

ICS 13.110;

PN-EN ISO 13849-1

listopad 2008

Wprowadza
EN ISO 13849-1:2008, IDT

ISO 13849-1:2006, IDT

Zastępuje
PN-EN ISO 13849-1:2006

**Bezpieczeństwo maszyn -- Elementy systemów sterowania związane z
bezpieczeństwem -- Część 1: Ogólne zasady projektowania**

Na wniosek Komitetu Technicznego nr 158

ds. Bezpieczeństwa Maszyn i Urządzeń Technicznych oraz Ergonomii - Zagadnienia Ogólne

**Norma Europejska EN ISO 13849-1:2008 Safety of machinery - Safety-related parts of control systems -
Part 1: General principles for design (ISO 13849-1:2006),**
ma status Polskiej Normy

© Copyright by PKN, Warszawa 2008

nr ref. PN-EN ISO 13849-1:2008

HOLOGRAM
PKN

Wszelkie prawa autorskie zastrzeżone. Żadna część niniejszej publikacji nie może być zwielokrotniana jakąkolwiek techniką bez pisemnej zgody Prezesa Polskiego Komitetu Normalizacyjnego

ISBN 978-83-251-6369-3

EUROPÄISCHE NORM
EUROPEAN STANDARD
NORME EUROPÉENNE

EN ISO 13849-1

Juni 2008

ICS 13.110

Ersatz für EN ISO 13849-1:2006

Deutsche Fassung

Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze (ISO 13849-1:2006)

Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design (ISO 13849-1:2006)

Sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 1: Principes généraux de conception (ISO 13849-1:2006)

Diese Europäische Norm wurde vom CEN am 18.Mai 2008 angenommen.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Management-Zentrum des CEN oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Zentralsekretariat mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, Ungarn, dem Vereinigten Königreich und Zypern.



EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

Management-Zentrum: rue de Stassart, 36 B-1050 Brüssel

EN ISO 13849-1:2008 (D)

Inhalt

	Seite
Vorwort	4
Einleitung.....	5
1 Anwendungsbereich	7
2 Normative Verweisungen	7
3 Begriffe, Formelzeichen und Abkürzungen	8
3.1 Begriffe	8
3.2 Formelzeichen und Abkürzungen	14
4 Gestaltungsaspekte.....	15
4.1 Sicherheitsziele in der Gestaltung	15
4.2 Strategie der Risikominderung	17
4.2.1 Allgemeines	17
4.2.2 Beitrag der Risikominderung durch das Steuerungssystem.....	17
4.3 Bestimmung des erforderlichen Performance Levels (PL _r)	21
4.4 Entwicklung des SRP/CS	21
4.5 Bewertung des erreichten Performance Levels PL und die Beziehung zum SIL	22
4.5.1 Performance Level PL	22
4.5.2 Mittlere Zeit bis zum gefahrbringenden Ausfall jedes Kanals (MTTF _d).....	24
4.5.3 Diagnosedeckungsgrad (DC)	25
4.5.4 Vereinfachtes Verfahren zur Abschätzung eines PL	25
4.6 Software-Sicherheitsanforderungen.....	28
4.6.1 Allgemeines	28
4.6.2 Sicherheitsbezogene Embedded-Software (SRESW)	29
4.6.3 Sicherheitsbezogene Anwendungssoftware (SRASW)	30
4.6.4 Softwarebasierende Parametrisierung.....	32
4.7 Verifikation, dass der erreichte PL den PL _r erfüllt	33
4.8 Ergonomische Aspekte der Gestaltung	34
5 Sicherheitsfunktionen	34
5.1 Spezifikation der Sicherheitsfunktionen	34
5.2 Nähere Angaben über die Sicherheitsfunktionen	37
5.2.1 Sicherheitsbezogene Stoppfunktion	37
5.2.2 Manuelle Rückstellungsfunktion.....	37
5.2.3 Start-/Wiederaufnahmefunktion	38
5.2.4 Lokale Steuerungsfunktion	38
5.2.5 Mutingfunktion	38
5.2.6 Ansprechzeit	39
5.2.7 Sicherheitsbezogene Parameter	39
5.2.8 Schwankungen, Verlust und Wiederkehr der Energiequellen	39
6 Die Kategorien und deren Beziehung zur MTTF _d jedes Kanals, DC _{avg} und CCF.....	39
6.1 Allgemeines	39
6.2 Spezifikation der Kategorien	40
6.2.1 Allgemeines	40
6.2.2 Vorgesehene Architekturen.....	40
6.2.3 Kategorie B.....	41
6.2.4 Kategorie 1	41
6.2.5 Kategorie 2	43
6.2.6 Kategorie 3	44
6.2.7 Kategorie 4	45
6.3 Kombination von SRP/CS, um einen Gesamt-PL zu erreichen.....	48
7 Berücksichtigung von Fehlern, Fehlerausschluss	50
7.1 Allgemeines.....	50
7.2 Fehlerbetrachtung	50
7.3 Fehlerausschluss.....	51

	Seite
8 Validierung	51
9 Instandhaltung	51
10 Technische Dokumentation	51
11 Benutzerinformation	52
Anhang A (informativ) Bestimmung des erforderlichen Performance Levels (PL_r)	54
Anhang B (informativ) Blockmethode und sicherheitsbezogenes Blockdiagramm	57
Anhang C (informativ) Berechnung oder Abschätzung von MTTF_d-Werten für einzelne Bauteile	59
Anhang D (informativ) Vereinfachtes Verfahren zur Bestimmung der MTTF_d für jeden Kanal	67
Anhang E (informativ) Abschätzungen des Diagnosedeckungsgrades (DC) für Funktionen und Module	69
Anhang F (informativ) Abschätzungen der Ausfälle aufgrund gemeinsamer Ursache (CCF)	72
Anhang G (informativ) Systematischer Ausfall	74
Anhang H (informativ) Beispiel der Kombination von verschiedenen sicherheitsbezogenen Teilen einer Steuerung	77
Anhang I (informativ) Beispiele	80
Anhang J (informativ) Software	87
Anhang K (informativ) Numerische Darstellung von Bild 5	90
Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EG-Richtlinie 98/37/EG geändert durch Richtlinie 98/79/EG	92
Anhang ZB (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EG-Richtlinie 2006/42/EG	93
Literaturhinweise	94

EN ISO 13849-1:2008 (D)

Vorwort

Der Text von ISO 13849-1:2006 wurde vom Technischen Komitee ISO/TC 199 „Safety of machinery“ der Internationalen Organisation für Standardisierung (ISO) erarbeitet und wurde als EN ISO 13849-1:2008 vom Technischen Komitee CEN/TC 114 „Safety of machinery“ übernommen, dessen Sekretariat vom DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis November 2008, und etwaige entgegenstehende nationale Normen müssen bis November 2009 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Texte dieses Dokuments Patentrechte berühren können. CEN [und/oder CENELEC] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Dieses Dokument ersetzt EN ISO 13849-1:2006.

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

Zum Zusammenhang mit EG-Richtlinien siehe informativen Anhang ZA und ZB, der Bestandteil dieses Dokuments ist.

Entsprechend der CEN/CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Slowakei, Slowenien, Spanien, Tschechische Republik, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

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

Einleitung

Die Struktur von Sicherheitsnormen auf dem Gebiet der Maschinen ist wie folgt.

- a) Typ-A-Normen (Sicherheitsgrundnormen) behandeln Grundbegriffe, Gestaltungsleitsätze und allgemeine Aspekte, die auf Maschinen angewandt werden können.
- b) Typ-B-Normen (Sicherheitsfachgrundnormen) behandeln einen Sicherheitsaspekt oder eine Art von Schutzeinrichtungen, die für eine ganze Reihe von Maschinen verwendet werden können:
 - Typ-B1-Normen für bestimmte Sicherheitsaspekte (z. B. Sicherheitsabstände, Oberflächentemperatur, Lärm);
 - Typ-B2-Normen für Schutzeinrichtungen (z. B. Zweihandschaltungen, Verriegelungseinrichtungen, druckempfindliche Schutzeinrichtungen, trennende Schutzeinrichtungen).
- c) Typ-C-Normen (Maschinensicherheitsnormen) behandeln detaillierte Sicherheitsanforderungen an eine bestimmte Maschinen oder eine Gruppe von Maschinen.

Dieser Teil der ISO 13849 ist eine Typ-B1-Norm wie in ISO 12100-1 dargelegt.

Wenn sich die Bestimmungen einer Typ-C-Norm von denen unterscheiden, die in einer Typ-A- oder Typ-B-Norm dargelegt sind, haben die Bestimmungen der Typ-C-Norm Vorrang vor anderen Normen für Maschinen, die nach den Bestimmungen der Typ-C-Norm entworfen und hergestellt worden sind.

Mit diesem Teil der ISO 13849 ist beabsichtigt, für diejenigen einen Leitfaden zu geben, die an der Gestaltung und Beurteilung von Steuerungen beteiligt sind und für Technische Komitees, die Typ-B2- und Typ-C-Normen erarbeiten, mit der Vermutung, mit den wesentlichen Sicherheitsanforderungen des Anhangs I der Maschinenrichtlinie 98/37/EG, der Maschinen-Richtlinie, übereinzustimmen. Sie gibt keine besondere Anleitung zur Übereinstimmung mit anderen EG-Richtlinien.

Als Teil einer Gesamtrisikominderung an einer Maschine wird ein Konstrukteur oft Maßnahmen durch die Anwendung von Schutzeinrichtungen zur Risikoreduzierung ergreifen, die eine oder mehrere Sicherheitsfunktionen verwenden.

Teile einer Maschinensteuerung, die Sicherheitsfunktionen liefern sollen, werden sicherheitsbezogene Teile einer Steuerung (SRP/CS) genannt, und diese Teile können entweder aus Hardware und Software bestehen und separater oder integraler Bestandteil der Maschinensteuerung sein. Zusätzlich zur Bereitstellung von Sicherheitsfunktionen kann ein SRP/CS auch Betriebsfunktionen liefern (z. B. eine Zweihandsteuerung zum Start eines Prozesses).

Die Fähigkeit sicherheitsbezogener Teile von Steuerungen, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen, wird einer von fünf Stufen zugeordnet, den so genannten Performance Level (PL). Diese Performance Level werden definiert in Form der Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde (siehe Tabelle 3).

Die Wahrscheinlichkeit eines gefahrbringenden Ausfalls der Sicherheitsfunktion hängt von mehreren Faktoren ab, einschließlich der Hardware- und Softwarestruktur, dem Umfang der Fehler-Detektionsmechanismen [Diagnosedeckungsgrad (DC)], der Zuverlässigkeit von Bauteilen [mittlere Zeit bis zum gefahrbringenden Ausfall (MTTF_d)], den Ausfällen infolge gemeinsamer Ursache (CCF)], dem Gestaltungsprozess, der Belastung im Betrieb, den Umgebungsbedingungen und den betrieblichen Einsatzbedingungen.

Um den Konstrukteur zu unterstützen und als Hilfe zur Bestimmung des erreichten PL, stellt diese Norm eine Methode auf Basis einer Kategorisierung von Strukturen nach speziellen Entwurfskriterien und spezifiziertem Verhalten bei Fehlerbedingungen bereit. Diese Kategorien werden einer von fünf Stufen zugeordnet, genannt Kategorien B, 1, 2, 3 und 4.

EN ISO 13849-1:2008 (D)

Die Performance Level und Kategorien können angewendet werden für sicherheitsbezogene Teile von Steuerungen, wie:

- nicht trennende Schutzeinrichtungen (z. B. Zweihandschaltungen, Verriegelungseinrichtungen), berührungslos wirkende Schutzeinrichtungen (z. B. Lichtschranken), druckempfindliche Schutzeinrichtungen,
- Steuerungsbaugruppen (z. B. die Logik für Steuerungsfunktionen, Datenverarbeitung, Überwachung usw.), und
- Leistungsschaltelemente (z. B. Relais, Ventile usw.)

als auch Sicherheitsfunktionen ausführende Steuerungen in allen Arten von Maschinen — von einfachen (z. B. einer kleinen Küchenmaschine oder automatischen Türen und Toren) bis zu einer Fertigungsanlage (z. B. Verpackungsmaschinen, Druckmaschinen, Pressen).

Dieser Teil der 13849 liefert eine verständliche Basis, auf der die Gestaltung und Leistungsfähigkeit jeder Anwendung eines SRP/CS (und der Maschine) beurteilt werden kann, z. B. durch Dritte, innerhalb einer Organisation oder durch eine unabhängige Prüfstelle.

Informationen zur empfohlenen Anwendung der IEC 62061 und dieses Teils der ISO 13849

Die IEC 62061 und dieser Teil der ISO 13849 legen Anforderungen für den Entwurf und die Realisierung sicherheitsbezogener Steuerungssysteme von Maschinen fest. Der Anwender einer von beiden Normen kann in Übereinstimmung mit deren Anwendungsbereichen annehmen, die relevanten und erforderlichen Sicherheitsanforderungen zu erfüllen. Die folgende Tabelle fasst die Anwendungsbereiche der IEC 62061 und dieses Teils der ISO 13849 zusammen.

Tabelle 1 — Empfohlene Anwendung der IEC 62061 und ISO 13849-1

	Technologie für die Implementierung der sicherheitsbezogenen Steuerungsfunktion(en)	ISO 13849-1	IEC 62061
A	Nicht elektrisch, z. B. hydraulisch	X	Nicht enthalten
B	Elektromechanisch, z. B. Relais und/oder nicht komplexe Elektronik	Beschränkt auf die vorgesehenen Architekturen ^a und bis PL = e	Alle Architekturen und bis SIL 3
C	Komplexe Elektronik, z. B. programmierbar	Beschränkt auf die vorgesehenen Architekturen ^a und bis PL = d	Alle Architekturen und bis SIL 3
D	A kombiniert mit B	Beschränkt auf die vorgesehenen Architekturen ^a und bis PL = e	X ^c
E	C kombiniert mit B	Beschränkt auf die vorgesehenen Architekturen ^a und bis PL = d	Alle Architekturen und bis SIL 3
F	C kombiniert mit A, oder C kombiniert mit A und B	X ^b	X ^c
X	zeigt, dass dieses Merkmal in der Norm der entsprechenden Tabellenüberschrift behandelt wird.		
a	Um ein einfaches Verfahren zur Berechnung des Performance Levels zu ermöglichen, sind vorgesehene Architekturen in 6.2 beschrieben.		
b	Für komplexe Elektronik: Verwendung der vorgesehenen Architekturen nach diesem Teil der ISO 13849 bis PL = d oder irgendeine Architektur nach IEC 62061.		
c	Für nicht elektrische Technologie, Verwendung der Teile nach diesem Teil der ISO 13849 als Teilsysteme.		

1 Anwendungsbereich

Dieser Teil der ISO 13849 stellt Sicherheitsanforderungen und einen Leitfaden für die Prinzipien der Gestaltung und Integration sicherheitsbezogener Teile von Steuerungen (SRP/CS) bereit, einschließlich der Entwicklung von Software. Für diese Teile der SRP/CS werden Eigenschaften, einschließlich des Performance Levels, festgelegt, die zur Ausführung der entsprechenden Sicherheitsfunktionen erforderlich sind. Er ist anzuwenden auf SRP/CS aller Arten von Maschinen, ungeachtet der verwendeten Technologie und Energie (elektrisch, hydraulisch, pneumatisch, mechanisch usw.).

Er legt nicht fest, welche Sicherheitsfunktionen oder Performance Level für einen speziellen Fall verwendet werden.

Dieser Teil der ISO 13849 stellt spezielle Anforderungen für SRP/CS mit programmierbarer elektronischen Systemen bereit.

Er stellt keine speziellen Anforderungen an den Entwurf von Produkten, die Teile von SRP/CS sind. Trotzdem können die angegebenen Prinzipien, wie Kategorien oder Performance Level, verwendet werden.

ANMERKUNG 1 Beispiele von Produkten, die Teile von SRP/CS sind: Relais, Magnetventile, Positionsschalter, PLC(en), Antriebssteuerungen, Zweihandschaltungen, druckempfindliche Schutzeinrichtungen. Für den Entwurf solcher Produkte ist es wichtig, sich auf spezielle anwendbare Internationale Normen zu beziehen, z. B. ISO 13851, ISO 13856-1 und ISO 13856-2.

ANMERKUNG 2 Für die Definition des *erforderlichen Performance Levels*, siehe 3.1.24.

ANMERKUNG 3 Die in diesem Teil der ISO 13849 bereitgestellten Anforderungen für programmierbare elektronische Systeme sind kompatibel mit der Methodik für Gestaltung und Entwicklung sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungen für Maschinen in der IEC 62061.

ANMERKUNG 4 Für sicherheitsbezogene Embedded-Software in Komponenten mit $PL_r = e$, siehe IEC 61508-3:1998, Abschnitt 7.

ANMERKUNG 5 Siehe auch Tabelle 1.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

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 13849-2:2003, *Safety of machinery — Safety-related parts of control systems — Part 2: Validation*

ISO 14121¹⁾, *Safety of machinery — Principles of risk assessment*

IEC 60050-191:1990, *International Electrotechnical Vocabulary — Chapter 191: Dependability and quality of service* and IEC 60050-191: -am 1:1999 and IEC 60050-191-am2:2002:1999, *Amendment 1 and Amendment 2, International Electrotechnical Vocabulary — Chapter 191: Dependability and quality of service*

1) Noch zu veröffentlichen (Überarbeitung von ISO 14121:1999).

EN ISO 13849-1:2008 (D)

IEC 61508-3:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements*, and IEC 61508-3 Corr. 1:1999, *Corrigendum 1 — Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements*

IEC 61508-4:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations*, and IEC 61508-4 Corr. 1:1999, *Corrigendum 1 — Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations*

3 Begriffe, Formelzeichen und Abkürzungen**3.1 Begriffe**

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO 12100-1, IEC 60050-191 und die folgenden Begriffe.

3.1.1**sicherheitsbezogenes Teil einer Steuerung****SRP/CS**

Teil einer Steuerung, das auf sicherheitsbezogene Eingangssignale reagiert und sicherheitsbezogene Ausgangssignale erzeugt

ANMERKUNG 1 Die Kombination sicherheitsbezogener Teile einer Steuerung beginnt an dem Punkt, an dem sicherheitsbezogene Signale erzeugt werden (einschließlich z. B. Betätiger und Rolle eines Positionsschalters) und endet an den Ausgängen der Leistungssteuerungselemente (einschließlich z. B. Hauptkontakte eines Schützes).

ANMERKUNG 2 Werden Überwachungssysteme zur Diagnose verwendet, werden sie wie SRP/CS behandelt.

3.1.2**Kategorie**

Einstufung der sicherheitsbezogenen Teile einer Steuerung bezüglich ihres Widerstandes gegen Fehler und ihres nachfolgenden Verhaltens bei einem Fehler, das erreicht wird durch die Struktur der Anordnung der Teile, der Fehlererkennung und/oder ihrer Zuverlässigkeit

3.1.3**Fehler**

Zustand einer Einheit, charakterisiert durch die Unfähigkeit, eine geforderte Funktion auszuführen, ausgenommen der Unfähigkeit während vorbeugender Wartung oder anderer geplanter Handlungen, oder aufgrund des Fehlens externer Mittel

ANMERKUNG 1 Ein Fehler ist oft das Resultat eines Ausfalls der Einheit selbst, kann aber ohne vorherigen Ausfall bestehen.

[IEC 60050-191:1990, 05-01]

ANMERKUNG 2 In diesem Teil der ISO 13849 bedeutet der Begriff „Fehler“ *zufälliger Fehler*.

3.1.4**Ausfall**

Beendigung der Fähigkeit einer Einheit, eine geforderte Funktion zu erfüllen

ANMERKUNG 1 Nach einem Ausfall hat die Einheit einen Fehler.

ANMERKUNG 2 Der „Ausfall“ ist ein Ereignis, im Unterschied zum „Fehler“, dieser ist ein Zustand.

ANMERKUNG 3 Der so definierte Begriff kann nicht angewendet werden auf Einheiten, die nur aus Software bestehen.

[IEC 60050-191:1990, 04-01]

ANMERKUNG 4 Ausfälle, die nur die Verfügbarkeit des zu steuernden Prozesses betreffen, liegen nicht im Anwendungsbereich dieses Teils der ISO 13849.

3.1.5**gefährbringender Ausfall**

Ausfall der das Potential hat, das SRP/CS in einen gefährlichen Zustand oder eine Fehlfunktion zu bringen

ANMERKUNG 1 Ob dieses Potential bemerkt werden kann oder nicht, hängt von der Architektur des Systems ab; in einem redundanten System wird ein gefährlicher Hardwareausfall weniger wahrscheinlich zu einem gefährlichen Ausfall des Gesamtsystems führen.

ANMERKUNG 2 Abgeleitet von IEC 61508-4:1998, Begriff 3.6.7.

3.1.6**Ausfall infolge gemeinsamer Ursache****CCF**

Ausfälle verschiedener Einheiten aufgrund eines einzelnen Ereignisses, wobei diese Ausfälle nicht auf gegenseitiger Ursache beruhen

[IEC 60050-191-am 1:1999, 04-23]

ANMERKUNG Ausfälle infolge gemeinsamer Ursache sollten nicht verwechselt werden mit gleichartigen Ausfällen (siehe ISO 12100-1:2003, 3.34).

3.1.7**systematischer Ausfall**

Ausfall mit deterministischem Bezug zu einer bestimmten Ursache, der nur durch Änderung der Gestaltung oder des Herstellungsprozesses, Betriebsverfahren, Dokumentation oder zugehörigen Faktoren, beseitigt werden kann

ANMERKUNG 1 Instandsetzung ohne Änderung wird üblicherweise den Grund des Ausfalls nicht beseitigen.

ANMERKUNG 2 Ein systematischer Ausfall kann hervorgerufen werden durch Simulation der Ausfallursache.

[IEC 60050-191:1990, 04-19]

ANMERKUNG 3 Beispielursachen systematischer Ausfälle beinhalten menschliches Versagen in:

- der Spezifikation der Sicherheitsanforderungen,
- der Gestaltung, der Herstellung, der Installation, des Betriebs der Hardware und
- der Gestaltung, Realisierung usw. der Software.

3.1.8**Muting**

vorübergehende automatische Unterdrückung einer (der) Sicherheitsfunktion(en) durch das SRP/CS

3.1.9**manuelle Rückstellung**

interne Funktion des SRP/CS zum manuellen Wiederherstellen einer oder mehrerer Sicherheitsfunktionen, vor dem Neustart einer Maschine verwendet

3.1.10**Schaden**

physische Verletzung oder Schädigung der Gesundheit

[ISO 12100-1:2003, 3.5]

EN ISO 13849-1:2008 (D)

3.1.11

Gefährdung

potentielle Schadensquelle

ANMERKUNG 1 Eine Gefährdung kann spezifiziert werden, um damit den Ursprung (z. B. mechanische Gefährdung, elektrische Gefährdung) oder die Art des zu erwartenden Schadens (z. B. Gefährdung durch elektrischen Schlag, Gefährdung durch Schneiden, Gefährdung durch Vergiftung, Gefährdung durch Feuer) näher zu bezeichnen.

ANMERKUNG 2 Die Gefährdung im Sinne dieser Definition

- ist entweder bei der bestimmungsgemäßen Verwendung der Maschine dauerhaft vorhanden (z. B. Bewegung von gefährdenden beweglichen Teilen, Lichtbogen beim Schweißen, ungesunde Körperhaltung, Geräuschemission, hohe Temperatur);
- oder kann unerwartet auftreten (z. B. Explosion, Gefährdung durch Quetschen als Folge eines unbeabsichtigten/unerwarteten Anlaufs, Herausschleudern als Folge eines Bruchs, Stürzen als Folge von Beschleunigung/Abbremsen).

[ISO 12100-1:2003, 3.6]

3.1.12

Gefährdungssituation

Sachlage, bei der eine Person mindestens einer Gefährdung ausgesetzt ist, diese Situation führt unmittelbar oder über einen Zeitraum hinweg zu einem Schaden

[ISO 12100-1:2003, 3.9]

3.1.13

Risiko

Kombination der Wahrscheinlichkeit des Eintritts eines Schadens und seines Schadensausmaßes

[ISO 12100-1:2003, 3.11]

3.1.14

Restrisiko

verbleibendes Risiko, nachdem Schutzmaßnahmen ergriffen wurden

(Siehe Bild 2)

ANMERKUNG In Anlehnung an ISO 12100-1:2003, Begriff 3.12.

3.1.15

Risikobeurteilung

Gesamtheit des Verfahrens, das eine Risikoanalyse und Risikobewertung umfasst

[ISO 12100-1:2003, 3.13]

3.1.16

Risikoanalyse

Kombination aus Festlegung der Grenzen der Maschine, Identifizierung der Gefährdung und Risikoeinschätzung

[ISO 12100-1:2003, 3.14]

3.1.17

Risikobewertung

auf der Risikoanalyse beruhende Beurteilung, ob die Ziele zur Risikominderung erreicht wurden

[ISO 12100-1:2003, 3.16]

3.1.18**bestimmungsgemäße Verwendung einer Maschine**

Verwendung einer Maschine in Übereinstimmung mit den in der Benutzerinformation bereitgestellten Informationen

[ISO 12100-1:2003, 3.22]

3.1.19**vernünftigerweise vorhersehbare Fehlanwendung**

Verwendung einer Maschine in einer Weise, die vom Konstrukteur nicht vorgesehen ist, sich jedoch aus dem leicht vorhersehbaren menschlichen Verhalten ergeben kann

[ISO 12100-1:2003, 3.23]

3.1.20**Sicherheitsfunktion**

Funktion einer Maschine, wobei ein Ausfall der Funktion zur unmittelbaren Erhöhung des Risikos (der Risiken) führen kann

[ISO 12100-1:2003, 3.28]

3.1.21**Überwachung**

Sicherheitsfunktion, die sicherstellt, dass eine Schutzmaßnahme eingeleitet wird, wenn die Fähigkeit eines Bauteils oder eines Elements seine Funktion auszuführen, vermindert wird oder die Betriebsbedingungen so verändert werden, dass eine Reduzierung des Betrags der Risikominderung entsteht

3.1.22**programmierbares elektronisches System****PES**

System zur Steuerung, Schutz oder Überwachung, abhängig von seiner Funktion auf der Basis einer oder mehrerer programmierbarer elektronischer Geräte, einschließlich aller Elemente dieses Systems wie Stromversorgung, Sensoren und andere Eingabegeräte, Schütze und anderer Ausgabegeräte

ANMERKUNG In Anlehnung an IEC 61508-4:1998, Begriff 3.3.2.

3.1.23**Performance Level****PL**

diskreter Level, der die Fähigkeit von sicherheitsbezogenen Teilen einer Steuerung spezifiziert, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen

ANMERKUNG Siehe 4.5.1.

3.1.24**erforderlicher Performance Level****PL_r**

angewandter Performance Level (PL), um die erforderliche Risikominderung für jede Sicherheitsfunktion zu erreichen

ANMERKUNG Siehe Bilder 2 und A.1.

3.1.25**mittlere Zeit bis zum gefahrbringenden Ausfall****MTTF_d**

Erwartungswert der mittleren Zeit bis zum gefahrbringenden Ausfall

ANMERKUNG In Anlehnung an IEC 62061:2005, Begriff 3.2.34.

EN ISO 13849-1:2008 (D)**3.1.26****Diagnosedeckungsgrad****DC**

Maß für die Wirksamkeit der Diagnose, die bestimmt werden kann als Verhältnis der Ausfallrate der bemerkten gefährlichen Ausfälle und Ausfallrate der gesamten gefährlichen Ausfälle

ANMERKUNG 1 Der Diagnosedeckungsgrad kann für die Gesamtheit oder für Teile des sicherheitsbezogenen Systems gelten. Zum Beispiel könnte ein Diagnosedeckungsgrad für die Sensoren und/oder das Logiksystem und/oder die Stellglieder vorhanden sein.

ANMERKUNG 2 In Anlehnung an IEC 61508-4:1998, Begriff 3.8.6.

3.1.27**Schutzmaßnahme**

Maßnahme zur vorgesehenen Minderung des Risikos

BEISPIEL 1 Umgesetzt vom Konstrukteur: inhärente Gestaltung, technische Schutzmaßnahmen und ergänzende Schutzmaßnahmen, Benutzerinformation.

BEISPIEL 2 Umgesetzt vom Benutzer: durch Organisation (sichere Arbeitsverfahren, Beaufsichtigung, Betriebs-erlaubnis zur Ausführung von Arbeiten), Bereitstellung und Anwendung zusätzlicher Schutzeinrichtungen (persönliche Schutzausrüstung; Ausbildung).

