	d	1,57 × 10 <sup>-7</sup>	d	6,62 × 10 <sup>-8</sup>	e	3,41 × 10 <sup>-8</sup>	e
82			1,39 × 10 <sup>-6</sup>	c	6,61 × 10 <sup>-7</sup>	d	3,01 × 10 <sup>-7</sup>	d	1,35 × 10 <sup>-7</sup>	d	5,79 × 10 <sup>-8</sup>	e	3,08 × 10 <sup>-8</sup>	e
91			1,25 × 10 <sup>-6</sup>	c	5,88 × 10 <sup>-7</sup>	d	2,61 × 10 <sup>-7</sup>	d	1,14 × 10 <sup>-7</sup>	d	4,94 × 10 <sup>-8</sup>	e	2,74 × 10 <sup>-8</sup>	e
100			1,14 × 10 <sup>-6</sup>	c	5,28 × 10 <sup>-7</sup>	d	2,29 × 10 <sup>-7</sup>	d	1,01 × 10 <sup>-7</sup>	d	4,29 × 10 <sup>-8</sup>	e	2,47 × 10 <sup>-8</sup>	e

Tabelle K.1 (fortgesetzt)

MTTF <sub>d</sub> für jeden Kanal Jahre	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (1/h) und der zugehörige Performance Level (PL)													
	Kat. B	PL	Kat. 1	PL	Kat. 2	PL	Kat. 2	PL	Kat. 3	PL	Kat. 3	PL	Kat. 4	PL
	DC <sub>avg</sub> = kein		DC <sub>avg</sub> = kein		DC <sub>avg</sub> = niedrig		DC <sub>avg</sub> = mittel		DC <sub>avg</sub> = niedrig		DC <sub>avg</sub> = mittel		DC <sub>avg</sub> = hoch	
110													$2,23 \times 10^{-8}$	e
120													$2,03 \times 10^{-8}$	e
130													$1,87 \times 10^{-8}$	e
150													$1,61 \times 10^{-8}$	e
160													$1,50 \times 10^{-8}$	e
180													$1,33 \times 10^{-8}$	e
200													$1,19 \times 10^{-8}$	e
220													$1,08 \times 10^{-8}$	e
240													$9,81 \times 10^{-9}$	e
270													$8,67 \times 10^{-9}$	e
300													$7,76 \times 10^{-9}$	e
330													$7,04 \times 10^{-9}$	e
360													$6,44 \times 10^{-9}$	e
390													$5,94 \times 10^{-9}$	e
430													$5,38 \times 10^{-9}$	e
470													$4,91 \times 10^{-9}$	e
510													$4,52 \times 10^{-9}$	e
560													$4,11 \times 10^{-9}$	e
620													$3,70 \times 10^{-9}$	e
680													$3,37 \times 10^{-9}$	e
750													$3,05 \times 10^{-9}$	e
820													$2,79 \times 10^{-9}$	e
910													$2,51 \times 10^{-9}$	e
1 000													$2,28 \times 10^{-9}$	e

Tabelle K.1 (fortgesetzt)

MTTF <sub>d</sub> für jeden Kanal Jahre	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (1/h) und der zugehörige Performance Level (PL)													
	Kat. B	PL	Kat. 1	PL	Kat. 2	PL	Kat. 2	PL	Kat. 3	PL	Kat. 3	PL	Kat. 4	PL
	DC <sub>avg</sub> = kein		DC <sub>avg</sub> = kein		DC <sub>avg</sub> = niedrig		DC <sub>avg</sub> = mittel		DC <sub>avg</sub> = niedrig		DC <sub>avg</sub> = mittel		DC <sub>avg</sub> = hoch	
1 200													$1,90 \times 10^{-9}$	e
1 300													$1,75 \times 10^{-9}$	e
1 500													$1,51 \times 10^{-9}$	e
1 600													$1,42 \times 10^{-9}$	e
1 800													$1,26 \times 10^{-9}$	e
2 000													$1,13 \times 10^{-9}$	e
2 200													$1,03 \times 10^{-9}$	e
2 300													$9,85 \times 10^{-10}$	e
2 400													$9,44 \times 10^{-10}$	e
2 500													$9,06 \times 10^{-10}$	e

## Literaturhinweise

Folgendes ist zu ergänzen:

“ISO/TR 23849, *Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery (identisch mit IEC/TR 62061-1)*“

BGIA-Report 2/2008e, *Funktionale Sicherheit von Maschinensteuerungen — Anwendung der DIN EN ISO 13849*, Deutsche Gesetzliche Unfallversicherung (DGUV), Juni 2009, ISBN 978-3-88383-793-2, kostenloser Download im Internet unter [www.dguv.de/ifa/en/pub](http://www.dguv.de/ifa/en/pub)“