ANMERKUNG In Anlehnung an ISO 12100-1:2003, Begriff 3.18.

3.1.28**Gebrauchsdauer** **T_M**

Zeitraum, der die vorgegebene Verwendung der SRP/CS abdeckt

3.1.29**Testrate** **r_t**

Häufigkeit der automatischen Tests, um Fehler in einem SRP/CS zu bemerken, Kehrwert des Diagnose-Testintervalls

3.1.30**Anforderungsrate** **r_d**

Häufigkeit je Zeiteinheit von Anforderungen an eine sicherheitsbezogene Reaktion eines SRP/CS

3.1.31**Reparaturrate** **r_r**

Kehrwert der Zeitspanne zwischen der Erkennung eines gefahrbringenden Ausfalls, durch entweder einen Online-Test oder einer offensichtlichen Fehlfunktion des Systems, und Wiederanlauf nach System-/ Bauteilaustausch.

ANMERKUNG Die Reparaturzeit beinhaltet nicht die Zeitspanne, die zur Fehlererkennung benötigt wird.

3.1.32**Maschinensteuerung**

System, das auf Eingangssignale von Teilen der Maschine, des Benutzers, externer Steuerungseinrichtungen oder irgendeiner Kombination dieser, reagiert und Ausgangssignale erzeugt, damit sich die Maschine in der vorgesehenen Art und Weise verhält

ANMERKUNG Die Maschinensteuerung kann jede Technologie oder Kombination verschiedener Technologien verwenden (z. B. elektrische/elektronische, hydraulische, pneumatische, mechanische).

3.1.33**Sicherheits-Integritätslevel****SIL**

diskrete Stufe (eine von vier möglichen) zur Spezifizierung der Sicherheitsintegrität der Sicherheitsfunktionen, die dem E/E/PE-sicherheitsbezogenen System zugeordnet werden, wobei der Sicherheits-Integritätslevel 4 die höchste Stufe und der Sicherheits-Integritätslevel 1 die niedrigste ist

[IEC 61508-4:1998, 3.5.6]

3.1.34**Programmiersprache mit eingeschränktem Sprachumfang****LVL**

Typ einer Sprache, die die Fähigkeit hat, vordefinierte, anwendungsspezifische, Bibliotheksfunktionen zu kombinieren, um die Spezifikation der Sicherheitsanforderungen zu implementieren

ANMERKUNG 1 In Anlehnung an IEC 61511-1:2003, Begriff 3.2.80.1.2.

ANMERKUNG 2 Typische Beispiele von LVL (Kontaktplan, Funktions-Blockdiagramm) sind in IEC 61131-3 angegeben.

ANMERKUNG 3 Ein typisches Beispiel von einem System, das die LVL verwendet: PLC.

3.1.35**Programmiersprache mit nicht eingeschränktem Sprachumfang****FVL**

Typ einer Sprache mit der Fähigkeit, einen großen Bereich von Funktionen und Anwendungen zu implementieren

BEISPIEL C, C++, Assembler.

ANMERKUNG 1 In Anlehnung an IEC 61511-1:2003, Begriff 3.2.80.1.3.

ANMERKUNG 2 Ein typisches Beispiel von Systemen für die Verwendung von FVL: Embedded-Systeme.

ANMERKUNG 3 Im Bereich der Maschinen wird FVL in Embedded-Software und gelegentlich in Anwendungssoftware eingesetzt.

3.1.36**Anwendungssoftware**

Software, die speziell für die Anwendung vom Hersteller in die Maschine implementiert, und üblicherweise logische Sequenzen, Grenzwerte und Ausdrücke zum Steuern der entsprechenden Eingänge, Ausgänge, Berechnungen und Entscheidungen enthält, um die notwendigen Anforderungen des SRP/CS zu erfüllen

3.1.37**Embedded-Software**

Firmware

Systemsoftware

Software, die als Teil des Systems durch den Steuerungshersteller geliefert wird und die durch den Anwender der Maschine nicht verändert werden kann

ANMERKUNG Üblicherweise wird Embedded-Software in FVL geschrieben.

EN ISO 13849-1:2008 (D)

3.2 Formelzeichen und Abkürzungen

Siehe Tabelle 2.

Tabelle 2 — Formelzeichen und Abkürzungen

Formelzeichen oder Abkürzung	Beschreibung	Definition oder Fundort
a, b, c, d, e	Bezeichnung für die Performance Level	Tabelle 3
AOPD	aktive opto-elektronische Schutzeinrichtungen (z. B. Lichtschranke)	Anhang H
B, 1, 2, 3, 4	Bezeichnung für die Kategorien	Tabelle 7
B_{10d}	Anzahl von Zyklen, bis 10 % der Komponenten gefährlich ausgefallen sind (für pneumatische und elektromechanische Komponenten)	Anhang C
Cat.	Kategorie	3.1.2
CC	Stromrichter	Anhang I
CCF	Ausfall aufgrund gemeinsamer Ursache	3.1.6
DC	Diagnosedeckungsgrad	3.1.26
DC_{avg}	durchschnittlicher Diagnosedeckungsgrad	E.2
F, F1, F2	Häufigkeit und/oder Dauer der Gefährdungsexposition	A.2.2
FB	Funktionsblock	4.6.3
FVL	Programmiersprache mit nicht eingeschränktem Sprachumfang	3.1.35
FMEA	Ausfallarten und Effekt-Analyse	7.2
I, I1, I2	Eingabegerät, z. B. Sensor	6.2
i, j	Index für Zählung	Anhang D
I/O	Eingänge/Ausgänge	Tabelle E.1
i_{ab}, i_{bc}	Verbindungsmittel	Bild 4
K1A, K1B	Schütze	Anhang I
L, L1, L2	Logik	6.2
LVL	Programmiersprache mit eingeschränktem Sprachumfang	3.1.34
M	Motor	Anhang I
MTTF	mittlere Zeit bis zum Ausfall	Anhang C
$MTTF_d$	mittlere Zeit bis zum gefahrbringenden Ausfall	3.1.25
n, N, \tilde{N}	Anzahl von Einheiten	6.3, D.1
$N_{niedrig}$	Anzahl von SRP/CS mit $PL_{niedrig}$ in einer Kombination von SRP/CS	6.3
O, O1, O2, OTE	Ausgabegerät, z. B. Antriebselement	6.2
P, P1, P2	Möglichkeit zur Vermeidung der Gefährdung	A.2.3
PES	programmierbares elektronisches System	3.1.22

Tabelle 2 (fortgesetzt)

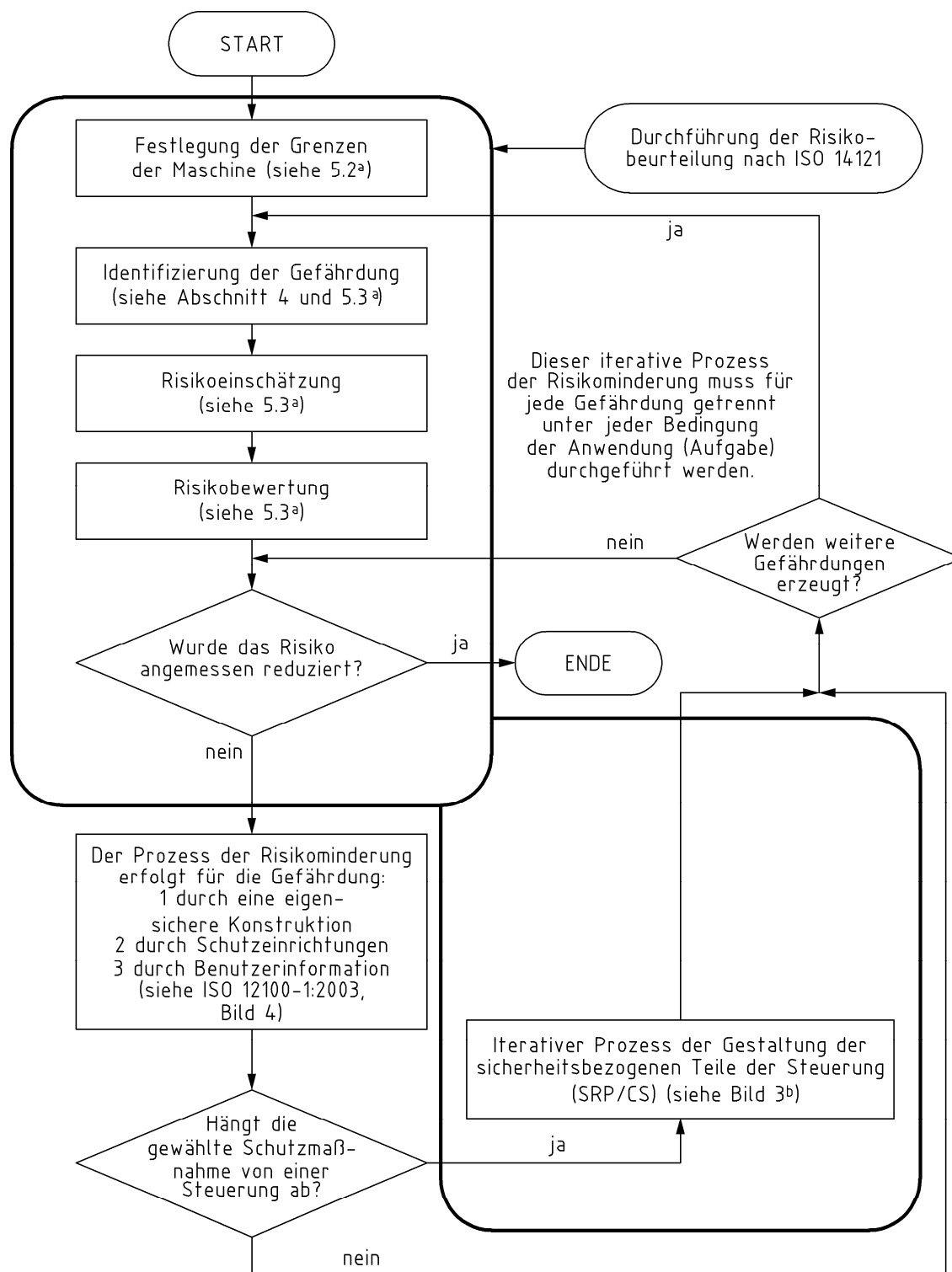
Formelzeichen oder Abkürzung	Beschreibung	Definition oder Fundort
PL	Performance Level	3.1.23
PLC	speicherprogrammierbare Steuerung	Anhang I
PL _{niedrig}	niedrigster Performance Level einer SRP/CS in einer Kombination von SRP/CS	6.3
PL _r	erforderlicher Performance Level	3.1.24
r_d	Anforderungsrate	3.1.30
RS	Drehgeber	Anhang I
S, S1, S2	Schwere der Verletzung	A.2.1
SW1A, SW1B, SW2	Positionschalter	Anhang I
SIL	Sicherheits-Integritätslevel	Tabelle 4
SRASW	sicherheitsbezogene Anwendungssoftware	4.6.3
SRESW	sicherheitsbezogene Embedded-Software	4.6.2
SRP	sicherheitsbezogenes Teil	Allgemein
SRP/CS	sicherheitsbezogenes Teil einer Steuerung	3.1.1
TE	Testeinrichtung	6.2
T_M	Gebrauchsdauer	3.1.28

4 Gestaltungsaspekte

4.1 Sicherheitsziele in der Gestaltung

Das SRP/CS muss so gestaltet und konstruiert werden, dass die Prinzipien der ISO 12100 und ISO 14121 vollständig berücksichtigt werden (siehe Bilder 1 und 3). Alle vorgesehenen Anwendungen und vorhersehbaren Fehlanwendungen müssen betrachtet werden.

EN ISO 13849-1:2008 (D)



a Bezieht sich auf ISO 12100-1:2003

b Bezieht sich auf diesen Teil der ISO 13849

Bild 1 — Übersicht über die Risikobeurteilung/Risikominderung

4.2 Strategie der Risikominderung

4.2.1 Allgemeines

Die Strategie zur Risikominderung an einer Maschine wird in der ISO 12100-1:2003, Abschnitt 5 genannt und weitere Anleitungen in der ISO 12100-2:2003, Abschnitt 4 (inhärent sichere Konstruktion) und Abschnitt 5 (technische Schutzmaßnahmen und ergänzende Schutzmaßnahmen). Diese Strategie deckt den gesamten Lebenszyklus der Maschine ab.

Die Gefährdungsanalyse und der Prozess der Risikoreduzierung an einer Maschine erfordert, dass Gefährdungen durch eine Hierarchie von Maßnahmen beseitigt oder reduziert werden:

- Beseitigung von Gefährdungen oder Risikoreduzierung durch den Entwurf (siehe ISO 12100-2:2003, Abschnitt 4);
- Risikominderung durch Schutzeinrichtungen und mögliche ergänzende Schutzmaßnahmen (siehe ISO 12100-2:2003, Abschnitt 5);
- Risikominderung durch Bereitstellung einer Benutzerinformation über das Restrisiko (siehe ISO 12100-2:2003, Abschnitt 6).

4.2.2 Beitrag der Risikominderung durch das Steuerungssystem

Das Ziel der Befolgung der gesamten Entwurfsprozedur für die Maschine ist es, die Sicherheitsziele zu erreichen (siehe 4.1). Der Entwurf des SRP/CS, um die erforderliche Risikominderung bereitzustellen, ist ein integraler Teil der gesamten Entwurfsprozedur für die Maschine. Das SRP/CS stellt die Sicherheitsfunktion(en) mit einem PL bereit, der die erforderliche Risikominderung erreicht. Durch Bereitstellung von Sicherheitsfunktionen, entweder als ein inhärent sicheres Teil der Konstruktion oder als Steuerung einer Schutzeinrichtung oder nicht trennenden Schutzeinrichtung, ist die Gestaltung des SRP/CS Teil der Strategie der Risikominderung. Dies ist ein iterativer Prozess und wird in Bild 1 und 3 gezeigt.

Die Eigenschaften jeder Sicherheitsfunktion (siehe Abschnitt 5) und der erforderliche Performance Level müssen in der Spezifikation der Sicherheitsanforderungen beschrieben und dokumentiert werden.

In diesem Teil der ISO 13849 werden die Performance Level definiert in Form der Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde. Fünf Performance Level (a bis e) sind festgelegt mit definierten Bereichen der Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (siehe Tabelle 3).

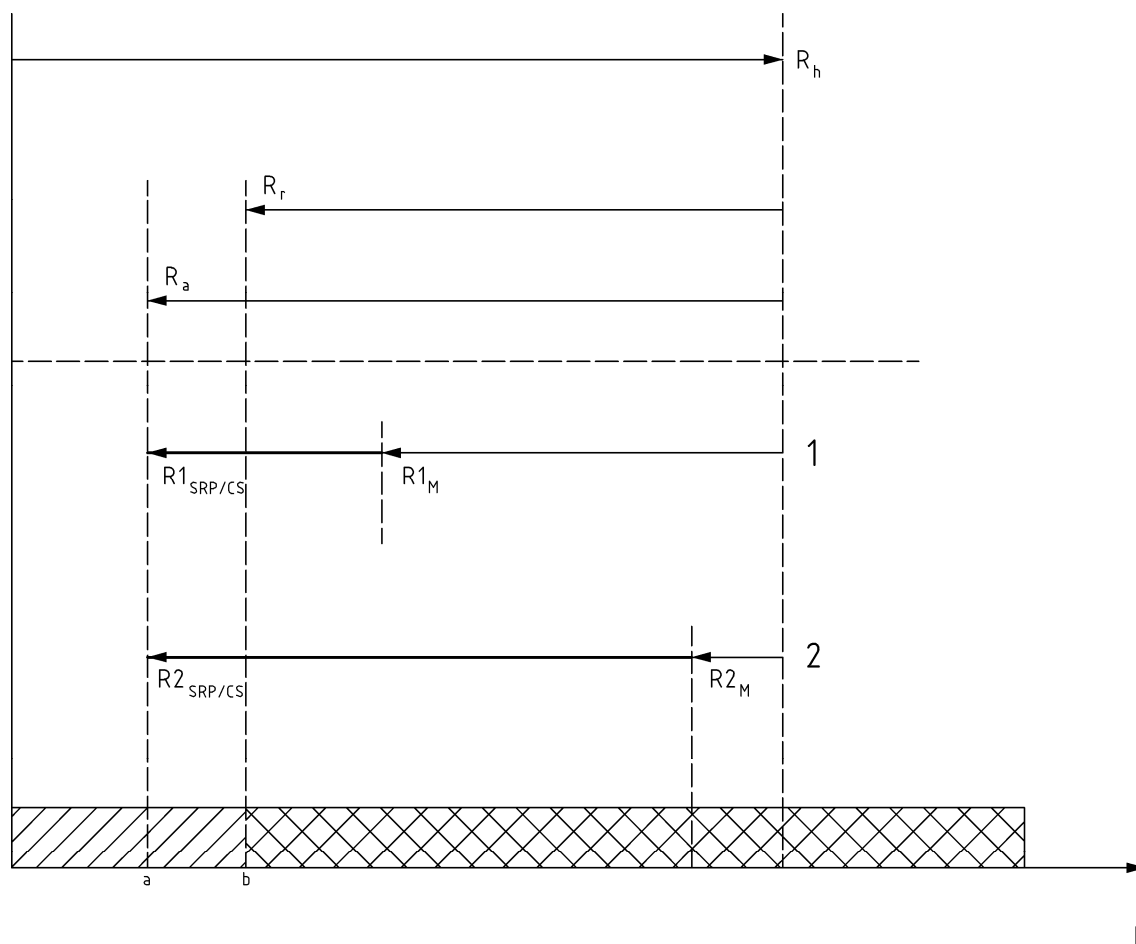
Tabelle 3 — Performance Level (PL)

Performance Level (PL)	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde 1/h
a	$\geq 10^{-5}$ bis $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ bis $< 10^{-5}$
c	$\geq 10^{-6}$ bis $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ bis $< 10^{-6}$
e	$\geq 10^{-8}$ bis $< 10^{-7}$
ANMERKUNG Neben der durchschnittlichen Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde, sind weitere Maßnahmen notwendig, um den PL zu erreichen.	



EN ISO 13849-1:2008 (D)

Nach der Risikobeurteilung (siehe ISO 14121) an der Maschine, muss der Konstrukteur entscheiden, welchen Beitrag der Risikominderung von jeder relevanten Sicherheitsfunktion benötigt wird, die das SRP/CS ausführt. Dieser Beitrag deckt nicht das Gesamtrisiko der betrachteten Maschine ab, z. B. wird nicht das Gesamtrisiko einer mechanischen Presse oder Waschmaschine betrachtet, sondern der Teil des Risikos, der durch die Anwendung spezieller Sicherheitsfunktionen vermindert wird. Beispiele solcher Funktionen sind die Stoppfunktion durch eine berührungslos wirkende Schutteinrichtung an einer Presse oder die Funktion der Türverriegelung einer Waschmaschine.

Die Risikominderung kann erreicht werden durch die Anwendung verschiedener Schutzmaßnahmen (sowohl SRP/CS als auch nicht SRP/CS) mit dem Endergebnis, einen sicheren Zustand zu erreichen (siehe Bild 2).



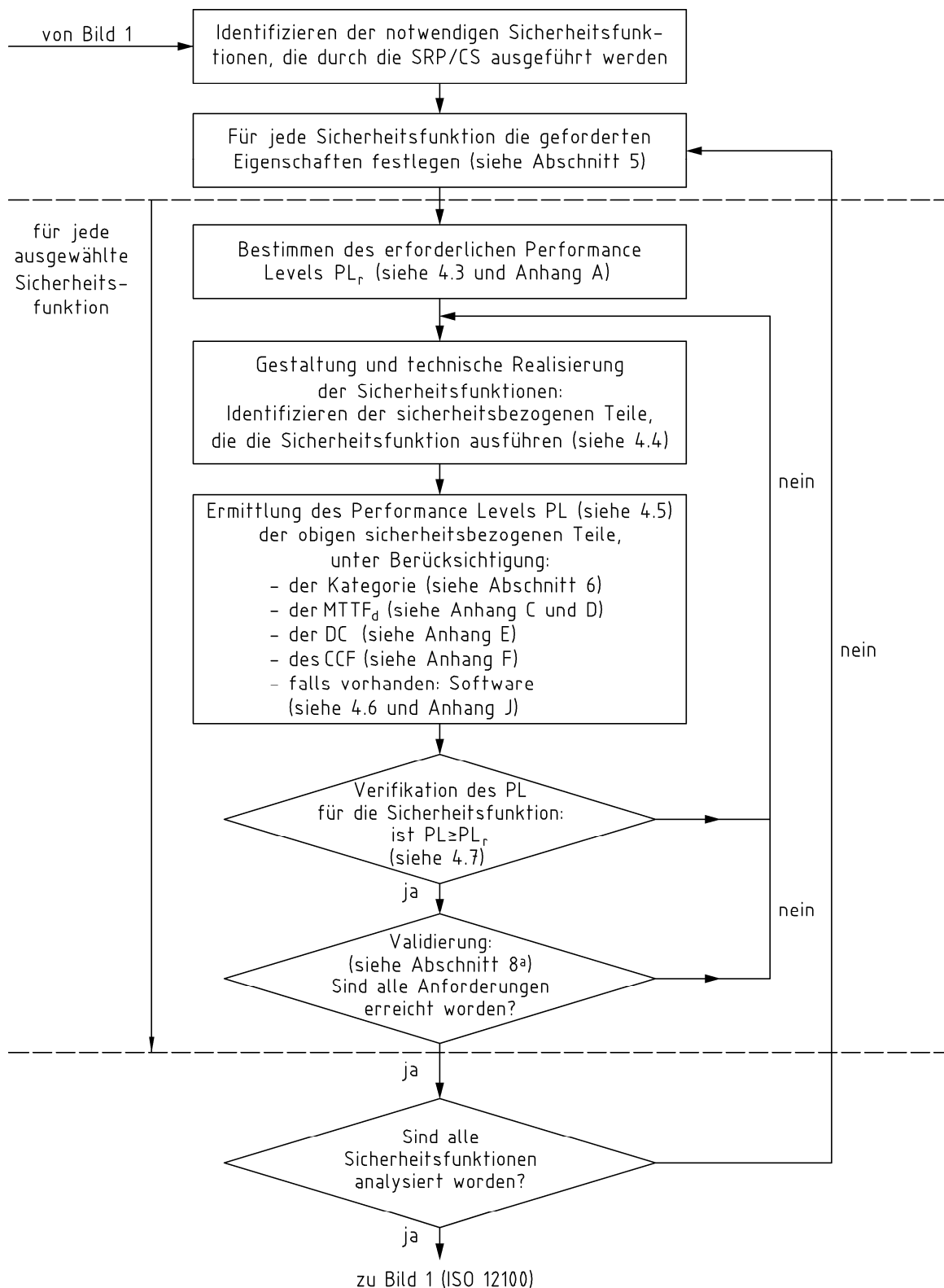
Legende

R_h	Risiko einer speziellen Gefährdungssituation, bevor Schutzmaßnahmen angewendet werden
R_r	geforderte Risikominderung durch Schutzmaßnahmen
R_a	aktuelle, durch Schutzmaßnahmen erreichte Risikominderung
1	Lösung 1 — Ein wesentlicher Teil der Risikominderung erfolgt aufgrund anderer Schutzmaßnahmen als durch ein SRP/CS (z. B. mechanische Maßnahmen), ein kleiner Beitrag der Risikominderung erfolgt durch ein SRP/CS
2	Lösung 2 — Ein wesentlicher Teil der Risikominderung erfolgt aufgrund eines SRP/CS (z. B. Lichtgitter), ein kleiner Beitrag der Risikominderung erfolgt aufgrund anderer Schutzmaßnahmen als durch ein SRP/CS (z. B. mechanische Maßnahmen)
	angemessen vermindertes Risiko
	unzureichend vermindertes Risiko
R	Risiko
a	Restrisiko, das durch die Lösungen 1 und 2 erhalten wird
b	angemessen vermindertes Risiko
$R1_{SRP/CS}, R2_{SRP/CS}$	Risikominderung, die durch die Sicherheitsfunktion des SRP/CS erfolgt
$R1_M, R2_M$	Risikominderung durch andere Schutzmaßnahmen als das SRP/CS (z. B. mechanische Maßnahmen)

ANMERKUNG Für weitere Informationen zur Risikominderung, siehe ISO 12100.

Bild 2 — Übersicht über den Prozess der Risikominderung für jede Gefährdungssituation

EN ISO 13849-1:2008 (D)



a ISO 13849-2 enthält weitere Hilfe zur Validierung.

Bild 3 — Iterativer Prozess zur Gestaltung der sicherheitsbezogenen Teile von Steuerungen (SRP/CS)

4.3 Bestimmung des erforderlichen Performance Levels (PL_r)

Für jede gewählte Sicherheitsfunktion, die durch ein SRP/CS ausgeführt wird, muss ein erforderlicher Performance Level (PL_r) festgelegt und dokumentiert werden (siehe Anhang A). Die Bestimmung des erforderlichen Performance Levels ist das Ergebnis der Risikobeurteilung, bezogen auf den Anteil der Risikominderung durch die sicherheitsbezogenen Teile der Steuerung (siehe Bild 2).

Je größer der Anteil der durch die SRP/CS zu leistenden Risikoreduzierung ist, desto größer muss der erforderliche PL_r sein.

4.4 Entwicklung des SRP/CS

Ein Teil des Prozesses der Risikominderung ist es, die Sicherheitsfunktionen der Maschine zu bestimmen. Dies beinhaltet die Sicherheitsfunktionen der Steuerung, z. B. Verhinderung des unerwarteten Anlaufs.

Eine Sicherheitsfunktion kann durch ein oder mehrere SRP/CS realisiert sein, und mehrere Sicherheitsfunktionen können sich ein oder mehrere SRP/CS teilen [z. B. Logikbaugruppe, Energieübertragungselement(e)]. Es ist aber auch möglich, dass ein SRP/CS Sicherheitsfunktionen und normale Steuerungsfunktionen beinhaltet. Der Konstrukteur kann jede verfügbare Technologie, einzeln oder in Kombination verwenden. Ein SRP/CS kann auch eine Betriebsfunktion bereitstellen (z. B. eine AOPD als Möglichkeit eines zyklischen Starts).

Eine typische Sicherheitsfunktion zeigt Bild 4 als Blockschaltbild, welches eine Kombination sicherheitsbezogener Teile einer Steuerung (SRP/CS) ist, mit:

- Eingang (SRP/CS_a),
- Logik/Bearbeitung (SRP/CS_b),
- Ausgang/Energieübertragungselementen (SRP/CS_c), und
- Verbindungen (i_{ab} , i_{bc}) (z. B. elektrisch, optisch).

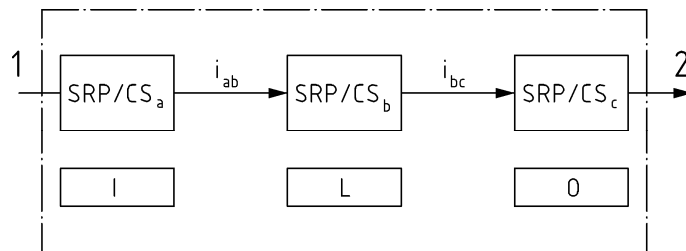
ANMERKUNG 1 Es ist wichtig, innerhalb der gleichen Maschinenanlage zwischen den Sicherheitsfunktionen und deren zugehörigen SRP/CS(en) zu unterscheiden, die eine bestimmte Sicherheitsfunktion ausführen.

Wenn die Sicherheitsfunktionen eines Steuerungssystems bestimmt worden sind, muss der Konstrukteur das SRP/CS bestimmen (siehe Bilder 1 und 3) und muss ihm, wo notwendig, Eingang, Logik und Ausgang zuweisen, im Fall von Redundanz die einzelnen Kanäle festlegen und dann den Performance Level PL bestimmen (siehe Bild 3).

ANMERKUNG 2 Vorgesehene Architekturen werden im Abschnitt 6 angegeben.

ANMERKUNG 3 Alle Verbindungen sind in den sicherheitsbezogenen Teilen enthalten.

EN ISO 13849-1:2008 (D)

**Legende**

I Eingang
L Logik
O Ausgang

- 1 Startereignis, z. B. manuelle Betätigung eines Tasters, Öffnung einer trennenden Schutzeinrichtung, Unterbrechung des Strahls einer AOPD
2 Antriebselement der Maschine, z. B. Bremsen des Motors

Bild 4 — Schematische Darstellung einer Kombination sicherheitsbezogener Teile von Steuerungen zur Verarbeitung einer typischen Sicherheitsfunktion

4.5 Bewertung des erreichten Performance Levels PL und die Beziehung zum SIL

4.5.1 Performance Level PL

Für die Anwendung in diesem Teil der ISO 13849 wird die Fähigkeit sicherheitsbezogener Teile eine Sicherheitsfunktion auszuführen, durch die Bestimmung eines Performance Levels ausgedrückt.

Für jedes gewählte SRP/CS und/oder der Kombination von SRP/CS, die eine Sicherheitsfunktion ausführt, muss eine Abschätzung des PL durchgeführt werden.

Der PL der SRP/CS muss durch die Abschätzung folgender Aspekte bestimmt werden:

- des $MTTF_d$ -Wertes einzelner Bauteile (siehe Anhänge C und D);
- der DC (siehe Anhang E);
- des CCF (siehe Anhang F);
- der Struktur (siehe Abschnitt 6);
- des Verhaltens der Sicherheitsfunktion unter Fehlerbedingung(en) (siehe Abschnitt 6);
- sicherheitsbezogener Software (siehe 4.6 und Anhang J);
- systematischer Ausfälle (siehe Anhang G);
- der Fähigkeit, eine Sicherheitsfunktion unter vorhersehbaren Umgebungsbedingungen auszuführen.

ANMERKUNG 1 Weitere Parameter, z. B. betriebliche Gesichtspunkte, Anforderungsrate, Testrate, können zusätzliche Einflüsse haben.

Diese Aspekte können unter folgenden zwei Ansätzen im Bezug zum Bewertungsprozess zusammengefasst werden:

- a) quantifizierbare Aspekte ($MTTF_d$ -Wert für einzelne Bauteile, DC, CCF, Struktur);
- b) nicht quantifizierbare, qualitative Aspekte, die das Verhalten des SRP/CS beeinflussen (Verhalten der Sicherheitsfunktion unter Fehlerbedingungen, sicherheitsbezogene Software, systematische Ausfälle und Umgebungsbedingungen).

Unter den quantifizierbaren Aspekten kann der Beitrag der Zuverlässigkeit (z. B. MTTF_d, Struktur) mit der verwendeten Technologie variieren. Zum Beispiel ist es möglich (in bestimmten Grenzen), dass ein einzelner Kanal sicherheitsrelevanter Teile hoher Verfügbarkeit in einer Technologie, den gleichen oder höheren PL bereitstellt als eine fehlertolerante Struktur mit niedrigerer Verfügbarkeit in einer anderen Technologie.

Es gibt mehrere Verfahren zur Abschätzung der quantifizierbaren Aspekte des PL für beliebige Systemtypen (z. B. einer komplexen Struktur), z. B. Markov-Modelle, allgemeine stochastische Petrinetze (GSPN), Zuverlässigkeits-Blockdiagramme (siehe z. B. IEC 61508).

Um die Beurteilung der quantifizierbaren Aspekte des PL zu erleichtern, liefert dieser Teil der ISO 13849 ein vereinfachtes Verfahren, basierend auf der Definition von fünf vorgesehenen Architekturen, die spezielle Konstruktionsmerkmale und Verhalten bei einem Fehler erfüllen (siehe 4.5.4).

Für ein SRP/CS oder einer Kombination von SRP/CS, welches nach den in Abschnitt 6 gegebenen Anforderungen entworfen wurde, kann die durchschnittliche Wahrscheinlichkeit eines gefährbringenden Ausfalls mithilfe von Bild 5 und den Verfahren in Anhang A bis H, J und K abgeschätzt werden.

Für ein SRP/CS, das von den vorgesehenen Architekturen abweicht, muss eine ausführliche Berechnung durchgeführt werden, um das Erreichen des erforderlichen Performance Levels (PL_r) nachzuweisen.

In Anwendungen, bei denen das SRP/CS als einfach betrachtet werden kann und der erforderliche Performance Level zwischen a und c liegt, kann eine qualitative Abschätzung des PL in der Entwurfsbeschreibung begründet werden.

ANMERKUNG 2 Für den Entwurf komplexer Steuerungssysteme, wie PES für Sicherheitsfunktionen, kann die Anwendung anderer Normen angemessen sein (z. B. IEC 61508, IEC 62061 oder IEC 61496).

Das Erreichen der qualitativen Aspekte des PL kann durch die Anwendung der empfohlenen Maßnahmen in 4.6 und Anhang G bewiesen werden.

Bei Normen in Übereinstimmung mit IEC 61508 wird die Fähigkeit einer sicherheitsbezogenen Steuerung eine Sicherheitsfunktion auszuführen, durch den SIL angegeben. Tabelle 4 zeigt die Beziehung zwischen den beiden Konzepten (PL und SIL).

Der PL a hat keine Entsprechung auf der SIL-Skala und wird hauptsächlich verwendet, um das Risiko leichter, üblicherweise reversibler, Verletzungen zu reduzieren. Da der SIL 4 möglichen katastrophalen Ereignissen in der Prozessindustrie zugeordnet ist, ist dieses Risiko für Maschinen nicht relevant. So entspricht PL e dem SIL 3 und wird als höchste Stufe definiert.

Tabelle 4 — Beziehung zwischen dem Performance Level (PL) und dem Sicherheits-Integritätslevel (SIL)

PL	SIL (IEC 61508-1, zur Information) hohe/kontinuierliche Betriebsart
a	keine Entsprechung
b	1
c	1
d	2
e	3

EN ISO 13849-1:2008 (D)

Deshalb müssen, um das Risiko zu mindern, Schutzmaßnahmen ergriffen werden, grundsätzlich die Folgenden.

- Reduzierung der Wahrscheinlichkeit eines Fehlers auf Bauteilebene. Das Ziel ist es, die Wahrscheinlichkeit von Fehlern oder Ausfällen, die die Sicherheitsfunktion beeinflussen, zu vermindern. Dies kann erreicht werden durch Erhöhung der Zuverlässigkeit der Bauteile, z. B. durch Auswahl von bewährten Bauteilen und/oder die Anwendung von bewährten Sicherheitsprinzipien, um damit kritische Fehler oder Ausfälle zu minimieren oder auszuschließen (siehe ISO 13849-2).
- Verbesserung der Struktur des SRP/CS. Das Ziel ist es, den gefährlichen Effekt eines Fehlers zu vermeiden. Einige Fehler können erkannt, und eine redundante und/oder überwachte Struktur könnten notwendig werden.

Beide Maßnahmen können separat oder in Kombination angewendet werden. Mit einigen Technologien kann die Risikominderung durch Auswahl zuverlässiger Bauteile und durch Fehlerausschluss erreicht werden, aber mit anderen Technologien könnte zur Risikominderung ein redundantes und/oder überwacht System erforderlich sein. Zusätzlich müssen Ausfälle infolge gemeinsamer Ursache (CCF) mit in Betracht gezogen werden (siehe Bild 3).

Zu Einschränkungen aufgrund der Architektur, siehe Abschnitt 6.

4.5.2 Mittlere Zeit bis zum gefahrbringenden Ausfall jedes Kanals (MTTF_d)

Der Wert der MTTF_d jedes Kanals wird in drei Stufen angegeben (siehe Tabelle 5) und muss für jeden Kanal individuell berücksichtigt werden (z. B. einzelner Kanal oder jeder Kanal eines redundanten Systems).

In Bezug auf die MTTF_d kann ein maximaler Wert von 100 Jahren angesetzt werden.

Tabelle 5 — Mittlere Zeit jedes Kanals bis zum gefahrbringenden Ausfall (MTTF_d)

MTTF _d	
Bezeichnung für jeden Kanal	Bereich für jeden Kanal
niedrig	3 Jahre ≤ MTTF _d < 10 Jahre
mittel	10 Jahre ≤ MTTF _d < 30 Jahre
hoch	30 Jahre ≤ MTTF _d ≤ 100 Jahre
<p>ANMERKUNG 1 Die Wahl der MTTF_d-Bereiche eines Kanals basiert nach dem in der Praxis vorgefundenen Stand der Technik auf einer logarithmischen Skala, die sich der logarithmischen Skala des PL anpasst. Es wird nicht angenommen, dass ein MTTF_d-Wert eines Kanals für ein reales SRP/CS kleiner als drei Jahre gefunden werden kann, denn das würde bedeuten, dass nach einem Jahr etwa 30 % aller Systeme auf dem Markt defekt sind und ersetzt werden müssten. Ein MTTF_d-Wert eines Kanals größer als 100 Jahre wird nicht akzeptiert, denn ein SRP/CS für hohe Risiken sollte nicht von der Zuverlässigkeit von Bauteilen alleine abhängig sein. Um ein SRP/CS gegen systematische und zufällige Fehler zu ertüchtigen, sind zusätzliche Mittel wie Redundanzen und Tests erforderlich. Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf drei beschränkt. Die Beschränkung des MTTF_d-Wertes jedes Kanals auf ein Maximum von 100 Jahren bezieht sich auf den einzelnen Kanal des SRP/CS, der die Sicherheitsfunktion ausführt. Höhere MTTF_d-Werte können für einzelne Bauteile verwendet werden (siehe Tabelle D.1).</p> <p>ANMERKUNG 2 Für die gezeigten Grenzwerte der Tabelle 5 wird eine Genauigkeit von 5 % angenommen.</p>	

Zur Abschätzung der $MTTF_d$ eines Bauteils muss folgendes abgestufte Verfahren in der angegebenen Reihenfolge angewendet werden, um Daten zu finden:

- a) Verwendung von Herstellerdaten;
- b) Verwendung der Verfahren in den Anhängen C und D;
- c) Verwendung eines Wertes von zehn Jahren.

4.5.3 Diagnosedeckungsgrad (DC)

Der Wert für den DC wird in vier Stufen angegeben (siehe Tabelle 6).

Zur Abschätzung des DC kann in den meisten Fällen die Ausfallarten- und Effektanalyse (FMEA — siehe IEC 60812) oder ähnliche Verfahren verwendet werden. In diesem Fall sollten alle relevanten Fehler und/oder Ausfallarten berücksichtigt werden, und der PL der Kombination des SRP/CS, die die Sicherheitsfunktion ausführen sollte, gegen den erforderlichen Performance Level (PL_r) geprüft werden. Für einen vereinfachten Ansatz zur Abschätzung des DC, siehe Anhang E.

Tabelle 6 — Diagnosedeckungsgrad (DC)

Bezeichnung	DC
	Bereich
kein	$DC < 60 \%$
niedrig	$60 \% \leq DC < 90 \%$
mittel	$90 \% \leq DC < 99 \%$
hoch	$99 \% \leq DC$
<p>ANMERKUNG 1 Für ein SRP/CS, das aus mehreren Teilen besteht, wird in dieser Norm in Bild 5, Abschnitt 6 und E.2 ein Durchschnittswert DC_{avg} für den DC verwendet.</p> <p>ANMERKUNG 2 Die Wahl der DC-Bereiche basiert auf den Schlüsselwerten 60 %, 90 % und 99 %, die ebenfalls in anderen Normen, die sich mit Diagnosedeckungsgrad und Tests beschäftigen, eingeführt sind (z. B. IEC 61508). Untersuchungen zeigen, dass (1-DC) eher als DC selbst eine typische Maßeinheit für die Effektivität eines Tests ist. (1-DC) für die Schlüsselwerte 60 %, 90 % und 99 % bildet eine Art logarithmische Skala, die sich der logarithmischen Skala des PL anpasst. Ein DC-Wert kleiner als 60 % hat nur geringen Einfluss auf die Zuverlässigkeit eines getesteten Systems und wird deshalb mit „kein“ bezeichnet. Ein DC-Wert für komplexe Systeme größer als 99 % ist nur sehr schwer zu erreichen. Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.</p>	

4.5.4 Vereinfachtes Verfahren zur Abschätzung eines PL

Der PL kann abgeschätzt werden durch Berücksichtigung aller relevanter Parameter und geeigneter Verfahren für die Berechnung (siehe 4.5.1).

Dieser Abschnitt beschreibt ein vereinfachtes Verfahren, um den PL eines SRP/CS auf der Basis vorgesehener Architekturen abzuschätzen. Einige andere Architekturen mit ähnlichen Strukturen können in diese vorgesehenen Architekturen umgewandelt werden, um eine Abschätzung des PL zu ermöglichen.

Die vorgesehenen Architekturen werden als Blockschaltbilder dargestellt und sind in 6.2 für jede Kategorie aufgelistet. Informationen über das Blockverfahren und die sicherheitsbezogenen Blockdiagramme werden in 6.2 und Anhang B gegeben.

EN ISO 13849-1:2008 (D)

Die vorgesehenen Architekturen zeigen die logische Darstellung der Systemstruktur für jede Kategorie. Die technische Realisierung, z. B. der funktionale Schaltplan, kann komplett anders aussehen.

Die vorgesehenen Architekturen sind für die zusammengefassten SRP/CS gezeichnet, beginnend an dem Punkt an dem die sicherheitsbezogenen Signale erzeugt werden und endend am Ausgang der Energieübertragungselemente (siehe auch ISO 12100-1:2003, Anhang A). Die vorgesehenen Architekturen können auch verwendet werden, um einen Teil des Steuerungssystems zu beschreiben, das auf Eingangssignale reagiert und sicherheitsbezogene Ausgangssignale erzeugt. Deshalb kann das „Eingangselement“ z. B. einen Lichtvorhang (AOPD) ebenso abbilden, wie Eingangsschaltungen von Elementen einer Steuerungslogik oder Eingangsschalter. „Ausgang“ kann ebenso z. B. ein Ausgangsschaltelement (OSSD) oder die Ausgänge eines Laserscanners darstellen.

Für vorgesehene Architekturen werden folgende typische Annahmen getroffen:

- Gebrauchsdauer, 20 Jahre (siehe Abschnitt 10);
- konstante Ausfallraten innerhalb der Gebrauchsdauer;
- für Kategorie 2, Anforderungsrate $\leq 1/100$ der Testrate;
- für Kategorie 2, $MTTF_{d,TE}$ größer als die Hälfte der $MTTF_{d,L}$.

ANMERKUNG Wenn Blöcke eines jeden Kanals nicht aufgeteilt werden können, kann folgendes angewendet werden: $MTTF_d$ des zusammengefassten Testkanals (TE, OTE) größer als die halbe $MTTF_d$ des zusammengefassten Funktionskanals (I, L, O).

Die Methodik berücksichtigt die Kategorien als Architekturen mit definiertem DC_{avg} . Der PL jedes SRP/CS hängt ab von der Architektur, der mittleren Zeit bis zum Ausfall ($MTTF_d$) jedes Kanals und des DC_{avg} .

Ausfälle aufgrund gemeinsamer Ursachen (CCF) sollten ebenfalls berücksichtigt werden (siehe Anhang F).

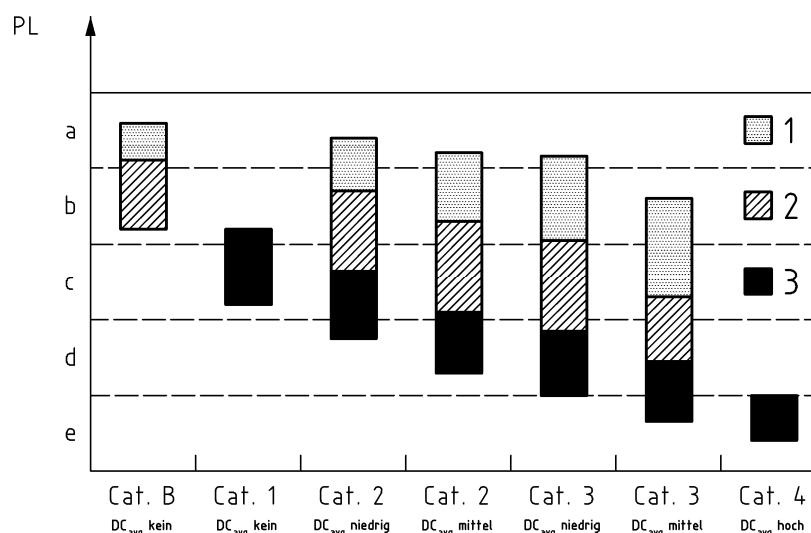
Für SRP/CS mit Software sind die Anforderungen aus 4.6 anzuwenden.

Wenn keine quantitativen Daten verfügbar sind oder verwendet werden (z. B. bei Systemen niedriger Komplexität) sollte der ungünstigste Fall (Worst Case) für alle relevanten Parameter gewählt werden.

Eine Kombination von SRP/CS oder ein einzelnes SRP/CS kann einen PL haben. Die Kombination mehrerer SRP/CS mit unterschiedlichen PL werden in 6.3 betrachtet.

Bei Applikationen mit einem PL_r a bis c können Maßnahmen zur Fehlervermeidung ausreichen; bei Anwendungen mit höherem Risiko PL_r d bis e, kann die Struktur des SRP/CS die Maßnahmen bereitstellen, die Fehler zu vermeiden, zu bemerken oder zu tolerieren. Geeignete Maßnahmen beinhalten Redundanz, Diversität, Überwachung (siehe auch ISO 12100-2:2003, Abschnitt 3 und IEC 60204-1:2000).

Bild 5 zeigt das Verfahren zur Auswahl der Kategorien in Kombination mit $MTTF_d$ für jeden Kanal und der DC_{avg} , um den erforderlichen PL für jede Sicherheitsfunktion zu erreichen.



Legende

- PL Performance Level
- 1 MTTF_d jedes Kanals = niedrig
- 2 MTTF_d jedes Kanals = mittel
- 3 MTTF_d jedes Kanals = hoch

Bild 5 — Beziehung zwischen den Kategorien DC_{avg} , MTTF_d jedes Kanals und PL

Bild 5 zeigt die unterschiedlichen möglichen Kombinationen zur Abschätzung der Kategorie mit DC_{avg} (horizontale Achse) und der MTTF_d jedes Kanals (Balken). Die Balken im Diagramm zeigen die drei MTTF_d-Bereiche jedes Kanals (niedrig, mittel und hoch), die gewählt werden können, um den erforderlichen PL zu erreichen.

Bevor das vereinfachte Verfahren aus Bild 5 angewendet wird (das die Ergebnisse verschiedener Markov-Modelle auf der Basis vorgesehener Architekturen aus Abschnitt 6 zeigt), muss die Kategorie des SRP/CS ebenso wie DC_{avg} und die MTTF_d jedes Kanals bestimmt worden sein (siehe Abschnitt 6 und Anhang C bis E).

Bei den Kategorien 2, 3 und 4 müssen ausreichende Maßnahmen gegen Ausfälle aufgrund gemeinsamer Ausfälle erfüllt werden (siehe Anhang F). Diese Parameter in Betracht ziehend, liefert das Bild 5 ein grafisches Verfahren zur Bestimmung des PL der durch das SRP/CS erreicht wird. Die Kombination von Kategorie (einschließlich Ausfälle aufgrund gemeinsamer Ausfälle) und DC_{avg} bestimmt, welche Spalte in Bild 5 zu wählen ist. Entsprechend der MTTF_d jedes Kanals muss einer der drei unterschiedlich schraffierten Bereiche der zutreffenden Spalte gewählt werden.

Die vertikale Position dieser Bereiche legt den erreichten PL fest, der an der vertikalen Achse abgelesen werden kann. Wenn der Bereich zwei oder drei mögliche PL abdeckt, wird der erreichte PL in Tabelle 7 angegeben. Für eine exakte Auswahl des PL auf der Basis des genauen Wertes der MTTF_d jedes Kanals, siehe Anhang K.

EN ISO 13849-1:2008 (D)

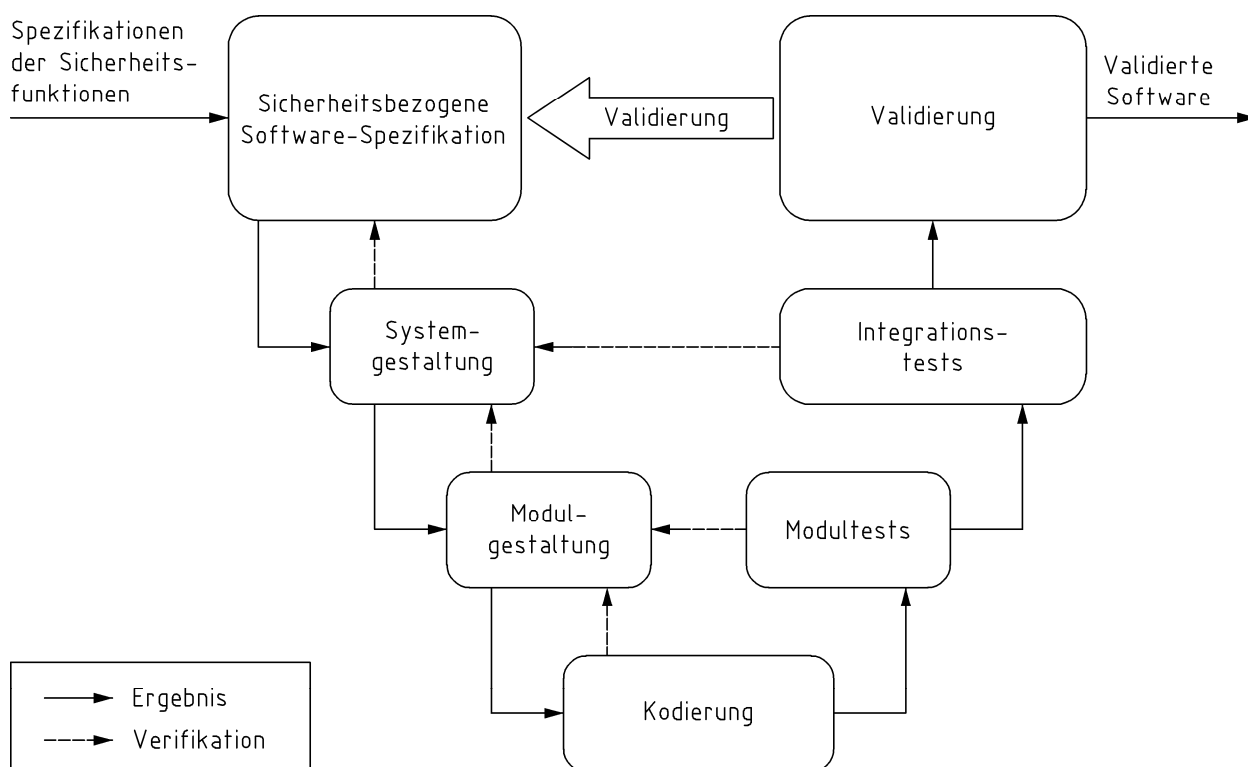
Tabelle 7 — Vereinfachtes Verfahren zur Bewertung des durch ein SRP/CS erreichten PL

Kategorie	B	1	2	2	3	3	4
DC _{avg}	kein	kein	niedrig	mittel	niedrig	mittel	hoch
MTTF _d jedes Kanals							
niedrig	a	nicht abgedeckt	a	b	b	c	nicht abgedeckt
mittel	b	nicht abgedeckt	b	c	c	d	nicht abgedeckt
hoch	Nicht abgedeckt	c	c	d	d	d	e

4.6 Software-Sicherheitsanforderungen

4.6.1 Allgemeines

Alle Tätigkeiten im Lebenszyklus von sicherheitsbezogener Embedded- oder Anwendungssoftware müssen hauptsächlich die Vermeidung von Fehlern berücksichtigen, die während des Softwarelebenszyklus (siehe Bild 6) eingebracht werden. Das Hauptziel der folgenden Anforderungen ist es, lesbare, verständliche, testbare und wartbare Software zu erhalten.



ANMERKUNG Anhang J zeigt detailliertere Tätigkeiten des Lebenszyklus.

Bild 6 — Vereinfachtes V-Modell des Softwarelebenszyklus

4.6.2 Sicherheitsbezogene Embedded-Software (SRESW)

Für SRESW in Bauteilen mit einem PL_r von a bis d müssen die folgenden Basismaßnahmen angewendet werden:

- Software-Sicherheitslebenszyklus mit Verifikation und Validierung, siehe Bild 6;
- Dokumentation der Spezifikation und Entwurf;
- modulare und strukturierte Entwicklung und Codierung;
- Beherrschung von systematischen Ausfällen (siehe G.2);
- bei Verwendung softwarebasierter Maßnahmen zur Beherrschung von zufälligen Hardwareausfällen, Verifikation der korrekten Implementierung;
- funktionale Tests, z. B. Black-Box-Tests;
- geeignete Aktivitäten für den Software-Sicherheitslebenszyklus nach Änderungen.

Für SRESW in Bauteilen mit einem PL_r von c oder d müssen die folgenden zusätzlichen Maßnahmen angewendet werden:

- Projektmanagement- und Qualitätsmanagementsystem vergleichbar mit z. B. der Reihe IEC 61508 oder ISO 9001;
- Dokumentation aller relevanter Aktivitäten während des Software-Sicherheitslebenszyklus;
- Konfigurationsmanagement, um alle Konfigurationsmerkmale und Dokumente mit Bezug zu einer SRESW-Freigabe festzustellen;
- strukturierte Spezifikation mit Sicherheitsanforderungen und Entwicklung;
- Verwendung geeigneter Programmiersprachen und rechnergestützter Werkzeuge mit Betriebsbewährung;
- modulare und strukturierte Programmierung, Abgrenzung in nicht sicherheitsbezogene Software, beschränkte Modulgröße mit vollständig definierten Schnittstellen, Verwendung von Entwurfs- und Codierungsrichtlinien;
- Verifikation des Codes durch ein Walk-Through-Review (Überprüfung) mit einer Kontrollflussanalyse;
- erweiterte Funktionstests, z. B. Grey-Box-Tests, Leistungstests oder Simulation;
- Einflussanalyse und angemessene Software-Sicherheitslebenszyklus-Aktivitäten nach Änderungen.

SRESW für Bauteile mit $PL_r = e$ muss mit den Anforderungen der IEC 61508-3:1998, Abschnitt 7, geeignet für SIL 3, übereinstimmen. Wenn Diversität in Spezifikation, Entwurf und Codierung für die beiden Kanäle des SRP/CS in Kategorie 3 oder 4 verwendet wird, kann ein $PL_r = e$ mit den oben erwähnten Maßnahmen für PL_r von c oder d erreicht werden.

ANMERKUNG 1 Für eine genaue Beschreibung solcher Maßnahmen, siehe z. B. IEC 61508-7:2000.

ANMERKUNG 2 Für SRESW mit Diversität in Entwurf und Codierung für Bauteile von SRP/CS in Kategorie 3 oder 4 kann der Aufwand, um systematische Ausfälle zu vermeiden, vermindert werden durch z. B. Überprüfung von Teilen der Software nur durch Berücksichtigung der strukturellen Aspekte, statt durch prüfen jeder Codezeile.

EN ISO 13849-1:2008 (D)**4.6.3 Sicherheitsbezogene Anwendungssoftware (SRASW)**

Der Softwarelebenszyklus (siehe Bild 6) gilt auch bei SRASW (siehe Anhang J).

SRASW, in LVL geschrieben und mit den folgenden Anforderungen übereinstimmend, kann einen PL von a bis e erreichen. Wenn SRASW in FVL geschrieben ist, müssen die Anforderungen für SRESW angewendet werden, und der erreichbare PL ist a bis e. Wenn ein Teil der SRASW innerhalb eines Bauteils irgendeinen Einfluss (z. B. bei Modifikation) auf verschiedene Funktionen mit unterschiedlichen PL hat, dann müssen die Anforderungen des zugehörigen höchsten PL angewendet werden. Bei SRASW für Bauteile mit einem PL_r von a bis e müssen die folgenden Basismaßnahmen angewendet werden:

- Entwicklungslebenszyklus mit Verifikation und Validierung, siehe Bild 6;
- Dokumentation der Spezifikation und Entwurf;
- modulare und strukturierte Programmierung;
- funktionale Tests;
- geeignete Entwicklungsaktivitäten nach Änderungen.

Für SRASW in Komponenten mit PL_r von c bis e werden die folgenden zusätzlichen Maßnahmen mit steigender Wirksamkeit (niedrigere Wirksamkeit für PL_r von c, mittlere Wirksamkeit für PL_r von d, höhere Wirksamkeit für PL_r von e) erforderlich oder empfohlen.

- a) Die Spezifikation der sicherheitsbezogenen Software muss überprüft werden (siehe auch Anhang J) und jeder Person, die am Lebenszyklus beteiligt ist, verfügbar sein und muss die Beschreibung enthalten von:
 - 1) Sicherheitsfunktionen mit erforderlichem PL und zugehörigen Betriebsarten,
 - 2) Leistungskriterien, z. B. Reaktionszeiten,
 - 3) Hardwarearchitektur mit externen Signalschnittstellen und
 - 4) Erkennung und Beherrschung externer Ausfälle.
- b) Auswahl der Werkzeuge, Bibliotheken, Sprachen:
 - 1) Geeignete Werkzeuge mit Betriebsbewährung: Für PL = e, der mit einer Komponente und deren Werkzeug erreicht wird, muss das Werkzeug mit einer geeigneten Sicherheitsnorm übereinstimmen; wenn zwei diversitäre Komponenten mit diversitären Werkzeugen verwendet werden, kann Betriebsbewährung ausreichend sein. Technische Fähigkeiten, die Bedingungen erkennen können, die zu systematischen Fehlern führen könnten (wie z. B. Datentyp-Unverträglichkeit, mehrdeutige dynamische Speicherzuordnung, unvollständiger Aufruf von Schnittstellen, Rekursion, Zeigerarithmetik), müssen verwendet werden. Prüfungen sollten hauptsächlich während der Kompilierung durchgeführt werden und nicht nur während der Laufzeit. Werkzeuge sollten Sprachenteilmengen und Programmierrichtlinien erzwingen oder mindestens den Entwickler leiten oder führen.
 - 2) Wann immer angemessen durchführbar, sollten validierte Funktionsblock-Bibliotheken (FB) verwendet werden — entweder vom Werkzeughersteller gelieferte sicherheitsbezogene FB-Bibliotheken (besonders empfohlen für PL = e) oder validierte anwendungsspezifische FB-Bibliotheken in Übereinstimmung mit diesem Teil der ISO 13849.
 - 3) Eine begründete LVL-Teilmenge, geeignet für ein modulares Verfahren sollte verwendet werden, z. B. eine anerkannte Teilmenge der IEC 61131-3-Sprachen. Grafische Sprachen (z. B. Funktionsbaustein-Sprache, Kontaktplan) sind besonders empfohlen.

c) Der Softwareentwurf muss folgende Merkmale haben:

- 1) Semiformale Verfahren, um den Daten- und Kontrollfluss zu beschreiben, z. B. Zustandsdiagramm oder Programmflussdiagramm.
- 2) Modulare und strukturierte Programmierung, überwiegend realisiert durch die Bereitstellung validierter sicherheitsbezogener Funktionsblock-Bibliotheken.
- 3) Funktionsblöcke mit minimierter Codelänge.
- 4) Innerhalb des Funktionsblocks sollte die Ausführung des Codes mit einem Eingangssprung und einem Ausgangssprung erfolgen.
- 5) Architektur des Modells in drei Stufen: Eingänge \Rightarrow Verarbeitung \Rightarrow Ausgänge (siehe Bild 7 und Anhang J).
- 6) Zuordnung des Sicherheitsausgangs zu nur einem Programmteil.
- 7) Verwendung von Methoden zur Detektion externer Ausfälle und zur defensiven Programmierung innerhalb von Eingangs-, Verarbeitungs- und Ausgangsblöcken, die zum sicheren Zustand führen.

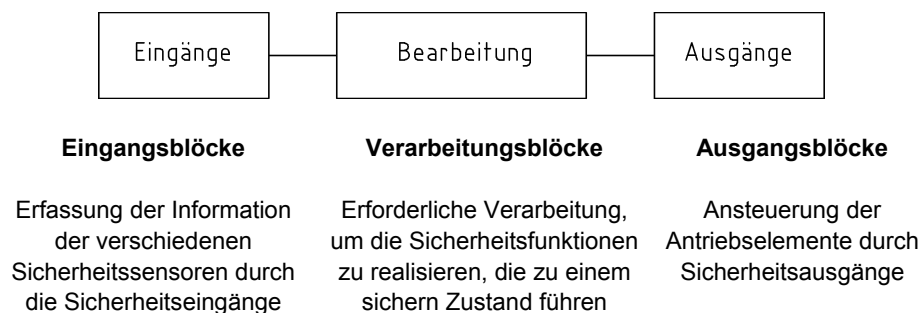


Bild 7 — Allgemeines Architekturmodell für Software

d) Wo SRASW und nicht sicherheitsrelevante Software in einer Komponente kombiniert werden:

- 1) SRASW und nicht sicherheitsrelevante Software müssen in unterschiedlichen Funktionsblöcken codiert werden, mit sorgfältig definierten Datenschnittstellen.
- 2) Es darf keine logische Verknüpfung von nicht sicherheitsbezogenen und sicherheitsbezogenen Daten geben, die zur Herabstufung der Integrität der sicherheitsbezogenen Signale führen könnten, z. B. Verknüpfen eines sicherheitsbezogenen und eines nichtsicherheitsbezogenen Signals durch ein logisches „ODER“, dessen Ausgang sicherheitsbezogene Signale steuert.

e) Softwareimplementierung/Codierung:

- 1) Der Code muss lesbar, verständlich und testbar sein, und aufgrund dessen sollten symbolische Variablen (anstelle expliziter Hardwareadressen) angewendet werden.
- 2) Begründete oder akzeptierte Programmierrichtlinien müssen verwendet werden (siehe auch Anhang J).
- 3) Datenintegritäts- und Plausibilitätsprüfungen (z. B. Bereichsüberprüfungen) auf Anwendungsebene (defensive Programmierung), sollten verwendet werden.
- 4) Der Code sollte durch Simulation getestet werden.
- 5) Die Verifikation sollte durch Kontroll- und Datenflussanalyse bei PL = d oder e erfolgen.

EN ISO 13849-1:2008 (D)

f) Testen:

- 1) Das angemessene Validierungsverfahren ist der Black-Box-Test des funktionellen Verhaltens und der Leistungskriterien (z. B. zeitliches Leistungsverhalten).
- 2) Für PL = d oder e wird eine Testfallausführung auf der Basis von Grenzwertanalysen empfohlen.
- 3) Eine Testplanung wird empfohlen und sollte Testfälle mit Abschlussbedingungen und erforderlichen Werkzeugen enthalten.
- 4) I/O-Tests müssen sicherstellen, dass die sicherheitsbezogenen Signale in der SRASW korrekt verwendet werden.

g) Dokumentation:

- 1) Alle Lebenszyklus- und Änderungsaktivitäten müssen dokumentiert werden.
- 2) Die Dokumentation muss vollständig, verfügbar, lesbar und verständlich sein.
- 3) Die Codedokumentation innerhalb des Quelltextes muss Modulköpfe enthalten mit einer juristischen Person, Funktions- und I/O-Beschreibung, Version der verwendeten Funktionsblock-Bibliothek und ausreichende Kommentierung der Netzwerke/Anweisungen und Deklarationszeilen.

h) Verifikation²⁾:

BEISPIEL Überprüfung, Inspektion, Walk-Through oder andere geeignete Aktivitäten.

i) Konfigurationsmanagement:

Die Einführung von Verfahren und Datensicherung wird besonders empfohlen, um alle Dokumente, Softwaremodule, Ergebnisse der Verifikation/Validierung und Werkzeugkonfiguration, die im Bezug zu einer bestimmten SRASW stehen, zu identifizieren und zu archivieren.

j) Änderungen:

Nach Änderungen einer SRASW muss eine Einflussanalyse zur Sicherstellung der Spezifikation durchgeführt werden. Nach Änderungen müssen angemessene Lebenszyklusaktivitäten stattfinden. Zugriffsrechte auf die Änderungen müssen geprüft und die Änderungshistorie muss dokumentiert werden.

ANMERKUNG Änderung betrifft nicht Systeme, die bereits in Betrieb sind.

4.6.4 Softwarebasierende Parametrisierung

Softwarebasierende Parametrisierung sicherheitsbezogener Parameter muss als ein sicherheitsbezogener Aspekt des SRP/CS-Entwurfs betrachtet werden, der in der Spezifikation der Software-Sicherheitsanforderungen beschrieben wird. Die Parametrisierung muss unter Verwendung eines geeigneten Softwarewerkzeugs ausgeführt werden, das vom Lieferanten der SRP/CS bereitgestellt wird. Dieses Werkzeug muss eine eigene Kennzeichnung besitzen (Name, Version usw., und muss unbefugte Modifikation verhindern, z. B. durch Verwendung eines Passwortes.

Die Integrität aller für die Parametrisierung verwendeten Daten muss aufrechterhalten bleiben. Dies muss durch Anwendung folgender Maßnahmen erreicht werden:

— Kontrolle des Bereiches gültiger Eingaben;

2) Eine Verifikation ist nur für einen anwendungsspezifischen Code notwendig und nicht für validierte Bibliotheksfunktionen.

- Beherrschung von Datenverfälschungen vor der Datenübertragung;
- Beherrschung der Auswirkungen von Abweichungen beim Prozess der Parameterübertragung;
- Beherrschung der Auswirkungen beim Übertragen unvollständiger Parameter; und
- Beherrschung der Auswirkungen von Fehlern und Ausfällen der Hardware und Software des für die Parametrisierung verwendeten Werkzeugs.

Das für die Parametrisierung verwendete Werkzeug muss alle Anforderungen an SRP/CS entsprechend dieses Teils der ISO 13849 erfüllen. Alternativ muss ein spezielles Verfahren für die Einstellung der sicherheitsbezogenen Parameter verwendet werden. Dieses Verfahren muss die Bestätigung von Eingabeparametern für das SRP/CS einschließen, entweder durch

- Rückübertragung der modifizierten Parameter zum Parametrisierungswerkzeug, oder
- andere geeignete Mittel zur Bestätigung der Integrität der Parameter,

als auch nachfolgende Bestätigung, z. B. durch eine ausreichend geschulte Person und eine automatische Überprüfung durch ein Parametrisierungswerkzeug.

ANMERKUNG 1 Dies ist von besonderer Wichtigkeit, wenn die Parametrisierung unter Verwendung eines Gerätes ausgeführt wird, das nicht speziell für den Zweck vorgesehen ist (z. B. Personalcomputer oder Ähnliches).

Die Softwaremodule, die für Codierung/Decodierung innerhalb des Übertragungs-/Rückübertragungsprozesses verwendet werden, und die Softwaremodule, die für die Anzeige von sicherheitsbezogenen Parametern für den Anwender verwendet werden, müssen mindestens Diversität für die Funktion(en) verwenden, um systematische Ausfälle zu verhindern.

Die Dokumentation einer softwarebasierenden Parametrisierung muss die verwendeten Daten (z. B. vordefinierte Parametersätze) und notwendige Informationen zur Identifikation der dem SRP/CS zugeordneten Parameter, der Person(en), die die Parametrisierung ausgeführt hat (haben) zusammen mit anderen relevanten Informationen, wie Datum der Parametrisierung, aufzeigen.

Die folgenden Verifikationsaktivitäten müssen für eine softwarebasierende Parametrisierung angewendet werden:

- Verifikation der korrekten Einstellung für jeden sicherheitsbezogenen Parameter (Minimum-, Maximum- und repräsentative Werte);
- Verifikation, dass die sicherheitsbezogenen Parameter auf Plausibilität überprüft werden, z. B. durch Eingabe ungültiger Werte usw.;
- Verifikation, dass unbefugte Modifikation von sicherheitsbezogenen Parametern verhindert ist;
- Verifikation, dass die Daten/Signale einer Parametrisierung so erzeugt und verarbeitet werden, dass Fehler nicht zu einem Verlust der Sicherheitsfunktion führen können.

ANMERKUNG 2 Dies ist von besonderer Wichtigkeit, wenn die Parametrisierung unter Verwendung eines Geräts ausgeführt wird, das nicht speziell für diesen Zweck vorgesehen ist (z. B. Personalcomputer oder Ähnliches).

4.7 Verifikation, dass der erreichte PL den PL_r erfüllt

Für jede einzelne Sicherheitsfunktion muss der PL des zugehörigen SRP/CS dem nach 4.3 bestimmten erforderlichen Performance Level (PL_r) entsprechen (siehe Bild 3). Wenn das nicht der Fall ist, wird eine Wiederholung des Prozesses, wie in Bild 3 beschrieben, notwendig.

EN ISO 13849-1:2008 (D)

Die PLs verschiedener SRP/CS, die Teil einer Sicherheitsfunktion sind, müssen größer oder gleich dem erforderlichen Performance Level (PL_r) dieser Funktion sein.

4.8 Ergonomische Aspekte der Gestaltung

Die Schnittstelle zwischen Benutzer und den SRP/CS(en) muss so gestaltet und realisiert werden, dass keine Person während jeder geplanten Verwendung und vernünftigerweise vorhersehbaren Fehlanwendung der Maschine gefährdet wird (siehe auch ISO 12100-2, EN 614-1, ISO 9355-1, ISO 9355-2, ISO 9355-3, EN 1005-3, IEC 60204-1:2000, Abschnitt 10, IEC 60447 und IEC 61310).

Es müssen ergonomische Prinzipien verwendet werden, sodass die Maschine und die Steuerung, einschließlich der sicherheitsbezogenen Teile, einfach zu verwenden ist und der Benutzer nicht verleitet wird, in einer gefährlichen Weise zu handeln.

Die Sicherheitsanforderungen zur Erfüllung ergonomischer Prinzipien der ISO 12100-2:2003, 4.8 werden angewendet.

5 Sicherheitsfunktionen**5.1 Spezifikation der Sicherheitsfunktionen**

Dieser Abschnitt stellt eine Liste und Einzelheiten von Sicherheitsfunktionen zur Verfügung, die durch SRP/CS bereitgestellt werden können. Der Konstrukteur (oder Typ-C-Normensetzer) muss die Notwendigen einbeziehen, um die von der Steuerung auszuführenden Sicherheitsmaßnahmen für die spezielle Anwendung zu verwirklichen.

BEISPIEL Sicherheitsbezogene Stoppfunktion, Verhinderung des unerwarteten Anlaufes, manuelle Rücksetzfunktion, Mutingfunktion, Einrichtung mit selbsttätiger Rückstellung.

ANMERKUNG Maschinensteuerungen stellen Betriebs- und/oder Sicherheitsfunktionen bereit. Betriebsfunktionen (z. B. Start, normaler Stopp) können auch Sicherheitsfunktionen sein, aber dies kann erst nach einer vollständigen Risikobeurteilung an der Maschine ermittelt werden.

Die Tabellen 8 und 9 zählen einige typische Sicherheitsfunktionen und einige ihrer jeweiligen Eigenschaften und sicherheitsbezogener Parameter auf, indem sie auf andere Internationale Normen verweist, deren Anforderungen sich auf die Sicherheitsfunktion, Eigenschaft oder Parameter beziehen. Der Konstrukteur (oder Typ-C-Normensetzer) muss sicherstellen, dass alle anwendbaren Anforderungen nach den Tabellen 8 und 9 für die entsprechenden in den Tabellen aufgelisteten Sicherheitsfunktionen erfüllt werden.

In diesem Abschnitt werden zusätzliche Anforderungen an bestimmte Eigenschaften der Sicherheitsfunktion festgelegt.

Wo notwendig, müssen die Anforderungen für Eigenschaften und Sicherheitsfunktionen an die Verwendung mit unterschiedlichen Energiequellen angepasst werden.

Da sich die meisten Verweisungen in den Tabellen 8 und 9 auf Elektronormen beziehen, bedürfen die zutreffenden Anforderungen ein Angleichen an andere Technologien (z. B. Hydraulik, Pneumatik).

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 12100-1:2003	ISO 12100-2:2003	
Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrich- tung ^a	5.2.1	3.26.8	4.11.3	IEC 60204-1:2005, 9.2.2, 9.2.5.3, 9.2.5.5
Manuelle Rückstell- funktion	5.2.2	—	—	IEC 60204-1:2005, 9.2.5.3, 9.2.5.4
Start-/Wiederanlauf- funktion	5.2.3	—	4.11.3, 4.11.4	IEC 60204-1:2005, 9.2.1, 9.2.5.1, 9.2.5.2, 9.2.6
Lokale Steuerungs- funktion	5.2.4	—	4.11.8, 4.11.10	IEC 60204-1:2005, 10.1.5
Mutingfunktion	5.2.5	—	—	—
Einrichtung mit selbst- tätiger Rückstellung (Tippschalter)	—	—	4.11.8 b)	IEC 60204-1:2005, 9.2.6.1
Zustimmfunktion	—	—	—	IEC 60204-1:2005, 9.2.6.3, 10.9
Verhinderung des unerwarteten Anlaufs	—	—	4.11.4	ISO 14118, IEC 60204-1:2005, 5.4
Befreiung und Rettung eingeschlossener Personen	—	—	5.5.3	—
Isolations- und Energie- ableitungsfunktion	—	—	5.5.4	ISO 14118, IEC 60204-1:2005, 5.3, 6.3.1
Steuerungsfunktionen und Betriebsartenwahl	—	—	4.11.8, 4.11.10	IEC 60204-1: 2005, 9.2.3, 9.2.4
Beeinflussung zwischen verschiedenen sicher- heitsbezogenen Teilen der Steuerungen	—	—	4.11.1 (letzter Satz)	IEC 60204-1:2005, 9.3.4
Überwachung der Parametrisierung der sicherheitsbezogenen Eingangswerte	4.6.4	—	—	—
Funktion zum Stillsetzen im Notfall ^b	—	—	5.5.2	ISO/IEC 13850, IEC 60204-1:2005, 9.2.5.4
^a Einschließlich Verriegelungseinrichtung und Grenzwertüberwachung (z. B. Höchstdrehzahl, Übertemperatur, Überdruck)				
^b Ergänzende Schutzmaßnahme, siehe ISO 12100-1:2003				

EN ISO 13849-1:2008 (D)**Tabelle 9 — Einige Internationale Normen, die Anforderungen für bestimmte Sicherheitsfunktionen und sicherheitsbezogene Parameter geben**

Sicherheitsfunktion/ sicherheitsbezogener Parameter	Anforderung		Für weitere Informationen, siehe:
	ISO 13849-1	ISO 12100-2:2003	
Ansprechzeit	5.2.6	—	ISO 13855:2002, 3.2, A.3, A.4
Sicherheitsbezogene Parameter (z. B. Geschwindigkeit Temperatur, Druck)	5.2.7	4.11.8 e)	IEC 60204-1:2005, 7.1, 9.3.2, 9.3.4
Schwankungen, Verlust und Wiederkehr der Spannungsversorgung	5.2.8	4.11.8 e)	IEC 60204-1:2005, 4.3, 7.1, 7.5
Anzeigen und Alarme	—	4.8	ISO 7731 ISO 11428 ISO 11429 ISO 61310-1 IEC 60204-1:2005, 10.3, 10.4 IEC 61131-3 IEC 62061

Bei der Identifikation und Spezifikation der Sicherheitsfunktion(en) muss mindestens Folgendes betrachtet werden:

- a) Ergebnisse der Risikobeurteilung für jede bestimmte Gefährdung oder Gefährdungssituation;
- b) Betriebseigenschaften der Maschine, mit
 - der beabsichtigten Verwendung der Maschine (einschließlich der vernünftigerweise vorhersehbaren Fehlanwendung),
 - den Betriebsarten (z. B. lokale Betriebsart, Automatikbetrieb, Betrieb mit Bezug zu einem Bereich oder Teilen der Maschine),
 - Zykluszeit, und
 - Ansprechzeit;
- c) Handlung im Notfall;
- d) Beschreibung der Wechselwirkung verschiedener Arbeitsprozesse und manueller Aktionen (Reparatur, Einrichten, Reinigung, Fehlersuche usw.);
- e) dem Verhalten der Maschine, welches durch eine Sicherheitsfunktion zu erreichen oder zu verhindern ist;
- f) Bedingung(en) (z. B. Betriebsart) der Maschine, in der sie aktiv oder gesperrt ist;
- g) der Häufigkeit der Betätigung;
- h) Priorität derjenigen Funktionen, die gleichzeitig aktiv sein können und dadurch zu Konflikten führen.

5.2 Nähere Angaben über die Sicherheitsfunktionen

5.2.1 Sicherheitsbezogene Stoppfunktion

Zusätzlich zu den Anforderungen aus Tabelle 8 wird Folgendes angewendet.

Eine sicherheitsbezogene Stoppfunktion (z. B. eingeleitet durch eine Schutzeinrichtung) muss so schnell wie notwendig nach der Auslösung die Maschine in den sicheren Zustand bringen. Solch ein Stopp muss Vorrang vor einem betriebsmäßigen Stopp haben.

Wenn eine Gruppe von Maschinen koordiniert zusammenarbeitet, müssen Vorkehrungen getroffen werden, der übergeordneten Steuerung und/oder den anderen Maschinen eine solche Stoppbedingung zu signalisieren.

ANMERKUNG Eine sicherheitsbezogene Stoppfunktion kann im Betrieb Probleme und einen schwierigen Wiederanlauf bereiten, z. B. beim Lichtbogenschweißen. Um die Versuchung zu reduzieren, diese Stoppfunktion zu umgehen, kann diese einem Betriebsstopp vorausgehen, um den aktuellen Arbeitsgang abschließen zu können und die Vorbereitung für einen leichten und schnellen Wiederanlauf (ohne Schaden an der Produktion) zu treffen. Eine Lösung ist die Verwendung von Verriegelungseinrichtungen mit Zuhaltung, wobei die Zuhaltung erst entriegelt wird, wenn ein Zyklus eine definierte Position erreicht hat und ein einfacher Wiederanlauf möglich ist.

5.2.2 Manuelle Rückstellungsfunktion

Zusätzlich zu den Anforderungen aus Tabelle 8 wird Folgendes angewendet.

Nach der Einleitung eines Stoppbefehls durch eine Schutzeinrichtung muss der Stoppzustand aufrechterhalten bleiben, bis eine manuelle Rückstelleinrichtung betätigt wird und der sichere Zustand für einen Wiederanlauf gegeben ist.

Die Wiederherstellung der Sicherheitsfunktion durch die Rückstellung der Schutzeinrichtung unterbricht den Stoppbefehl. Wenn durch die Risikobeurteilung angezeigt, muss diese Aufhebung des Stoppbefehls durch eine manuelle, separate und beabsichtigte Handlung (manuelle Rückstellung) bestätigt werden.

Die manuelle Rückstellfunktion:

- muss durch ein getrenntes, manuell zu bedienendes Gerät in dem SRP/CS bereitgestellt werden,
- darf nur dann erreicht werden, wenn alle Sicherheitsfunktionen und Schutzeinrichtungen funktionsfähig sind,
- darf selbst keine Bewegung oder Gefährdungssituation einleiten,
- muss eine beabsichtigte Handlung sein,
- muss der Steuerung ermöglichen, einen separaten Startbefehl anzunehmen,
- darf nur erfolgen durch das Loslassen des Antriebselements in seiner betätigten (Ein)Position.

Der Performance Level der sicherheitsbezogenen Teile für die manuelle Rückstellfunktion muss so ausgewählt werden, dass die Einbeziehung der manuellen Rückstellfunktion die erforderliche Sicherheit der zugehörigen Sicherheitsfunktion nicht mindert.

Das Antriebselement zum Rücksetzen muss außerhalb des Gefahrenbereichs und an einer sicheren Position mit guter Einsicht zur Überprüfung, dass sich keine Person im Gefahrenbereich befindet, angebracht werden.

Wo die Einsicht in den Gefahrenbereich nicht vollständig ist, wird ein spezielles Rückstellverfahren erforderlich.

EN ISO 13849-1:2008 (D)

ANMERKUNG Eine Lösung ist die Verwendung eines zweiten Antriebselements zum Rücksetzen. Die Rückstellfunktion wird innerhalb des Gefahrenbereichs durch das erste Antriebselement in Kombination mit einem zweiten Antriebselement außerhalb des Gefahrenbereichs (nahe der Schutzeinrichtung) eingeleitet. Dieses Rückstellverfahren erfolgt innerhalb einer eingeschränkten Zeit, bevor die Steuerung einen separaten Startbefehl akzeptiert.

5.2.3 Start-/Wiederaufnahmefunktion

Zusätzlich zu den Anforderungen aus Tabelle 8 wird Folgendes angewendet.

Ein Wiederanlauf darf nur dann automatisch erfolgen, wenn keine Gefährdungssituation bestehen kann. Insbesondere bei einer verriegelten trennenden Schutzeinrichtung mit Startfunktion, ISO 12100-2:2003, 5.3.2.5 trifft zu.

Diese Anforderungen an Start und Wiederanlauf müssen auch bei Maschinen angewendet werden, die fern gesteuert werden können.

ANMERKUNG Die Rückmeldung eines Sensorsignals kann einen automatischen Start auslösen.

BEISPIEL Beim automatischen Maschinenablauf wird die Rückmeldung eines Sensorsignals häufig zur Steuerung des Prozessablaufs verwendet. Wenn ein Werkstück seine Position verlässt, wird der Ablauf gestoppt. Wenn die Überwachung der verriegelnden Schutzeinrichtung der automatischen Steuerung nicht übergeordnet ist, könnte eine Gefahr bestehen, dass die Maschine wieder anläuft, wenn die Bedienerperson der Maschine die Lage des Werkstücks korrigiert. Deshalb sollte der fern gesteuerte Wiederanlauf nicht erlaubt werden, bis die Schutzeinrichtung wieder geschlossen ist und der Monteur den Gefährdungsbereich verlassen hat. Der Beitrag zur Verhinderung eines unerwarteten Anlaufs durch die Steuerung hängt vom Ergebnis der Risikobeurteilung ab.

5.2.4 Lokale Steuerungsfunktion

Zusätzlich zu den Anforderungen aus Tabelle 8 wird Folgendes angewendet.

Wird eine Maschine lokal gesteuert, z. B. durch ein tragbares Bedienteil oder eine Hängebedienungstafel, müssen folgende Anforderungen angewendet werden:

- die Mittel zur Anwahl der lokalen Steuerung müssen außerhalb des Gefahrenbereichs angebracht sein;
- es darf durch eine lokale Steuerungsfunktion nur in einem Bereich, der durch eine Risikobeurteilung definiert wurde, möglich sein, Gefährdungsbedingungen auszulösen;
- die Umschaltung von Lokal- auf Hauptsteuerung darf keine Gefährdungssituationen erzeugen.

5.2.5 Mutingfunktion

Zusätzlich zu den Anforderungen aus Tabelle 8 wird Folgendes angewendet.

Muting darf nicht dazu führen, dass eine Person Gefährdungssituationen ausgesetzt wird. Während des Mutings muss der sichere Zustand durch andere Maßnahmen erreicht werden.

Nach dem Muting müssen alle Sicherheitsfunktionen der SRP/CS wieder hergestellt werden.

Die Performance Level der sicherheitsbezogenen Teile, die die Mutingfunktion ausführen, müssen so ausgewählt werden, dass deren Implementierung die erforderliche Sicherheit der entsprechenden Sicherheitsfunktion nicht verringert.

ANMERKUNG In einigen Anwendungen ist ein Signal zur Anzeige des Mutings notwendig.

5.2.6 Ansprechzeit

Zusätzlich zu den Anforderungen aus Tabelle 9 wird Folgendes angewendet.

Wenn die Risikobeurteilung der SRP/CS die Notwendigkeit zeigt, muss die Reaktionszeit der SRP/CS bestimmt werden (siehe auch Abschnitt 11).

ANMERKUNG Die Ansprechzeit der Steuerung ist Teil der Gesamt-Ansprechzeit der Maschine. Die erforderliche Gesamt-Ansprechzeit der Maschine kann die Gestaltung der sicherheitsbezogenen Teile beeinflussen, z. B. die Notwendigkeit, eine Bremse bereitzustellen.

5.2.7 Sicherheitsbezogene Parameter

Zusätzlich zu den Anforderungen aus Tabelle 9 wird Folgendes angewendet.

Wenn sicherheitsbezogene Parameter, z. B. Position, Geschwindigkeit, Temperatur oder Druck, von vorhandenen Grenzen abweichen, muss die Steuerung geeignete Maßnahmen einleiten (z. B. Einleiten eines Stopps, Warnsignals, Alarm).

Wenn Abweichungen in manuell eingegebenen sicherheitsbezogenen Daten für programmierbare elektronische Systeme zu Gefährdungssituationen führen können, muss in der sicherheitsbezogenen Steuerung ein Datentest bereitgestellt werden, z. B. Test auf Grenzen, Format und/oder Logik der Werte.

5.2.8 Schwankungen, Verlust und Wiederkehr der Energiequellen

Zusätzlich zu den Anforderungen aus Tabelle 9 wird Folgendes angewendet.

Wenn Schwankungen in Energiepegeln auftreten, die außerhalb des Betriebsbereichs liegen, einschließlich Verlust der Energieversorgung, muss das SRP/CS weiterhin Ausgangssignale bereitstellen oder einleiten, die anderen Teilen der Maschine ermöglichen, den sicheren Zustand aufrechtzuerhalten.

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

6.1 Allgemeines

Die SRP/CS müssen mit einer oder mehreren Anforderungen der fünf Kategorien, die in 6.2 beschrieben sind, übereinstimmen.

Kategorien sind der Basisparameter, um einen speziellen PL zu erreichen. Sie legen das erforderliche Verhalten der SRP/CS bezüglich ihrer Widerstandsfähigkeit gegenüber Fehlern, basierend auf ihrer in Abschnitt 4 beschriebenen Gestaltung fest.

Die Kategorie B ist die grundlegende Kategorie. Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen. In Kategorie 1 wird der verbesserte Widerstand gegen Fehler überwiegend durch Auswahl und Anwendung von Bauteilen erreicht. In den Kategorien 2, 3 und 4 wird die verbesserte Leistung bezüglich der spezifizierten Sicherheitsfunktion überwiegend durch die Verbesserung der Struktur der SRP/CS erreicht. In Kategorie 2 wird dies durch wiederkehrende Testung, ob die spezifizierte Sicherheitsfunktion ausgeführt wird, erreicht. In den Kategorien 3 und 4 wird dies erreicht, durch Sicherstellung, dass ein einzelner Fehler nicht zum Verlust der Sicherheitsfunktion führt. In Kategorie 4 und wann immer in Kategorie 3 in angemessener Weise möglich, wird ein solcher Fehler erkannt. In der Kategorie 4 wird die Widerstandsfähigkeit gegen Fehleranhäufungen festgelegt.

Tabelle 10 gibt eine Übersicht über die Kategorien der SRP/CS, die Anforderungen und das Verhalten des Systems im Fall von Fehlern.

Bei der Betrachtung von Ausfällen können für einige Komponenten bestimmte Fehler ausgeschlossen werden (siehe Abschnitt 7).

EN ISO 13849-1:2008 (D)

Die Auswahl einer Kategorie für ein spezielles SRP/CS hängt hauptsächlich von Folgendem ab:

- der Reduktion des Risikos, die durch die Sicherheitsfunktion erreicht werden soll, zu dem das Teil beiträgt,
- dem erforderlichen Performance Level (PL_r),
- der verwendeten Technologie,
- dem entstehenden Risiko im Fall eines Fehlers in diesem Teil,
- den Möglichkeiten, Fehler in diesem Teil zu vermeiden (systematische Fehler),
- der Wahrscheinlichkeit des Auftretens eines Fehlers in diesem Teil und den zugehörigen Parametern,
- der mittleren Zeit bis zum gefahrbringenden Ausfall ($MTTF_d$),
- dem Diagnosedeckungsgrad (DC), und
- dem Ausfall infolge gemeinsamer Ursache (CCF) bei Kategorien 2, 3 und 4.

6.2 Spezifikation der Kategorien

6.2.1 Allgemeines

Jedes SRP/CS muss mit den Anforderungen der entsprechenden Kategorie übereinstimmen (siehe 6.2.3 bis 6.2.7).

Die folgenden Architekturen sind typisch, um die Anforderungen der zugehörigen Kategorie zu erfüllen.

Die folgenden Bilder sind keine Beispiele, sondern allgemeine Architekturen. Eine Abweichung von diesen Architekturen ist immer möglich, aber jede Abweichung muss durch angemessene analytische Werkzeuge (z. B. Markov-Modelle, Fehlerbaumanalyse) begründet werden, sodass das System den erforderlichen Performance Level (PL_r) erreicht.

Die vorgesehenen Architekturen können nicht nur als Schaltplan, sondern auch als logische Schaltbilder betrachtet werden. Dies bedeutet für Kategorie 3 und 4 nicht notwendigerweise, dass alle Teile physikalisch redundant vorhanden sind, sondern das redundante Mittel bereitstehen, um sicherzustellen, dass ein Fehler nicht zum Verlust der Sicherheitsfunktion führen kann.

Die Linien und Pfeile in den Bildern 8 bis 12 stellen logische Verbindungs- und logische mögliche Diagnosemittel dar.

6.2.2 Vorgesehene Architekturen

Die Struktur eines SRP/CS ist ein Schlüsselmerkmal mit großem Einfluss auf den PL. Auch wenn die Vielfalt der möglichen Strukturen groß ist, sind die grundlegenden Konzepte oft ähnlich. So können die meisten Strukturen, die im Bereich der Maschinen existieren, auf einer der Kategorien abgebildet werden. Für jede Kategorie kann eine typische Darstellung in Form eines sicherheitsbezogenen Blockschalbildes gemacht werden. Diese typischen Ausführungen werden vorgesehene Architektur genannt und jede im Zusammenhang mit den folgenden Kategorien aufgelistet.

Es ist wichtig, dass der in Bild 5 gezeigte PL, der abhängig ist von der Kategorie, der $MTTF_d$ jedes Kanals und dem DC_{avg} , auf vorgesehenen Architekturen basiert. Wenn Bild 5 verwendet wird, um den PL zu bestimmen, sollte nachgewiesen sein, dass die Architektur der SRP/CS gleichwertig zur vorgesehenen Architektur der geforderten Kategorie ist. Entwicklungen, die die Merkmale der entsprechenden Kategorie erfüllen, sind im Allgemeinen gleichwertig zur entsprechenden vorgesehenen Architektur der Kategorie.

ANMERKUNG In einigen Fällen kann, sich aus einer speziellen Lösung ergebend oder durch eine TYP-C-Norm bestimmt, die sicherheitsbezogene Leistungsfähigkeit des SRO/CS nur durch eine Kategorie ohne zusätzlichen PL_r gefordert werden. Für solche speziellen Fälle wird die Sicherheit besonders durch die Architektur bereitgestellt, und die Anforderungen an die MTTF, den DC und den CCF sind nicht anwendbar.

6.2.3 Kategorie B

Die SRP/CS müssen in Übereinstimmung mit den zutreffenden Normen mindestens so gestaltet, gebaut, ausgewählt, zusammengestellt und kombiniert sein und bei Anwendung grundlegender Sicherheitsprinzipien für die bestimmte Anwendung Folgendem standhalten:

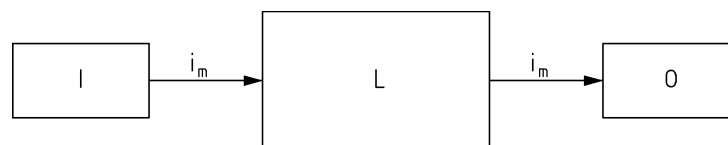
- den zu erwartenden Betriebsbeanspruchungen, z. B. der Zuverlässigkeit bezüglich des Schaltvermögens und Schalthäufigkeit,
- dem Einfluss des bearbeiteten Materials, z. B. dem Reinigungsmittel in einer Waschmaschine, und
- anderen relevanten äußeren Einflüssen, z. B. mechanische Schwingungen, elektromagnetischen Störungen, Unterbrechungen oder Störungen der Energieversorgung.

In Systemen der Kategorie B gibt es keinen Diagnosedeckungsgrad ($DC_{avg} = \text{kein}$), und die $MTTF_d$ jedes Kanals kann niedrig bis mittel sein. In solchen Strukturen (üblicherweise einkanalige Systeme) ist die Betrachtung von CCF nicht relevant.

Der maximale PL, der mit Kategorie B erreicht werden kann, ist $PL = b$.

ANMERKUNG Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen.

Besondere Anforderungen an die elektromagnetische Verträglichkeit sind in den entsprechenden Produktnormen, z. B. IEC 61800-3 über Antriebssysteme, zu finden. Besonders für die funktionale Sicherheit der SRP/CS sind die Anforderungen an die Störfestigkeit wichtig. Wenn keine Produktnorm vorhanden ist, sollten zumindest die Anforderungen der IEC 61000-6-2 an die Störfestigkeit befolgt werden.



Legende

- i_m Verbindungsmittel
- I Eingabeeinheit, z. B. Sensor
- L Logik
- O Ausgabeeinheit, z. B. Hauptschütz

Bild 8 — Vorgesehene Architektur für Kategorie B

6.2.4 Kategorie 1

Für Kategorie 1 müssen die gleichen Anforderungen erfüllt sein wie diese nach 6.2.3 für Kategorie B. Zusätzlich gilt Folgendes.

SRP/CS der Kategorie 1 müssen unter Verwendung bewährter Bauteile und bewährter Sicherheitsprinzipien gestaltet und gebaut werden (siehe ISO 13849-2).

Ein bewährtes Bauteil für eine sicherheitsbezogene Anwendung ist ein Bauteil, das entweder:

- a) in der Vergangenheit weit verbreitet mit erfolgreichen Ergebnissen in ähnlichen Anwendungen verwendet worden ist, oder
- b) unter Anwendung von Prinzipien hergestellt und verifiziert wurde, die seine Eignung und Zuverlässigkeit für sicherheitsbezogene Anwendungen zeigen.

EN ISO 13849-1:2008 (D)

Neu entwickelte Bauteile und Sicherheitsprinzipien können als gleichwertig bewährt betrachtet werden, wenn sie die in b) genannten Bedingungen erfüllen.

Die Entscheidung, ein bestimmtes Bauteil als bewährt zu akzeptieren, hängt von der Anwendung ab.

ANMERKUNG 1 Komplexe elektronische Bauteile (z. B. PLC, Mikroprozessor, anwendungsspezifische integrierte Schaltung) können nicht als gleichwertig zu bewährt betrachtet werden.

Die $MTTF_d$ jedes Kanals muss hoch sein.

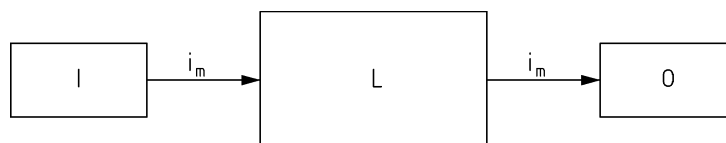
Der maximale PL, der mit Kategorie 1 erreicht werden kann, ist $PL = c$.

ANMERKUNG 2 In Systemen der Kategorie 1 gibt es keinen Diagnosedegrad ($DC_{avg} = \text{kein}$). In solchen Strukturen (einkanale Systeme) ist die Betrachtung von CCF nicht relevant.

ANMERKUNG 3 Bei Auftreten eines Fehlers kann dies zum Verlust der Sicherheitsfunktion führen. Jedoch ist die $MTTF_d$ in jedem Kanal der Kategorie 1 größer als in Kategorie B. Folglich ist der Verlust der Sicherheitsfunktion weniger wahrscheinlich.

Es ist wichtig, dass eine klare Unterscheidung zwischen „bewährtem Bauteil“ und „Fehlerausschluss“ (siehe Abschnitt 7) gemacht wird. Die Voraussetzung, dass ein Bauteil bewährt ist, hängt von seiner Anwendung ab. Zum Beispiel könnte ein Positionsschalter mit zwangsöffnenden Kontakten als bewährt für eine Werkzeugmaschine betrachtet werden, aber er wäre zum gleichen Zeitpunkt ungeeignet für die Anwendung in der Lebensmittelindustrie – in der Milchwirtschaft z. B. würde der Schalter nach wenigen Monaten durch die Milchsäure zerstört sein. Ein Fehlerausschluss kann zu einem sehr hohen PL führen, aber die getroffenen geeigneten Maßnahmen, die den Fehlerausschluss erlauben, sollten während der gesamten Lebensdauer des Bauteils gelten. Um dies sicherzustellen, können zusätzliche Maßnahmen außerhalb der Steuerung notwendig sein. Im Fall des Positionsschalters sind einige Beispiele von Maßnahmen dieser Art

- Mittel, um die Befestigung des Schalters nach der Justierung zu sichern,
- Mittel, um die Schaltnocke zu sichern,
- Mittel, um die Querstabilität der Schaltnocke zu sichern,
- Mittel, um ein Überfahren des Positionsschalters zu verhindern, z. B. ausreichende Festigkeit der Montage des Stoßdämpfers und Elemente zur Ausrichtung, und
- Mittel zur Verhinderung externer Beschädigung.

**Legende**

- i_m Verbindungsmittel
 I Eingabeeinheit, z. B. Sensor
 L Logik
 O Ausgabeeinheit, z. B. Hauptschütz

Bild 9 — Vorgesehene Architektur für Kategorie 1

6.2.5 Kategorie 2

Für Kategorie 2 müssen die gleichen Anforderungen erfüllt sein wie diese nach 6.2.3 für Kategorie B. Bewährten Sicherheitsprinzipien nach 6.2.4 muss ebenfalls gefolgt werden. Zusätzlich gilt Folgendes.

SRP/CS der Kategorie 2 müssen so gestaltet werden, dass ihre Funktionen in angemessenen Zeitabständen durch die Maschinensteuerung getestet werden. Der Test der Sicherheitsfunktion(en) muss durchgeführt werden:

- beim Anlauf der Maschine, und
- vor dem Einleiten einer Gefährdungssituation, z. B. Start eines neuen Zyklus, Start anderer Bewegungen und/oder periodisch während des Betriebs, wenn die Risikobeurteilung und die Betriebsart zeigen, dass dies notwendig ist.

Die Einleitung dieses Tests kann automatisch erfolgen. Jeder Test der Sicherheitsfunktion(en) muss entweder

- den Betrieb zulassen, wenn keine Fehler erkannt wurden, oder
- einen Ausgang für die Einleitung geeigneter Steuerungsmaßnahmen erzeugen, wenn ein Fehler erkannt wurde.

Wenn immer möglich, muss dieser Ausgang einen sicheren Zustand einleiten. Dieser sichere Zustand muss aufrechterhalten bleiben bis der Fehler behoben ist. Wenn die Einleitung eines sicheren Zustands nicht möglich ist (z. B. durch Verschweißen des Kontakts eines Schaltglieds), muss der Ausgang die Warnung vor der Gefährdung bereitstellen.

Für die in Bild 10 gezeigte vorgesehene Architektur der Kategorie 2 berücksichtigt die Berechnung der $MTTF_d$ und des DC_{avg} nur die Blöcke des Funktionskanals (d. h. I, L und O im Bild 10) und nicht die Blöcke des Testkanals (d. h. TE und OTE im Bild 10).

Der Diagnosedegrad (DC_{avg}) der gesamten SRP/CS einschließlich der Fehlererkennung muss niedrig sein. Die $MTTF_d$ jedes Kanals muss, abhängig vom erforderlichen Performance Level (PL_r), niedrig bis hoch sein. Maßnahmen gegen CCF müssen angewendet werden (siehe Anhang F).

Der Test darf selbst nicht zu einer Gefährdungssituation führen (z. B. aufgrund einer Erhöhung der Ansprechzeit). Die Testeinrichtung darf als Bestandteil der Sicherheitsfunktion ausführenden sicherheitsbezogenen Teile(s) oder getrennt davon vorgesehen sein.

Der maximale PL, der mit Kategorie 2 erreicht werden kann, ist PL = d.

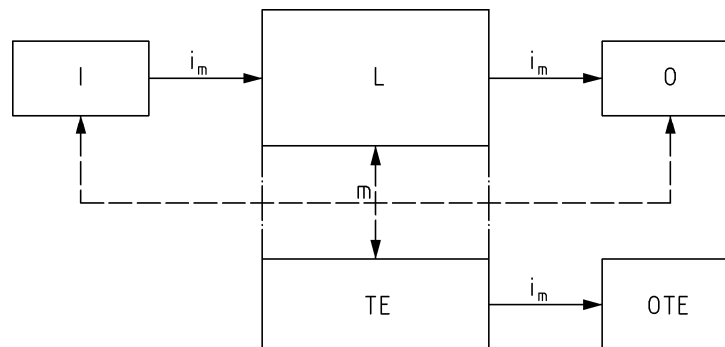
ANMERKUNG 1 In einigen Fällen ist die Kategorie 2 nicht anwendbar, da sich der Test der Sicherheitsfunktionen nicht bei allen Bauteilen durchführen lässt.

ANMERKUNG 2 Das Systemverhalten der Kategorie 2 lässt zu, dass

- zwischen den Tests das Auftreten eines Fehlers zum Verlust der Sicherheitsfunktion führen kann,
- der Verlust der Sicherheitsfunktion durch den Test erkannt wird.

ANMERKUNG 3 Das Prinzip, das die Gültigkeit einer Kategorie-2-Funktion stützt, ist, dass die angewendeten Festlegungen, z. B. die Wahl der Testhäufigkeit, die Wahrscheinlichkeit des Auftretens einer Gefährdungssituation verringert.

EN ISO 13849-1:2008 (D)



Die gestrichelten Linien zeigen die vernünftigerweise durchführbare Fehlererkennung.

Legende

i_m	Verbindungsmittel
I	Eingabeeinheit, z. B. Sensor
L	Logik
m	Überwachung
O	Ausgabeeinheit, z. B. Hauptschütz
TE	Testeinrichtung
OTE	Ausgang der TE

Bild 10 — Vorgesehene Architektur für Kategorie 2

6.2.6 Kategorie 3

Für Kategorie 3 müssen die gleichen Anforderungen erfüllt sein wie diese nach 6.2.3 für Kategorie B. Bewährten Sicherheitsprinzipien nach 6.2.4 muss ebenfalls gefolgt werden. Zusätzlich gilt Folgendes.

SRP/CS der Kategorie 3 müssen so gestaltet werden, dass ein einzelner Fehler in einem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt. Wenn immer in angemessener Weise durchführbar, muss ein einzelner Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt werden.

Der Diagnosedeckungsgrad (DC_{avg}) der gesamten SRP/CS einschließlich der Fehlererkennung muss niedrig sein. Die $MTTF_d$ jedes redundanten Kanals muss, abhängig vom PL_r , niedrig bis hoch sein. Maßnahmen gegen CCF müssen angewendet werden (siehe Anhang F).

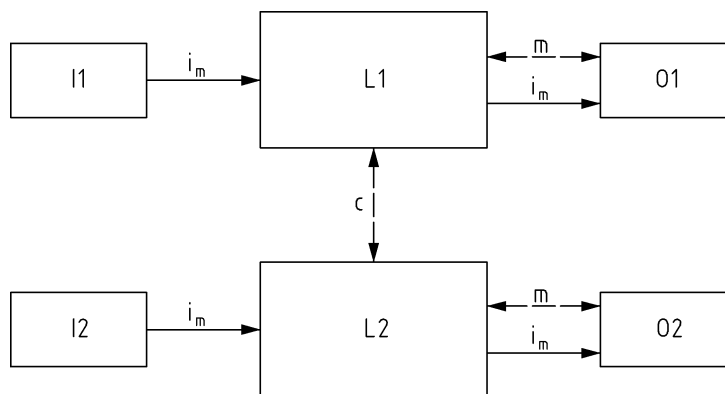
ANMERKUNG 1 Die Anforderung an die Erkennung einzelner Fehler bedeutet nicht, dass alle Fehler erkannt werden können. Folglich kann die Anhäufung unentdeckter Fehler zu einem unbeabsichtigten Ausgangssignal und einer Gefährdungssituation an der Maschine führen. Typische Beispiele für durchführbare Maßnahmen zur Fehlererkennung sind die Verwendung von zwangsgeführten Relaiskontakten und die Überwachung von redundanten elektrischen Ausgängen.

ANMERKUNG 2 Falls aufgrund der Technologie und Anwendung notwendig, sollte der Normensetzer von Typ-C-Normen weitere Einzelheiten zur Fehlererkennung nennen.

ANMERKUNG 3 Das Systemverhalten der Kategorie 3 lässt zu, dass

- bei Auftreten eines einzelnen Fehlers die Sicherheitsfunktion immer ausgeführt wird,
- einige, aber nicht alle Fehler erkannt werden,
- die Anhäufung unerkannter Fehler zum Verlust der Sicherheitsfunktion führen kann.

ANMERKUNG 4 Die verwendete Technologie hat Einfluss auf die Möglichkeiten zur Realisierung der Fehlererkennung.



Die gestrichelten Linien zeigen die vernünftigerweise durchführbare Fehlererkennung.

Legende

i_m	Verbindungsmittel
c	Kreuzvergleich
I1, I2	Eingabeeinheiten, z. B. Sensor
L1, L2	Logik
m	Überwachung
O1, O2	Ausgabeeinheiten, z. B. Hauptschütz

Bild 11 — Vorgesehene Architektur für Kategorie 3

6.2.7 Kategorie 4

Für Kategorie 4 müssen die gleichen Anforderungen erfüllt sein wie diese nach 6.2.3 für Kategorie B. Bewährten Sicherheitsprinzipien nach 6.2.4 muss ebenfalls gefolgt werden. Zusätzlich gilt Folgendes.

SRP/CS der Kategorie 4 müssen so gestaltet werden, dass

- ein einzelner Fehler in jedem dieser sicherheitsbezogenen Teile nicht zum Verlust der Sicherheitsfunktion führt, und
- der einzelne Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt wird, z. B. unmittelbar, beim Einschalten oder am Ende eines Maschinenzyklus,

aber wenn diese Erkennung nicht möglich ist, dann darf die Anhäufung von unerkannten Fehlern nicht zum Verlust der Sicherheitsfunktion führen.

Der Diagnosedeckungsgrad (DC_{avg}) der gesamten SRP/CS muss einschließlich der Anhäufung von Fehlern hoch sein. Die $MTTF_d$ jedes redundanten Kanals muss hoch sein. Maßnahmen gegen CCF müssen angewendet werden (siehe Anhang F).

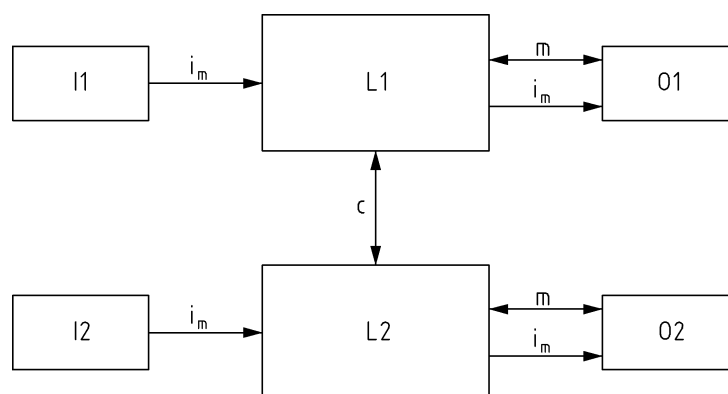
ANMERKUNG 1 Das Systemverhalten der Kategorie 4 lässt zu, dass

- bei Auftreten eines einzelnen Fehlers die Sicherheitsfunktion immer ausgeführt wird,
- Fehler rechtzeitig erkannt werden, um den Verlust der Sicherheitsfunktion zu verhindern,
- Anhäufungen von unerkannten Fehlern in Betracht gezogen werden.

ANMERKUNG 2 Der Unterschied zwischen Kategorie 3 und Kategorie 4 ist der höhere DC_{avg} in Kategorie 4 und die erforderliche $MTTF_d$ von nur „hoch“.

In der Praxis kann die Betrachtung einer Fehlerkombination für zwei Fehler ausreichend sein.

EN ISO 13849-1:2008 (D)



Die durchgezogenen Linien für die Überwachung stellen einen höheren Diagnosedeckungsgrad als bei der vorgesehenen Architektur der Kategorie 3 dar.

Legende

i _m	Verbindungsmittel
c	Kreuzvergleich
I1, I2	Eingabeeinheiten, z. B. Sensor
L1, L2	Logik
m	Überwachung
O1, O2	Ausgabeeinheiten, z. B. Hauptschütz

Bild 12 — Vorgesehene Architektur für Kategorie 4

Tabelle 10 — Zusammenfassung der Anforderungen für Kategorien

Kategorie	Zusammenfassung der Anforderungen	Systemverhalten	Prinzip zum Erreichen der Sicherheit	MTTF _d jedes Kanals	DC _{avg}	CCF
B (siehe 6.2.3)	SRP/CS(en) und/oder ihre Schutzeinrichtungen sowie ihre Bauteile müssen in Übereinstimmung mit den zutreffenden Normen so gestaltet, gebaut, ausgewählt, zusammengebaut und kombiniert werden, dass sie den zu erwartenden Einflüssen standhalten können. Grundlegende Sicherheitsprinzipien müssen verwendet werden.	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen.	Überwiegend durch die Auswahl von Bauteilen charakterisiert.	niedrig bis mittel	keine	nicht relevant
1 (siehe 6.2.4)	Die Anforderungen von B müssen erfüllt sein. Bewährte Bauteile und bewährte Sicherheitsprinzipien müssen angewendet werden.	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen, aber die Wahrscheinlichkeit des Auftretens ist geringer als in Kategorie B.	Überwiegend durch die Auswahl von Bauteilen charakterisiert.	hoch	keine	nicht relevant
2 (siehe 6.2.5)	Die Anforderungen von B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Die Sicherheitsfunktion muss in geeigneten Zeitabständen durch die Maschinensteuerung getestet werden.	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion zwischen den Tests führen. Der Verlust der Sicherheitsfunktion wird durch den Test erkannt.	Überwiegend durch die Struktur charakterisiert.	niedrig bis hoch	niedrig bis mittel	siehe Anhang F
3 (siehe 6.2.6)	Die Anforderungen von B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Sicherheitsbezogene Teile müssen so gestaltet werden, dass: — ein einzelner Fehler in jedem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt, und — wenn immer in angemessener Weise durchführbar, der einzelne Fehler erkannt wird.	Wenn ein einzelner Fehler auftritt, bleibt die Sicherheitsfunktion immer erhalten. Einige, aber nicht alle Fehler werden erkannt. Eine Anhäufung von unerkannten Fehlern kann zum Verlust der Sicherheitsfunktion führen.	Überwiegend durch die Struktur charakterisiert.	niedrig bis hoch	niedrig bis mittel	siehe Anhang F

EN ISO 13849-1:2008 (D)

Tabelle 10 (fortgesetzt)

Kategorie	Zusammenfassung der Anforderungen	Systemverhalten	Prinzip zum Erreichen der Sicherheit	MTTF _d jedes Kanals	DC _{avg}	CCF
4 (siehe 6.2.7)	<p>Die Anforderungen von B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein.</p> <p>Sicherheitsbezogene Teile müssen so gestaltet werden, dass:</p> <ul style="list-style-type: none"> — ein einzelner Fehler in jedem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt, und — der einzelne Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt wird. Wenn diese Erkennung nicht möglich ist, darf eine Anhäufung von unerkannten Fehlern nicht zum Verlust der Sicherheitsfunktion führen. 	<p>Wenn ein einzelner Fehler auftritt, bleibt die Sicherheitsfunktion immer erhalten.</p> <p>Die Erkennung von Fehleranhäufungen reduziert die Wahrscheinlichkeit des Verlustes der Sicherheitsfunktion (hohe DC).</p> <p>Die Fehler werden rechtzeitig erkannt, um einen Verlust der Sicherheitsfunktion zu verhindern.</p>	Überwiegend durch die Struktur charakterisiert.	hoch	hoch, einschl. der Fehleranhäufung	siehe Anhang F
ANMERKUNG Vollständige Anforderungen, siehe Abschnitt 6.						

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

Eine Sicherheitsfunktion kann durch eine Kombination von mehreren SRP/CS realisiert werden: Eingangssystem, Signalverarbeitung, Ausgangssystem. Diese Kombination kann einer und/oder unterschiedlichen Kategorien zugewiesen sein. Für jedes verwendete SRP/CS muss eine Kategorie nach 6.2 ausgewählt werden. Für die Gesamtkombination dieser SRP/CS kann nach Tabelle 11 ein Gesamt-PL ermittelt werden. In diesem Fall ist die Validierung der Kombination der SRP/CS erforderlich (siehe Bild 3).

Nach 6.2 beginnt die Kombination sicherheitsbezogener Teile einer Steuerung an dem Punkt, an dem sicherheitsbezogene Signale erzeugt werden und endet am Ausgang der Leistungssteuerungselemente. Die Kombination der SRP/CS könnte aber aus mehreren Teilen, die linear (Reihenschaltung) oder redundant (Parallelschaltung) verbunden sind, bestehen. Um eine erneute komplexe Einschätzung des erreichten Performance Levels (PL) der kombinierten SRP/CS zu vermeiden, wenn die einzelnen PL bereits berechnet waren, werden für eine Reihenschaltung folgende Abschätzungen gezeigt.

Angenommen werden N separate SRP/CS_{*i*} in einer Reihenschaltung, die zusammen eine Sicherheitsfunktion ausführen. Für jedes SRP/CS_{*i*} wurde bereits ein PL_{*i*} festgelegt. Diese Situation wird in Bild 13 dargestellt (siehe auch Bild 4 und Bild H.2).

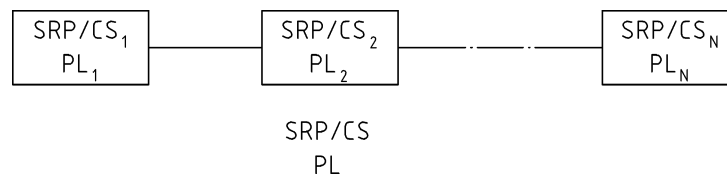


Bild 13 — Kombination von SRP/CS zum Erreichen des Gesamt-PL

Das folgende Verfahren erlaubt die Berechnung des PL der gesamten kombinierten SRP/CS, die die Sicherheitsfunktion ausführen:

- Bestimmen des niedrigsten PL_i , dies ist PL_{niedrig} .
- Bestimmen der Anzahl $N_{\text{niedrig}} \leq N$ der SRP/CS_i mit $PL_i = PL_{\text{niedrig}}$.
- Nachschlagen des PL in der folgenden Tabelle 11.

EN ISO 13849-1:2008 (D)

Tabelle 11 — Berechnung des PL für die Reihenschaltung von SRP/CS

PL_{niedrig}	N_{niedrig}	\Rightarrow	PL
a	> 3	\Rightarrow	kein, nicht erlaubt
	≤ 3	\Rightarrow	a
b	> 2	\Rightarrow	a
	≤ 2	\Rightarrow	b
c	> 2	\Rightarrow	b
	≤ 2	\Rightarrow	c
d	> 3	\Rightarrow	c
	≤ 3	\Rightarrow	d
e	> 3	\Rightarrow	d
	≤ 3	\Rightarrow	e
ANMERKUNG Die für das Nachschlagen berechneten Werte basieren auf Zuverlässigkeitswerten für die Mitte jedes PL.			

7 Berücksichtigung von Fehlern, Fehlerausschluss

7.1 Allgemeines

In Übereinstimmung mit der gewählten Kategorie müssen sicherheitsbezogene Teile so gestaltet werden, dass der erforderliche Performance Level (PL_r) erreicht wird. Die Fähigkeit, Fehlern zu widerstehen, muss beurteilt werden.

7.2 Fehlerbetrachtung

ISO 13849-2 zählt die wichtigsten Fehler und Ausfälle für verschiedene Technologien auf. Die Fehlerlisten sind nicht abschließend, und wenn notwendig, müssen weitere Fehler berücksichtigt und aufgezählt werden. In solchen Fällen sollte das Verfahren der Bewertung ebenfalls verständlich ausgearbeitet werden. Für neue Komponenten, die nicht in der ISO 13849-2 enthalten sind, muss eine Ausfallart und Effektanalyse (FMEA — siehe IEC 60812) durchgeführt werden, um festzulegen, welche Fehler für diese Bauteile berücksichtigt werden müssen.

Im Allgemeinen müssen folgende Fehlermerkmale in Betracht gezogen werden:

- wenn als eine Folge eines Fehlers weitere Bauteile ausfallen, müssen der erste Fehler zusammen mit allen Folgefehlern als ein Einzelfehler berücksichtigt werden;
- zwei oder mehrere einzelne Fehler, die eine gemeinsame Ursache haben, müssen als ein Fehler betrachtet werden (dies ist bekannt als ein CCF);
- das gleichzeitige Auftreten von zwei oder mehreren Fehlern unterschiedlicher Ursache wird als höchst unwahrscheinlich angesehen und braucht deswegen nicht betrachtet werden.

7.3 Fehlerausschluss

Es ist nicht immer möglich, die SRP/CS(en) zu bewerten ohne die Annahme, dass bestimmte Fehler ausgeschlossen werden können. Für ausführlichere Information zum Fehlerausschluss, siehe ISO 13849-2.

Der Fehlerausschluss ist ein Kompromiss zwischen den technischen Sicherheitsanforderungen und der theoretischen Möglichkeit des Auftretens eines Fehlers.

Der Fehlerausschluss kann basieren auf

- der technischen Unwahrscheinlichkeit des Auftretens einiger Fehler,
- der allgemeinen anerkannten technischen Erfahrung, unabhängig von der betrachteten Anwendung, und
- den technischen Anforderungen im Bezug zur Anwendung und der speziellen Gefährdung.

Wenn Fehler ausgeschlossen werden, muss eine genaue Begründung in der technischen Dokumentation gegeben werden.

8 Validierung

Die Gestaltung eines SRP/CS muss validiert werden (siehe Bild 3). Die Validierung muss zeigen, dass die Kombination für jede Sicherheitsfunktion des SRP/CS die entsprechenden Anforderungen dieses Teils der ISO 13849 erfüllen.

Für Einzelheiten zur Validierung, siehe ISO 13849-2.

9 Instandhaltung

Eine vorbeugende Instandhaltung oder Instandsetzung kann notwendig sein, um die festgelegte Leistung der sicherheitsbezogenen Teile aufrechtzuerhalten. Abweichungen von der festgelegten Leistung nach einer gewissen Zeit, kann zu einer Verschlechterung der Sicherheit oder sogar zu einer Gefährdungssituation führen. Die Betriebsanleitung des SRP/CS muss Anweisungen für die Instandhaltung (einschließlich periodischer Kontrollen) des SRP/CS enthalten.

Die Bedingungen für die Instandhaltbarkeit der sicherheitsbezogenen Teile einer Steuerung muss denen in ISO 12100-2:2003, 4.7 folgen. Alle Informationen der Instandhaltung müssen mit ISO 12100-2: 2003, 6.5.1 e) übereinstimmen.

10 Technische Dokumentation

Bei der Gestaltung eines SRP/CS muss deren Konstrukteur mindestens folgende Informationen über das sicherheitsbezogene Teil dokumentieren:

- die durch die SRP/CS bereitgestellte(n) Sicherheitsfunktion(en);
- die Eigenschaften jeder Sicherheitsfunktion;
- die genauen Punkte, wo die sicherheitsbezogenen Teile beginnen und enden;
- die Umgebungsbedingungen;
- den Performance Level (PL);

EN ISO 13849-1:2008 (D)

- die ausgewählte Kategorie oder die ausgewählten Kategorien;
- die auf die Zuverlässigkeit bezogenen Parameter (MTTF_d, DC, CCF und Einsatzdauer);
- die Maßnahmen gegen systematische Fehler;
- die verwendete Technologie oder die verwendeten Technologien;
- alle berücksichtigten sicherheitsbezogenen Fehler;
- die Begründungen für Fehlerausschlüsse (siehe ISO 13849-2);
- die Begründung der Gestaltung, (z. B. berücksichtigte Fehler, die ausgeschlossenen Fehler);
- Softwaredokumentation;
- Maßnahmen gegen vernünftigerweise vorhersehbare Fehlanwendung.

ANMERKUNG Im Allgemeinen ist diese Dokumentation für die herstellerinterne Verwendung gedacht und wird nicht an den Maschinennutzer weitergegeben.

11 Benutzerinformation

Die Grundsätze der ISO 12100-2:2003, 6.5.2 und anderer relevanter Dokumente (z. B. IEC 60204-1:2005, Abschnitt 17) müssen angewendet werden. Insbesondere müssen die Informationen, die zur sicheren Verwendung der SRP/CS wichtig sind, dem Benutzer gegeben werden. Dies muss einschließen, ist aber nicht auf das Folgende begrenzt:

- die Grenzen der sicherheitsbezogenen Teile zu den ausgewählten Kategorien und jedem Fehlerausschluss;
- die Grenzen der SRP/CS und jeden Fehlerausschluss (siehe 7.3) für diese, wenn sie wesentlich zur Aufrechterhaltung der gewählten Kategorie oder Kategorien und Sicherheitsleistung beitragen, müssen geeignete Informationen (z. B. für Änderung, Instandhaltung und Reparatur) geben, um die weitere Rechtfertigung der Fehlerausschlüsse aufrechtzuerhalten;
- Wirkungen von Abweichungen von der festgelegten Leistung für die Sicherheitsfunktion(en);
- verständliche Beschreibungen der Schnittstellen zu SRP/CS und Schutzeinrichtungen;
- Ansprechzeit;
- Grenzen für den Betrieb (einschließlich Umgebungsbedingungen);
- Anzeigen und Alarmen;
- Muting und zeitweiliges Aufheben der Sicherheitsfunktionen;
- Betriebsarten;
- Instandhaltung (siehe Abschnitt 9);
- Checklisten für die Instandhaltung;
- Erleichterung der Zugänglichkeit und Ersatz interner Teile;

- Mittel zur leichten und sicheren Fehlersuche;
- Information zur Erklärung der Einsatzmöglichkeiten für die Verwendung der entsprechenden Kategorie, auf die verwiesen wird;
- Kontrolle der Testintervalle, wenn relevant.

Besondere Informationen müssen zur Kategorie oder den Kategorien und dem Performance Level der SRP/CS wie folgt, angegeben werden:

- datierte Verweisung auf diesen Teil der ISO 13849 (d. h. „ISO 13849-1:2006“);
- die Kategorie B, 1, 2, 3, oder 4;
- den Performance Level a, b, c, d oder e.

BEISPIEL Auf ein SRP/CS nach dieser Ausgabe der ISO 13849-1 mit der Kategorie B und dem Performance Level a würde folgendermaßen verwiesen werden:

ISO 13849-1:2006 Kategorie B PL a

Anhang A (informativ)

Bestimmung des erforderlichen Performance Levels (PL_r)

A.1 Auswahl des PL_r

Dieser Anhang beschäftigt sich mit dem Beitrag zur Risikominderung durch die betrachteten sicherheitsbezogenen Teile der Steuerung. Das hier angegebene Verfahren stellt nur eine Einschätzung der Risikominderung zur Verfügung und ist als Anleitung für den Konstrukteur und Normensetzer vorgesehen, einen PL_r für jede notwendige, durch ein SRP/CS auszuführende Sicherheitsfunktion auszuwählen.

Die Risikobeurteilung nimmt eine Situation an, bevor die vorgesehene Sicherheitsfunktion bereitgestellt wird. Die Risikominderung durch andere technische Maßnahmen, die unabhängig von der Steuerung sind (z. B. mechanische trennende Schutzeinrichtungen) oder zusätzliche Sicherheitsfunktionen, können bei der Bestimmung des PL_r der vorgesehenen Sicherheitsfunktion berücksichtigt werden; in diesem Fall kann der Startpunkt im Bild A.1 an die Stelle nach der Implementierung dieser Maßnahmen gelegt werden (siehe auch Bild 2). Die Schwere der Verletzung (gekennzeichnet durch S) ist relativ einfach einzuschätzen (z. B. Fleischwunde, Amputation, Todesfall). Für die Häufigkeit des Auftretens werden zusätzliche Parameter verwendet, um die Bestimmung zu verbessern. Diese Parameter sind

- Häufigkeit und Dauer der Gefährdungsexposition (F) und
- Möglichkeit zur Vermeidung der Gefährdung oder Begrenzung des Schadens (P).

Die Erfahrung hat gezeigt, dass diese Parameter wie in Bild A.1 gezeigt kombiniert werden können, um eine Abstufung des Risikos von niedrig bis hoch zu geben. Es wird betont, dass dies nur ein qualitatives Verfahren ist, das nur eine Abschätzung des Risikos liefert.

A.2 Anleitung für die Auswahl der Parameter S, F und P zur Einschätzung des Risikos

A.2.1 Schwere der Verletzung S1 und S2

Bei der Einschätzung des Risikos durch einen Ausfall einer Sicherheitsfunktion werden nur leichte Verletzungen (üblicherweise reversible) und ernste Verletzungen (üblicherweise irreversibel und Tod) berücksichtigt.

Um eine Entscheidung treffen zu können, sollten die üblichen Auswirkungen der Unfälle und normale Heilungsprozesse bei der Bestimmung von S1 und S2 in Betracht gezogen werden. Zum Beispiel würden Quetschungen und/oder Fleischwunden ohne Komplikationen als S1 klassifiziert, wohingegen eine Amputation oder Tod S2 sein würde.

A.2.2 Häufigkeit und/oder Dauer der Gefährdungsexposition F1 und F2

Ein allgemeingültiger Zeitraum, wann Parameter F1 oder wann F2 auszuwählen ist, kann nicht festgelegt werden. Allerdings könnte die folgende Erklärung das Treffen der richtigen Entscheidung in Zweifelsfällen erleichtern.

F2 sollte ausgewählt werden, wenn eine Person häufig oder dauernd einer Gefährdung ausgesetzt ist. Dabei ist es unerheblich, ob dieselbe oder nacheinander unterschiedliche Personen der Gefährdung ausgesetzt werden, z. B. bei der Verwendung von Aufzügen. Der Parameter der Häufigkeit sollte ausgewählt werden nach der Häufigkeit und Dauer des Zugangs zur Gefährdung.

Wo die Anforderung an die Sicherheitsfunktion dem Konstrukteur bekannt ist, kann die Häufigkeit und Dauer dieser Anforderung anstelle der Häufigkeit und Dauer des Zugangs zur Gefährdung gewählt werden. In diesem Teil der ISO 13849 wird angenommen, dass die Häufigkeit einer Anforderung der Sicherheitsfunktion mehr als einmal je Jahr ist.

Die Dauer der Gefährdungsexposition sollte auf der Basis eines durchschnittlichen Werts bewertet werden, der im Verhältnis zur Gesamtzeit gesehen werden kann, über die die Einrichtung verwendet wird. Ist es z. B. notwendig, im zyklischen Betrieb zwischen die Werkzeuge der Maschine zu greifen, um Werkstücke zuzuführen oder zu bewegen, dann sollte F2 gewählt werden. Wenn der Zugang nur von Zeit zu Zeit erforderlich ist, dann sollte F1 gewählt werden.

ANMERKUNG Ohne andere Festlegung sollte F2 gewählt werden, wenn die Frequenz häufiger als einmal je Stunde ist.

A.2.3 Möglichkeit zur Vermeidung der Gefährdung P1 und P2

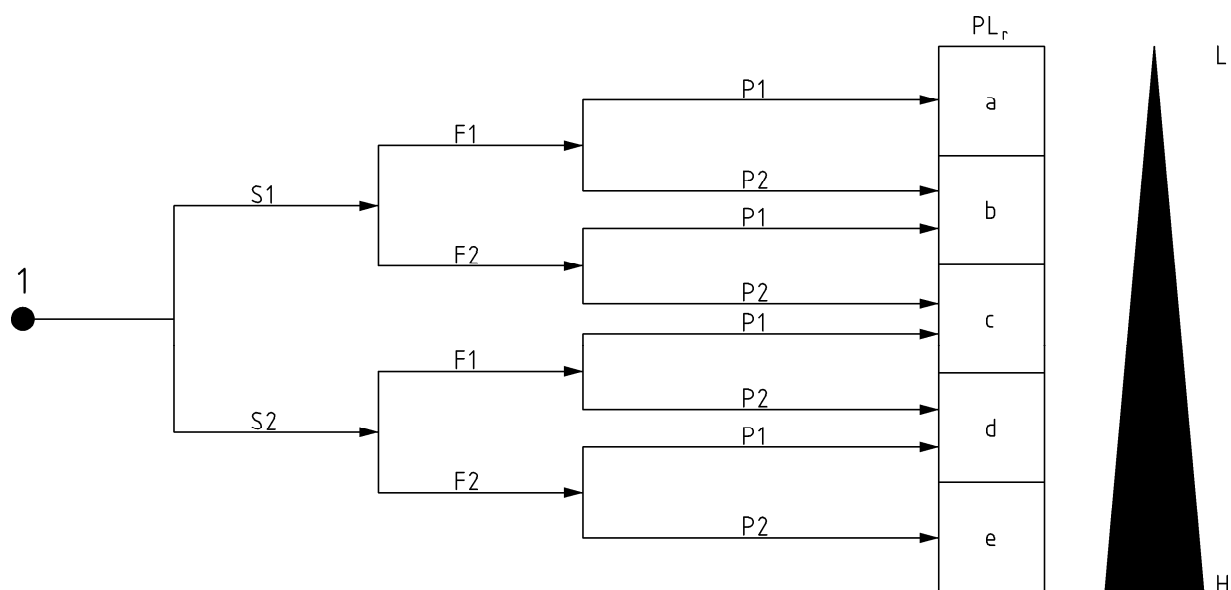
Es ist wichtig zu wissen, ob eine Gefährdungssituation erkannt oder vermieden werden kann, bevor sie zu einem Unfall führt. Eine wichtige Überlegung ist z. B., ob die Gefährdung direkt durch ihre physikalischen Eigenschaften identifiziert werden kann, oder nur durch technische Mittel erkannt werden kann, 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);
- Möglichkeiten 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.

Bild A.1 gibt eine Anleitung für die Bestimmung des sicherheitsbezogenen PL_r, abhängig von der Risikobeurteilung. Die grafische Darstellung sollte für jede Sicherheitsfunktion berücksichtigt werden. Das Verfahren der Risikobeurteilung basiert auf ISO 14121 und sollte nach ISO 12100-1 erfolgen.

EN ISO 13849-1:2008 (D)

**Legende**

- 1 Startpunkt zur Bewertung des Beitrags der Risikominderung
 L niedriger Beitrag zur Risikoreduzierung
 H hoher Beitrag zur Risikominderung
 PL_r erforderlicher Performance Level

Risikoparameter:

- S Schwere der Verletzung
 S1 leichte (üblicherweise reversible Verletzung)
 S2 ernste (üblicherweise irreversible Verletzung einschließlich Tod)
 F Häufigkeit und/oder Dauer der Gefährdungsexposition
 F1 selten bis weniger häufig und/oder die Zeit der Gefährdungsexposition ist kurz
 F2 häufig bis dauernd und/oder die Zeit der Gefährdungsexposition ist lang
 P Möglichkeit zur Vermeidung der Gefährdung oder Begrenzung des Schadens
 P1 möglich unter bestimmten Bedingungen
 P2 kaum möglich

Bild A.1 — Risikograf zur Bestimmung des PL_r für jede Sicherheitsfunktion

Anhang B (informativ)

Blockmethode und sicherheitsbezogenes Blockdiagramm

B.1 Blockmethode

Die vereinfachte Methode benötigt eine blockorientierte logische Darstellung der SRP/CS. Die SRP/CS sollten in eine kleine Anzahl von Blöcken wie folgt zerlegt werden:

- die Blöcke sollten die logischen Einheiten der SRP/CS abbilden, die sich auf die Ausführung der Sicherheitsfunktion beziehen;
- unterschiedliche Kanäle, die die Sicherheitsfunktion ausführen, sollten in separaten Blöcken dargestellt werden – wenn ein Block nicht mehr in der Lage ist, seine Funktion zu leisten, sollte die Ausführung der Sicherheitsfunktion durch die Blöcke des anderen Kanals nicht betroffen werden;
- jeder Kanal kann aus einem oder mehreren Blöcken bestehen – drei Blöcke je Kanal der vorgesehenen Architekturen, Eingang, Logik und Ausgang, ist keine bindende Anzahl, sondern nur ein Beispiel der logischen Aufteilung innerhalb jedes Kanals;
- jede Hardwareeinheit der SRP/CS sollte exakt einem Block zugeordnet werden, dies erlaubt die Berechnung der $MTTF_d$ des Blocks, basierend auf der $MTTF_d$ der Hardwareeinheiten, die zu diesem Block gehören (z. B. durch die Ausfallarten und Effektanalyse oder die „Parts-Count“-Verfahren (siehe Anhang D.1);
- Hardwareeinheiten, die nur zur Diagnose verwendet werden (z. B. Testeinrichtungen) und die Ausführung der Sicherheitsfunktion in den verschiedenen Kanälen nicht beeinflussen, wenn sie gefährlich ausfallen, können von den Einheiten getrennt werden, die notwendig sind, die Sicherheitsfunktion in den unterschiedlichen Kanälen auszuführen.

ANMERKUNG Für die Anwendung dieses Teils der ISO 13849 entsprechen „Blöcke“ nicht Funktionsblöcken oder Zuverlässigkeitsblöcken.

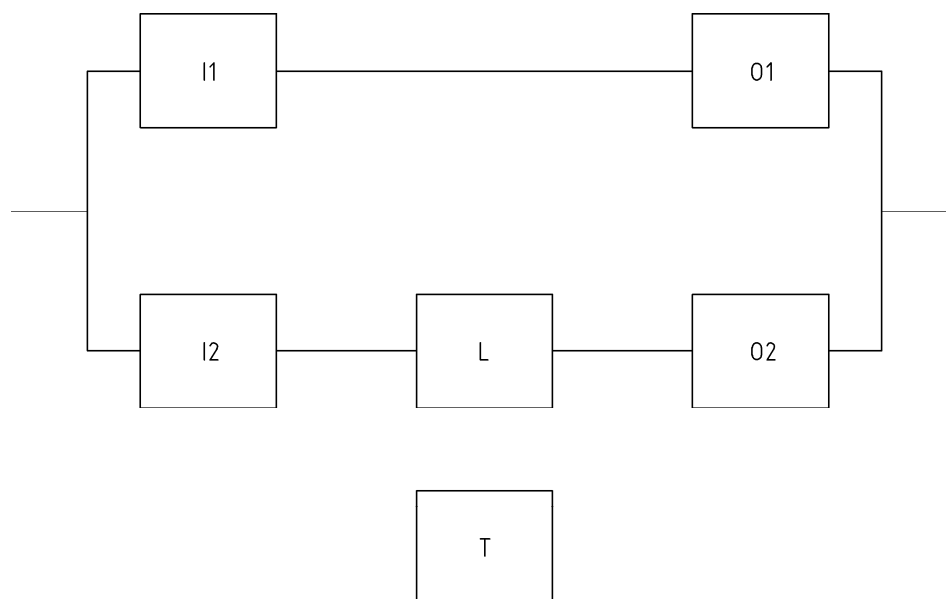
B.2 Sicherheitsbezogenes Blockdiagramm

Die durch die Blockmethode definierten Blöcke können verwendet werden, um die logische Struktur der SRP/CS in einem sicherheitsbezogenen Blockdiagramm darzustellen. Für die grafische Darstellung kann folgende Anleitung verwendet werden:

- der Ausfall eines Blocks in einer Serienschaltung von Blöcken führt zu einem Ausfall des gesamten Kanals (z. B. wenn eine Hardwareeinheit in einem Kanal gefährlich ausfällt, kann der gesamte Kanal seine Sicherheitsfunktion nicht weiter ausführen);
- nur der gefährliche Ausfall aller Kanäle in einer Parallelschaltung führt zum Verlust der Sicherheitsfunktion (z. B. eine durch mehrere Kanäle ausgeführte Sicherheitsfunktion wird so lange ausgeführt, solange mindestens ein Kanal keinen Ausfall hat);
- Blöcke, die nur für Testzwecke verwendet werden und die Ausführung der Sicherheitsfunktion in den verschiedenen Kanälen nicht beeinflussen, können von Blöcken in den verschiedenen Kanälen getrennt werden.

EN ISO 13849-1:2008 (D)

Siehe Bild B.1 als Beispiel.



I1 und O1 bilden den ersten Kanal (Serienschaltung), während I2, L und O2 den zweiten Kanal bilden (Serienschaltung), mit beiden Kanälen wird die Sicherheitsfunktion redundant ausgeführt (Parallelschaltung). T wird nur für die Testung verwendet.

Legende

I1, I2	Eingabeeinheit, z. B. Sensor
L	Logik
O1, O2	Ausgabeeinheiten, z. B. Hauptschütz
T	Testeinrichtung

Bild B.1 — Beispiel eines sicherheitsbezogenen Blockdiagramms

Anhang C (informativ)

Berechnung oder Abschätzung von $MTTF_d$ -Werten für einzelne Bauteile

C.1 Allgemeines

Dieser Anhang gibt verschiedene Verfahren an, um $MTTF_d$ -Werte für einzelne Bauteile zu berechnen oder abzuschätzen; das Verfahren in C.2 basiert auf guter ingenieurmäßiger Praxis für unterschiedliche Arten von Bauteilen; das in C.3 ist anwendbar auf hydraulische Bauteile; C.4 liefert ein Mittel zur Berechnung der $MTTF_d$ für pneumatische, hydraulische und elektromechanische Bauteile auf Basis von B_{10} -Werten (siehe C.4.1); C.5 listet $MTTF_d$ -Werte für elektrische Bauteile.

C.2 Verfahren guter ingenieurmäßiger Praxis

Wenn die folgenden Merkmale erfüllt sind, kann der $MTTF_d$ - oder B_{10d} -Wert für ein Bauteil nach Tabelle C.1 bestimmt werden:

- Der Hersteller des Bauteils bestätigt die Verwendung von grundlegenden und bewährten Sicherheitsprinzipien nach ISO 13849-2:2003 oder der entsprechenden Norm (siehe Tabelle C.1) für die Konstruktion des Bauteils (Bestätigung im Datenblatt des Bauteils).

ANMERKUNG Diese Information kann im Datenblatt des Bauteilherstellers gefunden werden.

- Der Hersteller des Bauteils beschreibt die geeignete Anwendung und Betriebsbedingungen für den Anwender.
- Der Hersteller des SRP/CS erfüllt die grundlegenden und bewährten Sicherheitsprinzipien nach ISO 13849-2:2003, für die Implementierung und den Betrieb des Bauteils.

C.3 Hydraulische Bauteile

Wenn die folgenden Merkmale erfüllt sind, kann der $MTTF_d$ -Wert für ein einzelnes hydraulisches Bauteil, z. B. Ventil, mit 150 Jahren angenommen werden:

- Der Hersteller des hydraulischen Bauteils bestätigt die Verwendung der grundlegenden und bewährten Sicherheitsprinzipien nach ISO 13849-2:2003, Tabellen C.1 und C.2 für die Konstruktion des hydraulischen Bauteils (Bestätigung im Datenblatt des Bauteils).

ANMERKUNG Diese Information kann im Datenblatt des Bauteilherstellers gefunden werden.

- Der Hersteller des hydraulischen Bauteils legt die geeignete Anwendung und Betriebsbedingungen für den Anwender fest. Der Anwender ist über seine Verantwortung zu informieren, die grundlegenden und bewährten Sicherheitsprinzipien nach ISO 13849-2:2003, Tabellen C.1 und C.2 für die Implementierung und den Betrieb des hydraulischen Bauteils zu erfüllen.

Wenn weder a) noch b) erreicht ist, ist der $MTTF_d$ -Wert für das hydraulische Bauteil durch den Hersteller anzugeben.

EN ISO 13849-1:2008 (D)

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

	Grundlegende und bewährte Sicherheitsprinzipien nach ISO 13849-2:2003	Andere relevante Normen	Typische Werte: $MTTF_d$ (Jahre) B_{10d} (Zyklus)
Mechanische Bauteile	Tabellen A.1 und A.2	—	$MTTF_d = 150$
Hydraulische Bauteile	Tabellen C.1 und C.2	EN 982	$MTTF_d = 150$
Pneumatische Bauteile	Tabellen B.1 und B.2	EN 983	$B_{10d} = 20\,000\,000$
Relais und Hilfsschütze mit geringer Last (mechanische Belastung)	Tabellen D.1 und D.2	EN 50205 IEC 61810 IEC 60947	$B_{10d} = 20\,000\,000$
Relais und Hilfsschütze mit maximaler Belastung	Tabellen D.1 und D.2	EN 50205 IEC 61810 IEC 60947	$B_{10d} = 400\,000$
Näherungsschalter mit geringer Last (mechanische Belastung)	Tabellen D.1 und D.2	IEC 60947 EN 1088	$B_{10d} = 20\,000\,000$
Näherungsschalter mit maximaler Belastung	Tabellen D.1 und D.2	IEC 60947 EN 1088	$B_{10d} = 400\,000$
Schütze mit geringer Last (mechanische Belastung)	Tabellen D.1 und D.2	IEC 60947	$B_{10d} = 20\,000\,000$
Schütze mit nominaler Last	Tabellen D.1 und D.2	IEC 60947	$B_{10d} = 2\,000\,000$
Positionsschalter, unabhängig von der Last ^a	Tabellen D.1 und D.2	IEC 60947 EN 1088	$B_{10d} = 20\,000\,000$
Positionsschalter (mit separatem Betätiger, Zuhaltung), unabhängig von der Last ^a	Tabellen D.1 und D.2	IEC 60947 EN 1088	$B_{10d} = 2\,000\,000$
Not-Aus-Einrichtungen, unabhängig von der Last ^a	Tabellen D.1 und D.2	IEC 60947 ISO 13850	$B_{10d} = 100\,000$
Not-Aus-Einrichtungen mit maximaler Beanspruchung ^a	Tabellen D.1 und D.2	IEC 60947 ISO 13850	$B_{10d} = 6\,050$
Druck-Taster (z. B. Zustimmungsschalter), unabhängig von der Last ^a	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 angenommen als zweimal B_{10} (50 % gefährlicher Ausfall).			
ANMERKUNG 2 „Geringe Last“ bedeutet z. B. 20 % des Bemessungswerts (für weitere Information siehe EN 13849-2).			
^a Falls Fehlerrückmeldung für Zwangsöffnung möglich ist.			

C.4 MTTF_d von pneumatischen, mechanischen und elektromechanischen Bauteilen

C.4.1 Allgemeines

Es kann schwierig sein, für pneumatische, mechanische und elektromechanische Bauteile (Pneumatikventile, Relais, Schütze, Positionsschalter, Nocken von Positionsschaltern usw.) die mittlere Zeit bis zum gefahrbringenden Ausfall (MTTF_d für Bauteile), die in Jahren angegeben wird und in diesem Teil der ISO 13849 benötigt wird, zu berechnen. Meistens gibt der Hersteller solcher Art von Bauteilen nur die Anzahl von Zyklen an, bis 10 % der Bauteile gefährlich ausfallen (B_{10d}). Dieser Abschnitt gibt ein Verfahren an, um die MTTF_d für Bauteile zu berechnen, unter Verwendung von B_{10} oder T (Lebensdauer), die vom Hersteller gegeben werden, mit engem Bezug zur anwendungsbezogenen Schalthäufigkeit.

Wenn die folgenden Merkmale erfüllt sind, kann der MTTF_d-Wert für ein einzelnes pneumatisches, elektromechanisches oder mechanisches Bauteil nach C.4.2 abgeschätzt werden.

- a) Der Hersteller des Bauteils bestätigt die Verwendung von grundlegenden Sicherheitsprinzipien nach ISO 13849-2:2003, Tabelle B.1 oder Tabelle D.1 für die Konstruktion des Bauteils.

ANMERKUNG Diese Information kann im Datenblatt des Bauteilherstellers gefunden werden.

- b) Der Hersteller eines Bauteils, das in Kategorie 1, 2, 3 oder 4 verwendet werden soll, bestätigt die Verwendung bewährter Sicherheitsprinzipien nach ISO 13849-2:2003, Tabellen B.2 oder D.2 für die Konstruktion des Bauteils.

ANMERKUNG Diese Information kann im Datenblatt des Bauteilherstellers gefunden werden.

- c) Der Hersteller des Bauteils legt die geeignete Anwendung und Betriebsbedingungen für den Anwender fest. Der Anwender ist über seine Verantwortung zu informieren, die grundlegenden Sicherheitsprinzipien nach ISO 13849-2:2003, Tabellen B.1 oder D.1 für die Implementierung und des Betriebs des Bauteils zu erfüllen. Für Kategorie 1, 2, 3 oder 4 ist der Anwender über seine Verantwortung zu informieren, die bewährten Sicherheitsprinzipien nach ISO 13849-2:2003, Tabellen B.2 oder D.2 für die Implementierung und den Betrieb des Bauteils zu erfüllen.

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

Die mittlere Anzahl von Zyklen, bis 10 % der Bauteile gefährlich ausgefallen sind (B_{10d})³⁾ sollte durch den Hersteller des Bauteils in Übereinstimmung mit den entsprechenden Produktnormen für die Prüfung bestimmt werden (z. B. IEC 60947-5-1, ISO 19973, IEC 61810). Die gefährlichen Ausfallarten der Bauteile sind zu definieren, z. B. Verkleben in einer Endposition oder Änderung der Schaltzeiten. Wenn während der Prüfung nicht alle Bauteile gefährlich ausfallen (z. B. sieben Bauteile geprüft, nur fünf gefährlich ausgefallen), dann sollte eine Analyse unter Berücksichtigung der Bauteile, die nicht ausgefallenen Bauteile waren, durchgeführt werden.

Mit B_{10d} und n_{op} , der mittleren Anzahl jährlicher Betätigungen, kann die MTTF_d für Bauteile wie folgt berechnet werden:

$$MTTF_d = \frac{B_{10d}}{0,1 \times n_{op}} \quad (C.1)$$

3) Wenn der gefährliche Anteil des B_{10} nicht angegeben ist, dürfen 50 % des B_{10} verwendet werden, deshalb wird $B_{10d} = 2 B_{10}$ empfohlen.

EN ISO 13849-1:2008 (D)

wobei

$$n_{op} = \frac{d_{op} \times h_{op} \times 3\,600 \text{ s/h}}{t_{Zyklus}} \quad (\text{C.2})$$

mit folgenden Annahmen, die in Bezug zur Anwendung des Bauteils getroffen worden sind:

h_{op} ist die mittlere Betriebszeit in Stunden je Tag;

d_{op} ist die mittlere Betriebszeit in Tagen je Jahr;

t_{Zyklus} ist die mittlere Zeit zwischen dem Beginn zweier aufeinander folgenden Zyklen des Bauteils (z. B. Schalten eines Ventils) in Sekunden je Zyklus.

Die Betriebszeit des Bauteils ist begrenzt auf T_{10d} , die mittlere Zeit bis 10 % der Bauteile gefährlich ausfallen.

$$T_{10d} = \frac{B_{10d}}{n_{op}} \quad (\text{C.3})$$

ANMERKUNG Erläuterung der Gleichungen in C.4.2.

B_{10d} , die mittlere Anzahl von Zyklen, bis 10 % der Bauteile gefährlich ausgefallen sind, kann zu T_{10d} , der Zeit, bis 10 % der Bauteile gefährlich ausgefallen sind, umgewandelt werden, durch Verwendung von n_{op} , der mittleren Anzahl jährlicher Betätigungen:

$$T_{10d} = \frac{B_{10d}}{n_{op}} \quad (\text{C.4})$$

Die Verfahren der Zuverlässigkeit in diesem Teil der ISO 13849 setzen voraus, dass die Ausfälle von Bauteilen exponentiell über der Zeit verteilt sind: $F(t) = 1 - \exp(-\lambda_d t)$. Bei pneumatischen und elektromechanischen Bauteilen ist eine Weibull-Verteilung wahrscheinlicher. Wenn aber die Betriebszeit der Bauteile auf die mittlere Zeit bis 10 % der Bauteile gefährlich ausfallen (T_{10d}) begrenzt wird, kann eine konstante gefahrbringende Ausfallrate (λ_d) während dieser Gebrauchsdauer wie folgt abgeschätzt werden:

$$\lambda_d \approx \frac{0,1}{T_{10d}} = \frac{0,1 \times n_{op}}{B_{10d}} \quad (\text{C.5})$$

Diese Gleichung (C.5) berücksichtigt, dass mit einer konstanten Ausfallrate 10 % der Bauteile in der angenommenen Anwendung nach T_{10d} [Jahre], ausfallen, entsprechend nach B_{10d} [Zyklen]. Um exakt zu sein:

$$F(T_{10d}) = 1 - \exp(-\lambda_d T_{10d}) = 10 \% \text{ bedeutet } \lambda_d = -\frac{\ln(0,9)}{T_{10d}} = \frac{0,105\,36}{T_{10d}} \approx \frac{0,1}{T_{10d}} \quad (\text{C.6})$$

Mit $MTTF_d = 1/\lambda_d$ für eine exponentielle Verteilung ergibt dies

$$MTTF_d = \frac{T_{10d}}{0,1} = \frac{B_{10d}}{0,1 \times n_{op}} \quad (\text{C.7})$$

C.4.3 Beispiel

Für ein Pneumatikventil gibt ein Hersteller eine mittlere Anzahl von 60 Millionen Schaltspielen als B_{10d} an. Das Ventil wird an zwei Schichten je Tag mit 220 Arbeitstagen je Jahr verwendet. Die mittlere Zeit zwischen dem Beginn zweier aufeinander folgender Schaltspiele des Ventils wird mit 5 s angenommen. Dies führt zu folgenden Werten:

- d_{op} von 220 Tagen je Jahr;
- h_{op} von 16 h je Tag;
- t_{Zyklus} von 5 s je Zyklus;
- B_{10d} von 60 Millionen Zyklen.

Mit diesen Eingangsdaten können die folgenden Werte berechnet werden:

$$n_{op} = \frac{220 \text{ Tage/Jahr} \times 16 \text{ h/Tag} \times 3\,600 \text{ s/h}}{5 \text{ s/Zyklen}} = 2,53 \times 10^6 \text{ Zyklen/Jahr} \quad (\text{C.8})$$

$$T_{10d} = \frac{60 \times 10^6 \text{ Zyklen}}{2,53 \times 10^6 \text{ Zyklen/Jahr}} = 23,7 \text{ Jahre} \quad (\text{C.9})$$

$$\text{MTTF}_d = \frac{23,7 \text{ Jahre}}{0,1} = 237 \text{ Jahre} \quad (\text{C.10})$$

Dies ergibt eine MTTF_d für das Bauteil von „hoch“ nach Tabelle 5. Diese Annahmen gelten nur für eine eingeschränkte Betriebsdauer von 23,7 Jahren für das Ventil.

C.5 MTTF_d -Daten elektrischer Bauteile

C.5.1 Allgemeines

Tabellen C.2 bis C.7 zeigen einige typische Durchschnittswerte von MTTF_d für elektronische Bauteile. Die Daten wurden der Datenbank SN 29500 Serie [40] entnommen. Alle Daten sind allgemeiner Art. Verschiedene Datenbanken sind verfügbar (siehe die unvollständige Liste in den Literaturhinweisen), die MTTF_d -Werte für verschiedene elektronische Bauteile enthalten. Wenn der Konstrukteur eines SRP/CS andere verlässliche spezifische Daten der verwendeten Bauteile hat, dann wird dringend empfohlen, diese speziellen Daten anstelle der anderen zu verwenden.

Die in den Tabellen C.2 bis C.7 angegebenen Werte sind gültig für eine Temperatur von 40 °C, Nennbelastung für Strom und Spannung.

In der MTTF -Spalte der Tabellen sind die Werte aus SN 29500 für allgemeine Bauteile für alle möglichen Ausfallarten gezeigt, die nicht notwendigerweise gefahrbringende Ausfälle sind. In der MTTF_d -Spalte wird üblicherweise angenommen, dass nicht alle Ausfallarten zu gefahrbringenden Ausfällen führen. Dies hängt hauptsächlich von der Anwendung ab. Ein genauer Weg der Bestimmung der „typischen“ MTTF_d für Bauteile ist die Durchführung einer FMEA. Einige Bauteile, z. B. Transistoren als Schalter verwendet, können Kurzschlüsse oder Unterbrechungen als Ausfall haben. Nur eine der beiden Arten kann gefährlich sein; deshalb nimmt die Spalte „Bemerkungen“ nur 50 % als gefahrbringende Ausfälle an, was bedeutet, dass die MTTF_d für Bauteile die Doppelte des gegebenen MTTF -Werts ist. Für die Anwendung in Zweifelsfällen ist für die Bauteile eine ungünstigste MTTF_d in der Spalte „ungünstigster Fall“ angegeben, wobei der Sicherheitsfaktor 10 beträgt.

EN ISO 13849-1:2008 (D)**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 _d für Bauteile Jahre		Bemerkungen
			typisch	ungünstigster Fall	
Bipolar	TO18, TO92, SOT23	34 247	68 493	6 849	50 % gefahrbringende Ausfälle
Bipolar, niedrige Leistung	TO5, TO39	5 708	11 416	1 142	50 % gefahrbringende Ausfälle
Bipolar, Leistung	TO3, TO220, D-Pack	1 941	3 881	388	50 % gefahrbringende Ausfälle
FET	Junction MOS	22 831	45 662	4 566	50 % gefahrbringende Ausfälle
MOS, Leistung	TO3, TO220, D-Pack	1 142	2 283	228	50 % gefahrbringende Ausfälle

Tabelle C.3 — Dioden, Leistungshalbleiter und integrierte Schaltungen

Diode	Beispiel	MTTF für Bauteile Jahre	MTTF _d für Bauteile Jahre		Bemerkungen
			typisch	ungünstigster Fall	
Allgemeine Anwendung	—	114 155	228 311	22 831	50 % gefahrbringende Ausfälle
Entstörgerät	—	15 981	31 963	3 196	50 % gefahrbringende Ausfälle
Zenerdiode $P_{\text{tot}} < 1 \text{ W}$	—	114 155	228 311	22 831	50 % gefahrbringende Ausfälle
Gleichrichterdioden	—	57 078	114 155	11 416	50 % gefahrbringende Ausfälle
Gleichrichterbrücken	—	11 415	22 831	2 283	50 % gefahrbringende Ausfälle
Thyristoren	—	2 283	4 566	457	50 % gefahrbringende Ausfälle
Triacs, Diacs	—	1 484	2 968	297	50 % gefahrbringende Ausfälle
Integrierte Schaltungen (programmierbar und nicht programmierbar)	Herstellerdaten verwenden				50 % gefahrbringende Ausfälle

C.6 Passive Bauteile

Siehe Tabellen C.4 bis C.7.

Tabelle C.4 — Kondensatoren

Kondensator	Beispiel	MTTF für Bauteile Jahre	MTTF _d für Bauteile Jahre		Bemerkungen
			typisch	ungünstigster Fall	
Standard, keine Leistung	KS, KP, KC, KT, MKT, MKC, MKP, MKU, MP, MKV	57 078	114 155	11 416	50 % gefahrbringende Ausfälle
Keramik	—	22 831	45 662	4 566	50 % gefahrbringende Ausfälle
Aluminiumelektrolyt	flüssiges Elektrolyt	22 831	45 662	4 566	50 % gefahrbringende Ausfälle
Aluminiumelektrolyt	festes Elektrolyt	37 671	75 342	7 534	50 % gefahrbringende Ausfälle
Tantalelektrolyt	flüssiges Elektrolyt	11 415	22 831	2 283	50 % gefahrbringende Ausfälle
Tantalelektrolyt	festes Elektrolyt	114 155	228 311	22 831	50 % gefahrbringende Ausfälle

Tabelle C.5 — Widerstände

Widerstand	Beispiel	MTTF für Bauteile Jahre	MTTF _d für Bauteile Jahre		Bemerkungen
			typisch	ungünstigster Fall	
Kohleschicht	—	114 155	228 311	22 831	50 % gefahrbringende Ausfälle
Metallfilm	—	570 776	1 141 552	114 155	50 % gefahrbringende Ausfälle
Metalloxyd und gewendelt	—	22 831	45 662	4 566	50 % gefahrbringende Ausfälle
Variabel	—	3 767	7 534	753	50 % gefahrbringende Ausfälle

EN ISO 13849-1:2008 (D)

Tabelle C.6 — Induktivitäten

Induktivität	Beispiel	MTTF für Bauteile Jahre	MTTF _d für Bauteile Jahre		Bemerkungen
			typisch	ungünstigster Fall	
Für MC-Anwendung	—	37 671	75 342	7 534	50 % gefahrbringende Ausfälle
Niederfrequenz-Induktivitäten und Transformatoren	—	22 831	45 662	4 566	50 % gefahrbringende Ausfälle
Leistungstransformatoren und Transformatoren für Schaltanwendungen und Netzteile	—	11 415	22 831	2 283	50 % gefahrbringende Ausfälle

Tabelle C.7 — Optokoppler

Optokoppler	Beispiel	MTTF für Bauteile Jahre	MTTF _d für Bauteile Jahre		Bemerkungen
			typisch	ungünstigster Fall	
Biopolar Ausgang	SFH 610	7 648	15 296	1 530	50 % gefahrbringende Ausfälle
FET Ausgang	LH 1056	2 854	5 708	571	50 % gefahrbringende Ausfälle

Anhang D (informativ)

Vereinfachtes Verfahren zur Bestimmung der $MTTF_d$ für jeden Kanal

D.1 „Parts-Count“-Verfahren

Das „Parts-Count“-Verfahren hilft bei der getrennten Bestimmung der $MTTF_d$ für jeden Kanal. Die $MTTF_d$ -Werte aller einzelnen Bauteile eines Kanals werden für diese Berechnung verwendet⁴⁾.

Die allgemeine Gleichung ist

$$\frac{1}{MTTF_d} = \sum_{i=1}^{\tilde{N}} \frac{1}{MTTF_{di}} = \sum_{j=1}^{\tilde{N}} \frac{n_j}{MTTF_{dj}} \quad (D.1)$$

wobei

$MTTF_d$ für den gesamten Kanal gilt

$MTTF_{di}$, $MTTF_{dj}$ ist die $MTTF_d$ jedes Bauteils, welches zur Sicherheitsfunktion beiträgt.

Die erste Summe wird über alle Bauteile getrennt gebildet; die zweite Summe ist gleichwertig aber vereinfacht, wobei alle n_j -identischen Bauteile mit der gleichen $MTTF_{dj}$ zusammengefasst werden.

Das in Tabelle D.1 gegebene Beispiel ergibt eine $MTTF_d$ des Kanals von 21,4 Jahren, was „mittel“ nach Tabelle 5 entspricht.

Tabelle D.1 — Beispiel der Teileliste auf einer Platine

<i>j</i>	Bauteil	Anzahl n_j	$MTTF_{dj}$ ungünstigster Fall Jahre	$1/MTTF_{dj}$ ungünstigster Fall 1/Jahr	$n_j/MTTF_{dj}$ ungünstigster Fall 1/Jahr
1	Transistoren, Bipolar, Kleinleistung (siehe Tabelle C.2)	2	1 142	0,000 876	0,001 752
2	Widerstand, Kohlefilm (siehe Tabelle C.5)	5	22 831	0,000 044	0,000 219
3	Kondensator, Standard, keine Leistung (siehe Tabelle C.4)	4	11 416	0,000 088	0,000 350
4	Relais (mit kleiner Last, siehe C.2) ($B_{10d} = 20\,000\,000$ Zyklen, $n_{op} = 633\,600$)	4	315,66	0,003 168	0,012 672
5	Schütz (mit nomineller Last, siehe C.2) ($B_{10d} = 2\,000\,000$ Zyklen, $n_{op} = 633\,600$)	1	31,57	0,031 676	0,031 676
$\Sigma(n_j/MTTF_{dj})$					0,046 669
$MTTF_d = 1/\Sigma(n_j/MTTF_{dj})$ [Jahre]		21,43			

4) Das „Parts-Count“-Verfahren ist eine Annäherung, deren Abweichung immer zur sicheren Seite geht. Wenn genauere Werte erforderlich sind, dann sollte der Konstrukteur die Ausfallarten berücksichtigen, was jedoch sehr kompliziert sein kann.

EN ISO 13849-1:2008 (D)

ANMERKUNG 1 Dieses Verfahren basiert auf der Annahme, dass ein gefährlicher Ausfall irgendeines Bauteils im Kanal zu einem gefährlichen Ausfall des Kanals führt. Die $MTTF_d$ -Berechnung der Tabelle D.1 basiert auf diese Annahme.

ANMERKUNG 2 In diesem Beispiel kommt der Haupteinfluss vom Schütz. Die gewählten Werte für $MTTF_d$ und B_{10d} in diesem Beispiel basieren auf dem Anhang C. Für das Beispiel werden $d_{op} = 220$ Tage/Jahr, $h_{op} = 8$ h/Tag und $f_{zyklus} = 10$ s/Zyklus angenommen, das ergibt $n_{op} = 633\,600$ Zyklen/Jahr. Im Allgemeinen wird die Wahl der Herstellerdaten für $MTTF_d$ und B_{10d} zu viel besseren Ergebnissen führen, also zu einem höheren $MTTF_d$ des Kanals.

D.2 Die $MTTF_d$ für unterschiedliche Kanäle, Symmetrisierung der $MTTF_d$ für jeden Kanal

Die vorgesehenen Architekturen in 6.2 gehen davon aus, dass in einem redundanten SRP/CS die Werte für $MTTF_d$ für jeden Kanal gleich sind. Dieser Wert je Kanal sollte die Eingangsgröße für Bild 5 sein.

Wenn die $MTTF_d$ der Kanäle unterschiedlich sind, gibt es zwei Möglichkeiten:

- als eine Annahme für den ungünstigsten Fall sollte der kleinere Wert in Betracht gezogen werden oder;
- Gleichung D.2 kann zur Einschätzung eines Ersatzwertes für $MTTF_d$ für jeden Kanal verwendet werden:

$$MTTF_d = \frac{2}{3} \left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}} \right] \quad (D.2)$$

wobei $MTTF_{dC1}$ und $MTTF_{dC2}$ die Werte für zwei unterschiedliche redundante Kanäle sind.

BEISPIEL Ein Kanal hat die $MTTF_{dC1} = 3$ Jahre, der andere Kanal hat eine $MTTF_{dC2} = 100$ Jahre, dann ist das Ergebnis $MTTF_d = 66$ Jahre für jeden Kanal. Das bedeutet, dass ein redundantes System mit einer $MTTF_d$ von 100 Jahren in einem Kanal und einer $MTTF_d$ von 3 Jahren im anderen Kanal gleichwertig ist zu einem System mit einer $MTTF_d$ von 66 Jahren in jedem Kanal.

Ein redundantes System mit zwei Kanälen und unterschiedlichen $MTTF_d$ -Werten jedes Kanals kann unter Verwendung der obigen Gleichung durch ein redundantes System mit identischen $MTTF_d$ -Werten für jeden Kanal ersetzt werden. Dieses Verfahren ist notwendig, um Bild 5 richtig anwenden zu können.

ANMERKUNG Dieses Verfahren setzt unabhängige, parallele Kanäle voraus.

Anhang E (informativ)

Abschätzungen des Diagnosedeckungsgrades (DC) für Funktionen und Module

E.1 Beispiele für den Diagnosedeckungsgrad (DC)

Siehe Tabelle E.1

Tabelle E.1 — Abschätzungen des Diagnosedeckungsgrades (DC)

Maßnahme	DC
Eingabeeinheit	
Zyklischer Testimpuls durch dynamische Änderung der Eingangssignale	90 %
Plausibilitätsprüfung, z. B. Verwendung der Schließer- und Öffnerkontakte von zwangsgeführten Relais	99 %
Kreuzvergleich von Eingangssignalen ohne dynamischem Test	0 % bis 99 %, abhängig davon, wie oft ein Signalwechsel durch die Anwendung erfolgt
Kreuzvergleich von Eingangssignalen mit dynamischem Test, wenn Kurzschlüsse nicht bemerkt werden können (bei Mehrfach-Ein-/Ausgängen)	90 %
Kreuzvergleich von Eingangssignalen mit unmittelbarem und Zwischenergebnissen in der Logik (L) und zeitlich und logische Programmlaufüberwachung und Erkennung statischer Ausfälle und Kurzschlüsse (bei Mehrfach-Ein-/Ausgängen)	99 %
Indirekte Überwachung (z. B. Überwachung durch Druckschalter, elektrische Positionsüberwachung von Antriebselementen)	90 % bis 99 %, abhängig von der Anwendung
Direkte Überwachung (z. B. elektrische Stellungsüberwachung der Steuerungsventile, Überwachung elektromechanischer Einheiten durch Zwangsführung)	99 %
Fehlererkennung durch den Prozess	0 % bis 99 %, abhängig von der Anwendung; diese Maßnahme ist allein nicht ausreichend für den erforderlichen Performance Level „e“!
Überwachung einiger Merkmale des Sensors (Ansprechzeit, der Bereich analoger Signale, z. B. elektrischer Widerstand, Kapazität)	60 %

EN ISO 13849-1:2008 (D)

Tabelle E.1 (fortgesetzt)

Maßnahme	DC
Logik	
Indirekte Überwachung (z. B. Überwachung durch Druckschalter, elektrische Positionsüberwachung von Antriebselementen)	90 % bis 99 %, abhängig von der Anwendung
Direkte Überwachung (z. B. elektrische Überwachung der Steuerungsventile, Überwachung elektromechanischer Einheiten durch Zwangsführung)	99 %
Einfache zeitliche Programmlaufüberwachung (z. B. Zeitglied als Watchdog, mit Triggersignalen im Programm der Logik)	60 %
Zeitliche und logische Programmlaufüberwachung durch den Watchdog, wobei die Testeinrichtung Plausibilitätstests des Verhaltens der Logik durchführt	90 %
Selbsttest bei Anlauf, um verborgene Fehler in Teilen der Logik zu finden (z. B. Programm- und Datenspeicher, Eingangs-/Ausgangsanschlüsse, Schnittstellen)	90 %, (abhängig von der Testausführung)
Testung der Reaktionsmöglichkeit der Überwachungseinrichtung (z. B. Watchdog) durch den Hauptkanal nach Anlauf, oder wann immer die Sicherheitsfunktion angefordert wird, oder wann immer ein externes Signal dies durch eine Eingangseinrichtung anfordert	90 %
Dynamische Prinzipien (alle Bauteile der Logik erfordern eine Zustandsänderung EIN-AUS-EIN, wenn die Sicherheitsfunktion angefordert wird), z. B. Verriegelungsschaltungen in Relais-technik	99 %
Invarianter Speicher: Signatur einfacher Wortbreite (8 Bit)	90 %
Invarianter Speicher: Signatur doppelter Wortbreite (16 Bit)	99 %
Varianter Speicher: RAM-Test durch Verwendung redundanter Daten, z. B. Flags, Merker, Konstanten, Timer, und Kreuzvergleich dieser Daten	60 %
Varianter Speicher: Test der Lesbarkeit und der Beschreibbarkeit der verwendeten Speicherzellen	60 %
Varianter Speicher: RAM-Überwachung mit modifiziertem Hammingcode oder RAM-Selbsttest (z. B. „Galpat“ oder „Abraham“)	99 %
Verarbeitungseinheit: Selbsttest durch Software	60 % bis 90 %
Verarbeitungseinheit: Kodierte Verarbeitung	90 % bis 99 %
Fehlererkennung durch den Prozess	0 % bis 99 %, abhängig von der Anwendung; diese Maßnahme ist allein nicht ausreichend für den erforderlichen Performance Level „e“!
Ausgabeeinheiten	
Überwachung der Ausgänge durch einen Kanal ohne dynamischen Test	0 % bis 99 %, abhängig davon, wie oft ein Signalwechsel durch die Anwendung erfolgt
Kreuzvergleich von Ausgangssignalen ohne dynamischem Test	0 % bis 99 %, abhängig davon, wie oft ein Signalwechsel durch die Anwendung erfolgt
Kreuzvergleich von Ausgangssignalen mit dynamischem Test, ohne Erkennung von Kurzschlüssen (bei Mehrfach-Ein-/Ausgängen)	90 %
Kreuzvergleich von Ausgangssignalen mit unmittelbarem Ergebnis in der Logik (L) und zeitlich und logischer Softwareüberwachung des Programmablaufs und Erkennen statischer Ausfälle und Kurzschlüsse (bei Mehrfach-Ein-/Ausgängen)	99 %

Tabelle E.1 (fortgesetzt)

Maßnahme	DC
Redundanter Abschaltpfad ohne Überwachung des Antriebselements	0 %
Redundanter Abschaltpfad mit Überwachung eines der Antriebselemente entweder durch die Logik oder durch eine Testeinrichtung	90 %
Redundanter Abschaltpfad mit Überwachung der Antriebselemente durch die Logik und Testeinrichtung	99 %
Indirekte Überwachung (z. B. Überwachung durch Druckschalter, elektrische Positionsüberwachung von Aktoren)	90 % bis 99 %, abhängig von der Anwendung
Fehlererkennung durch den Prozess	0 % bis 99 %, abhängig von der Anwendung; diese Maßnahme ist allein nicht ausreichend für den erforderlichen Performance Level „e“!
Direkte Überwachung (z. B. elektrische Überwachung der Steuerungsventile, Überwachung elektromechanischer Einheiten durch Zwangsführung)	99 %
ANMERKUNG 1 Für weitere Abschätzungen des DC, siehe z.B. IEC 61508-2:2000, Tabellen A.2 bis A.15.	
ANMERKUNG 2 Wenn mittel oder hoch als DC für die Logik gefordert wird, ist mindestens eine Maßnahme für varianten, invarianten Speicher und Verarbeitungseinheit, mit mindestens je 60 % zu wählen. Es können auch andere Maßnahmen als die in dieser Tabelle aufgelisteten verwendet werden.	

E.2 Abschätzung des durchschnittlichen DC (DC_{avg})

In vielen Systemen könnten mehrere Maßnahmen zur Fehlererkennung verwendet werden. Diese Maßnahmen könnten unterschiedliche Teile der SRP/CS testen und haben unterschiedliche DC. Zur Einschätzung des PL nach Bild 5 ist nur eine durchschnittliche DC für die gesamten SRP/CS, die die Sicherheitsfunktion ausführen, anwendbar.

Die DC kann bestimmt werden als das Verhältnis zwischen der Ausfallrate von erkannten gefahrbringenden Ausfällen und der Ausfallrate aller gefahrbringenden Ausfälle. Nach dieser Definition wird der durchschnittliche Diagnosedegrad DC_{avg} mit folgender Gleichung abgeschätzt:

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \dots + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \dots + \frac{1}{MTTF_{dN}}} \quad (E.1)$$

Hierbei sind alle Bauteile des SRP/CS ohne Fehlerausschluss zu berücksichtigen und aufzusummieren. Für jeden Block werden die $MTTF_d$ und der DC berücksichtigt. DC in dieser Gleichung bedeutet das Verhältnis der Ausfallrate erkannter gefahrbringender Ausfälle des Teils (ungeachtet der Maßnahmen, durch die die Ausfälle erkannt werden) zur Ausfallrate aller gefahrbringender Ausfälle des Teils. Somit bezieht sich der DC auf die getesteten Teile und nicht auf die Testeinrichtung. Bauteile ohne Ausfallerkennung (z. B. die nicht getestet werden) haben einen DC = 0 und tragen nur zum Nenner des DC_{avg} bei.

Anhang F (informativ)

Abschätzungen der Ausfälle aufgrund gemeinsamer Ursache (CCF)

F.1 Anforderungen an CCF

Ein umfassendes Verfahren zu Maßnahmen gegen CCF für Sensoren/Antriebsselemente und besonders für Steuerelektroniken wird z. B. in IEC 61508-6:2001, Anhang D gegeben. Nicht alle Maßnahmen, die darin gegeben werden, sind für den Maschinenbereich geeignet. Hier werden die wichtigsten Maßnahmen angegeben.

ANMERKUNG In diesem Teil der ISO 13849 wird angenommen, dass für redundante Systeme der β -Faktor nach IEC 61508-6:2000, Anhang D kleiner oder gleich 2 % ist.

F.2 Abschätzung der Auswirkung des CCF

Dieser quantitative Prozess sollte für das gesamte System angewendet werden. Jedes Teil der sicherheitsbezogenen Teile der Steuerung sollte berücksichtigt werden.

Die Tabelle F.1 listet Maßnahmen und enthält zugehörige Werte, basierend auf einer ingenieurmäßigen Beurteilung, die den Beitrag jeder Maßnahme zur Reduzierung der Ausfälle infolge gemeinsamer Ursache repräsentieren.

Für jede der gelisteten Maßnahmen kann nur die volle Punktezahl oder nichts beansprucht werden. Wird eine Maßnahme nur teilweise erfüllt, ist die entsprechende Punktezahl null.

Tabelle F.1 enthält eine Quantifizierung des CCF.

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

Nr	Maßnahme gegen CCF	Punktezahl
1	Trennung/Abtrennung	
	Physikalische Trennung zwischen den Signalpfaden: Trennung der Verdrahtung/Verrohrung, ausreichende Luft- und Kriechstrecken auf gedruckten Schaltungen.	15
2	Diversität	
	Unterschiedliche Technologien/Gestaltung oder physikalische Prinzipien werden verwendet, z. B.: der erste Kanal in programmierbarer Elektronik und der zweite Kanal fest verdrahtet, Art der Initiierung, Druck und Temperatur, Messung von Entfernung und Druck, digital und analog, Bauteile von unterschiedlichen Herstellern.	20
3	Entwurf/Anwendung/Erfahrung	
3.1	Schutz gegen Überspannung, Überdruck, Überstrom usw.	15
3.2	Verwendung bewährter Bauteile.	5
4	Beurteilung/Analyse	
	Sind die Ergebnisse einer Ausfallart und Effektanalyse berücksichtigt worden, um Ausfälle infolge gemeinsamer Ursache in der Entwicklung zu vermeiden?	5
5	Kompetenz/Ausbildung	
	Sind Konstrukteure/Monteure geschult worden, um die Gründe und Auswirkungen von Ausfällen infolge gemeinsamer Ursache zu erkennen?	5
6	Umgebung	
6.1	Schutz vor Verunreinigung und elektromagnetischer Beeinflussung (EMC) gegen CCF in Übereinstimmung mit den angemessenen Normen. 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. Elektrische Systeme: Wurde das System hinsichtlich elektromagnetischer Immunität geprüft, z. B. wie in zutreffenden Normen gegen CCF festgelegt? Bei kombinierten fluidischen und elektrischen Systemen sollten beide Aspekte berücksichtigt werden.	25
6.2	Andere Einflüsse Wurden alle Anforderungen hinsichtlich Unempfindlichkeit gegenüber allen relevanten Umgebungsbedingungen wie Temperatur, Schock, Vibration, Feuchte (z. B. wie in den zutreffenden Normen festgelegt) berücksichtigt?	10
	Gesamt	[max. erreichbar 100]
Gesamtpunkte		Maßnahmen, um CCF zu vermeiden ^a
65 oder besser		Anforderungen erreicht
kleiner als 65		Verfahren gescheitert ⇒ Auswahl zusätzlicher Maßnahmen
^a Wenn technische Maßnahmen nicht relevant sind, können die Punkte der rechten Spalte bei der ausführlichen Berechnung berücksichtigt werden.		

Anhang G (informativ)

Systematischer Ausfall

G.1 Allgemeines

ISO 13849-2 liefert eine umfassende Liste mit Maßnahmen gegen den systematischen Ausfall, die angewendet werden sollten, wie grundlegende Sicherheitsprinzipien und bewährte Sicherheitsprinzipien.

G.2 Maßnahmen zur Beherrschung systematischer Ausfälle

Die folgenden Maßnahmen sollten angewendet werden.

- Anwendung der Energieabschaltung (siehe ISO 13849-2)

Die sicherheitsbezogenen Teile der Steuerung (SRP/CS) sollten so gestaltet werden, dass mit Verlust der elektrischen Versorgung der sichere Zustand der Maschine erreicht oder aufrechterhalten werden kann.

- Maßnahmen, um die Auswirkungen von Spannungsausfall, Spannungsschwankungen, Überspannung und Unterspannung zu beherrschen

Das Verhalten der SRP/CS als Reaktion aufgrund der Bedingungen von Spannungsausfall, Spannungsschwankungen, Überspannung und Unterspannung sollten vorher bestimmt werden, sodass die SRP/CS den sicheren Zustand der Maschine erreichen oder aufrechterhalten kann (siehe auch IEC 60204-1 und IEC 61508-7:2000, A.8).

- Maßnahmen, um die Wirkungen physikalischer Umgebungsbedingungen (z. B. Temperatur, Feuchte, Wasser, Vibration, Staub, korrosive Substanzen, elektromagnetische Beeinflussung und deren Wirkungen) zu beherrschen oder zu verhindern

Das Verhalten der SRP/CS als Reaktion auf die Wirkungen der physikalischen Umgebungsbedingungen, sollte vorher bestimmt werden, sodass die SRP/CS den sicheren Zustand der Maschine erreichen oder aufrechterhalten können (siehe auch z. B. IEC 60529, IEC 60204-1).

- Für SRP/CS, die Software enthalten, muss eine Überwachung des Programmablaufs verwendet werden, um fehlerhafte Programmabläufe zu erkennen

Ein fehlerhafter Programmablauf liegt vor, wenn die einzelnen Elemente eines Programms (z. B. Softwaremodule, Unterprogramme oder Anweisungen) in der falschen Reihenfolge oder im falschen Zeitablauf bearbeitet werden oder wenn der Takt des Prozessors fehlerhaft ist (siehe EN 61508-7:2001, A.9).

- Maßnahmen, um die Auswirkungen von Abweichungen und anderer Auswirkungen, verursacht durch irgendeinen Datenkommunikationsprozess, zu beherrschen (siehe IEC 61508-2:2000, 7.4.8).

Zusätzlich sollten eine oder mehrere der folgenden Maßnahmen unter Berücksichtigung der Komplexität der SRP/CS und deren PL angewendet werden:

- Ausfallerkennung durch automatische Tests;
- Testung durch redundante Hardware;

- diversitäre Hardware;
- Betreiben im Ruhestromprinzip;
- zwangsgeführte Kontakte;
- zwangsöffnende Kontakte;
- ausfallorientierter Betrieb;
- Überdimensionierung mit einem angemessenen Faktor, wo der Hersteller zeigen kann, dass Unterbeanspruchung die Zuverlässigkeit erhöht wo eine Überdimensionierung geeignet ist, sollte ein Überdimensionierungs-Faktor von mindestens 1,5 verwendet werden.

Siehe auch ISO 13849-2:2002, D.3.

G.3 Maßnahmen zur Vermeidung systematischer Ausfälle

Die folgenden Maßnahmen sollten angewendet werden.

- Verwenden angemessener Materialien und geeignete Herstellung
Auswahl des Materials, Herstellungsverfahren und Behandlung in Bezug auf z. B. Belastung, Haltbarkeit, Elastizität, Reibung, Abnutzung, Korrosion, Temperatur, Leitfähigkeit, dielektrischer Festigkeit.
- Richtige Dimensionierung und Formgebung
Berücksichtigen von z. B. Belastung, Dehnung, Ermüdung, Temperatur, Oberflächenrauheit, Toleranzen, Verarbeitung.
- Richtige Auswahl, Kombination, Anordnung, Zusammenbau und Installation der Bauteile, einschließlich Verkabelung, Leitungsführung und Verbindungen
Anwenden geeigneter Normen und Herstellerhinweise zur Anwendung, z. B. Katalogblätter, Montageanweisungen, Spezifikationen und Anwendung guter technischer Erfahrung.
- Kompatibilität
Verwenden von Bauteilen mit kompatiblen Betriebskenndaten.
- Festigkeit gegen die festgelegten Umgebungsbedingungen
Gestalten des SRP/CS in der Form, dass es in der Lage ist, unter allen erwarteten Umgebungsbedingungen und vorhersehbaren widrigen Bedingungen, z. B. Temperatur, Feuchte, Schwingungen und elektromagnetischer Beeinflussung (EMI), zu arbeiten (siehe ISO 13849-2:2002, D.2).
- Verwendung von Bauteilen, die nach einer geeigneten Norm gebaut wurden und deren Ausfallarten eindeutig definiert sind
Vermindern des Risikos unerkannter Fehler durch Verwendung von Bauteilen mit speziellen Eigenschaften (siehe IEC 61508-7:2000, B.3.3).

EN ISO 13849-1:2008 (D)

Zusätzlich sollten eine oder mehrere der folgenden Maßnahmen, unter Berücksichtigung der Komplexität des SRP/CS und dessen PL, angewendet werden.

- Hardware-Gestaltungsüberprüfung (z. B. Inspektion oder Walk-through)

Durch Überprüfungen und Analyse Unstimmigkeiten zwischen der Spezifikation und Realisierung aufzuzeigen (siehe IEC 61508-7:2000, B.3.7 und B.3.8).

- Rechnergestützte Entwurfswerkzeuge, die in der Lage sind, zu simulieren oder zu analysieren

Systematisches Durchführen der Gestaltung und Einbeziehen geeigneter automatischer Konstruktionselemente, die bereits verfügbar und getestet sind (siehe IEC 61508-7:2000, B.3.5).

- Simulation

Systematisches und vollständiges Durchführen einer Inspektion der Gestaltung des SRP/CS im Hinblick auf beides, der funktionalen Leistung und der richtigen Dimensionierung ihrer Bauteile (siehe IEC 61508-7:2000, B.3.6).

G.4 Maßnahmen zur Vermeidung systematischer Ausfälle während der Integration des SRP/CS

Die folgenden Maßnahmen während der Integration des SRP/CS sollten angewendet werden:

- Funktionsprüfung;
- Projektmanagement;
- Dokumentation.

Zusätzlich sollte der Black-Box-Test unter Berücksichtigung der Komplexität der SRP/CS und deren PL angewendet werden.

Anhang H (informativ)

Beispiel der Kombination von verschiedenen sicherheitsbezogenen Teilen einer Steuerung

Bild H.1 zeigt eine schematische Darstellung sicherheitsbezogener Teile zur Bereitstellung einer der Funktionen, um das Maschinen-Antriebselement anzusteuern. Dies ist kein Funktionsschaltbild/Arbeitsdiagramm und wird nur gezeigt, um das Prinzip der Zusammenschaltung der Kategorien und Technologien in einer Funktion zu zeigen.

Die Steuerung erfolgt durch eine elektronische Steuerung und ein Wegeventil. Das Risiko wird durch eine AOPD vermindert, die den Zugang zur Gefährdungssituation erkennt und den Anlauf des hydraulischen Antriebselements verhindert, wenn der Lichtstrahl unterbrochen ist.

Die sicherheitsbezogenen Teile, welche die Sicherheitsfunktion bereitstellen, sind: AOPD, elektronische Steuerung, hydraulisches Wegeventil und die Verbindungsmittel.

Diese kombinierten sicherheitsbezogenen Teile stellen eine Stoppfunktion als Sicherheitsfunktion zur Verfügung. Wenn die AOPD unterbrochen wird, liefern die Ausgänge ein Signal an die elektronische Steuerung, welche dem hydraulischen Wegeventil ein Signal bereitstellt, um den hydraulischen Durchfluss als Ausgang der SRP/CS zu stoppen. An der Maschine stoppt dies die gefahrbringende Bewegung des Antriebselements.

Diese Kombination sicherheitsbezogener Teile bildet eine Sicherheitsfunktion, um die Kombination verschiedener Kategorien und Technologien auf der Basis der Anforderungen von Abschnitt 6 zu zeigen. Unter Verwendung der Grundsätze dieses Teils der ISO 13849 können die sicherheitsbezogenen Teile aus Bild H.2 wie folgt beschrieben werden.

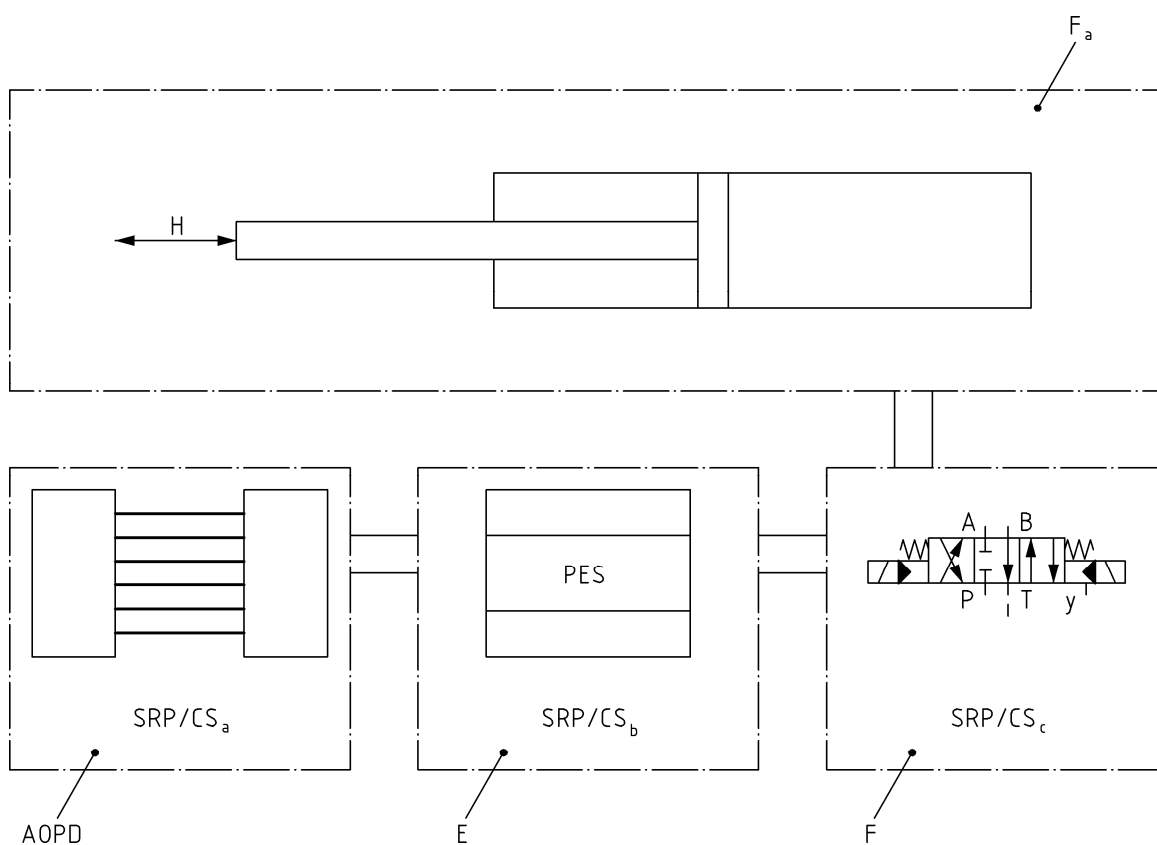
- Kategorie 2, $PL = c$ für die berührungslos wirkende Schutzeinrichtung (Lichtschranke). Um die Wahrscheinlichkeit von Fehlern zu vermindern, werden bewährte Sicherheitsprinzipien verwendet.
- Kategorie 3, $PL = d$ für die elektronische Steuerung. Um den Beitrag der elektronischen Steuerung zur Sicherheit zu erhöhen, ist die Struktur der SRP/CS redundant und enthält einige Fehlererkennungsmechanismen, sodass die meisten Einzelfehler erkannt werden.
- Kategorie 1, $PL = c$ für das Wegeventil. Der Status als bewährtes Bauteil ist überwiegend anwendungsbezogen. In diesem Beispiel wird das Ventil als bewährt angenommen. Um die Wahrscheinlichkeit von Fehlern in diesem Bauteil zu vermindern, besteht dieses aus bewährten Bauteilen, verwendet in bewährten Sicherheitsprinzipien, und alle Einsatzbedingungen wurden berücksichtigt (siehe 6.2.4).

ANMERKUNG 1 Die Lage, Größe und Anordnung der Verbindungsmittel wurden ebenfalls berücksichtigt.

Diese Kombination führt mit einem $PL_{\text{niedrig}} = c$ und $N_{\text{niedrig}} = 2$ zu einem Gesamt-Performance-Level von $PL = c$ (siehe 6.3).

ANMERKUNG 2 Im Fall eines Fehlers in den Teilen der Kategorie 1 oder Kategorie 2 des Bildes H.2 kann dies zum Verlust der Sicherheitsfunktion führen.

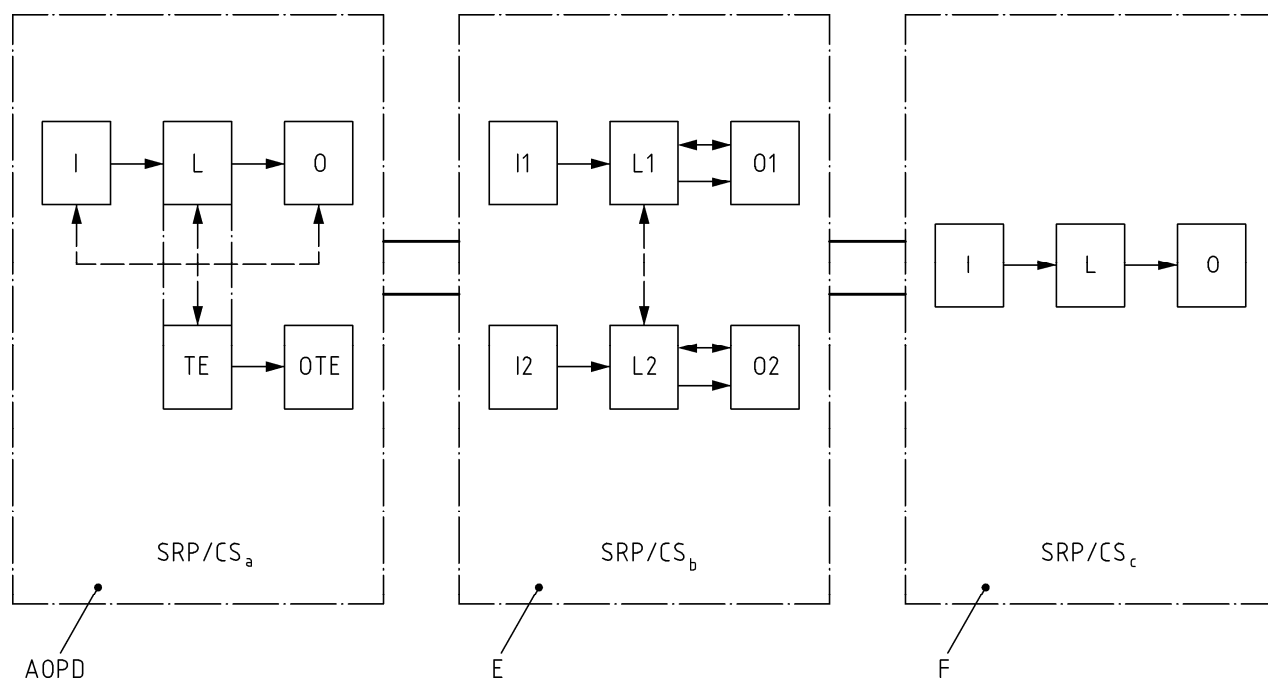
EN ISO 13849-1:2008 (D)



Legende

- AOPD aktive opto-elektronische Schutzeinrichtung (z. B. Lichtschranke), SRP/CS_a:
Kategorie 2 [Typ 2], PL = c
E elektronische Steuerungslogik, SRP/CS_b: Kategorie 3, PL = d
F Fluidtechnik, SRP/CS_c: Kategorie 1, PL = c
F_a fluidtechnischer Antrieb
H gefährbringende Bewegung

Bild H.1 — Beispiel – Blockdiagramm zur Erläuterung der Kombination von SRP/CS

**Legende**

AOPD	aktive opto-elektronische Schutzeinrichtung (z. B. Lichtschranke)
E	elektronische Steuerungslogik
F	fluidtechnischer Antrieb
I, I1, I2	Eingangselemente, z. B. Sensor
L, L1, L2	Logik
O, O1, O2, OTE	Ausgangselemente, z. B. Hauptschütz
TE	Testeinrichtung

Bild H.2 — Ersatz für Bild H.1 durch vorgesehene Architekturen

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 unterschiedliche Beispiele von Steuerstromkreisen A und B betrachtet, siehe Bilder I.1 und I.3. Beide zeigen die Leistungsfähigkeit der gleichen Sicherheitsfunktion der Verriegelung der trennenden Schutzeinrichtung. Das erste Beispiel ist einkanalig aus elektromechanischen Bauteilen mit hohen $MTTF_d$ -Werten aufgebaut, während das Zweite aus zwei Kanälen besteht — einem elektromechanischen und dem anderen in programmierbarer Elektronik — einschließlich Tests, aber bestehend aus Bauteilen mit niedriger $MTTF_d$.

I.2 Sicherheitsfunktion und erforderlicher Performance Level (PL_r)

Für beide Beispiele kann die Sicherheitsfunktion der Verriegelung einer trennenden Schutzeinrichtung wie folgt gewählt werden.

Die gefährliche Bewegung wird gestoppt, wenn die trennende Schutzeinrichtungen geöffnet wird (durch Abschalten der Energie des elektrischen Motors).

Die Risikoparameter nach dem Verfahren des Risikografs (siehe Bild A.1) sind die Folgenden:

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

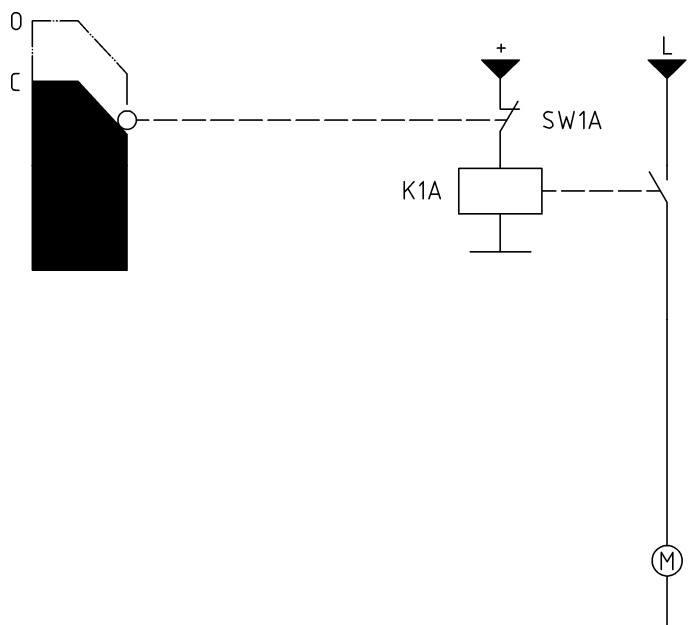
Diese Entscheidungen führen zu einem erforderlichen Performance Level PL_r von c.

Bestimmung der bevorzugten Kategorie: Ein Performance Level von c kann üblicherweise erreicht werden durch hochzuverlässige einkanalige Systeme (Kategorie 1) oder durch redundante Architekturen (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 beitragen, sind in Bild I.1 dargestellt. Funktionale Details, die nichts zur Sicherheitsfunktion der Verriegelung beitragen (wie Start- und Stopp-Schalter), sind weggelassen.



Legende

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

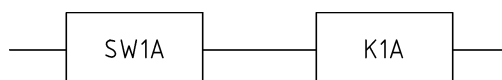
Bild I.1 — Schaltplan A zur Ausführung der Sicherheitsfunktion

In diesem Beispiel besitzt ein Türschalter Öffner-Kontakte (ohne begründeten Fehlerausschluss) und ist mit einem Hilfsschütz verbunden, das die Energiezuführung des Motors abschalten kann:

- ein Kanal mit elektromechanischen Bauteilen,
- der Schalter SW1A hat eine mittlere $MTTF_d$,
- das Hilfsschütz hat eine hohe $MTTF_d$.

Das gewählte Hilfsschütz in diesem Beispiel ist ein bewährtes Bauteil, wenn nach ISO 13849-2 implementiert.

Die sicherheitsbezogenen Teile und ihre Aufteilung in Kanäle kann so in einem sicherheitsbezogenen Blockdiagramm, wie in Bild I.2 gezeigt, dargestellt werden.



Legende

K1A	Hilfsschütz
SW1A	Schalter

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

EN ISO 13849-1:2008 (D)

I.3.2 Quantifizierung der $MTTF_d$ für jeden Kanal, DC_{avg} , Ausfall aufgrund gemeinsamer Ursache, Kategorie und PL

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

— **$MTTF_d$**

Das Hilfschütz K1A und der Schalter SW1A tragen zur $MTTF_d$ des einen Kanals bei. Es wird angenommen, dass die $MTTF_{d,K1A}$ von 50 Jahren und $MTTF_{d,SW1A}$ von 20 Jahren vom Hersteller angegeben werden. Das „Parts-Count“-Verfahren von D.1 ergibt für die $MTTF_d$ des einzelnen Kanals:

$$\frac{1}{MTTF_d} = \frac{1}{MTTF_{SW1A}} + \frac{1}{MTTF_{K1A}} = \frac{1}{20 \text{ Jahre}} + \frac{1}{50 \text{ Jahre}} = \frac{0,07}{\text{Jahre}} \quad (I.1)$$

was zu einer $MTTF_d = 14,3$ Jahre oder „mittel“ für einen Kanal nach 4.5.2, Tabelle 5 führt.

ANMERKUNG Wenn keine Information zum K1A zur Verfügung steht, könnte eine Annahme für den ungünstigsten Fall nach C.2 oder C.4 gemacht werden.

— **DC**

Da im Steuerstromkreis A keine Tests erfolgen, ist die $DC = 0$ oder „kein“ nach 4.5.3, Tabelle 6.

— **Kategorie**

Obwohl die bevorzugte Kategorie für diese Schaltung Kategorie 1 ist, ist die resultierende $MTTF_d$ des Kanals „mittel“. Dies ist das Argument, weshalb nur Kategorie B für diesen Entwurf erreicht wird.

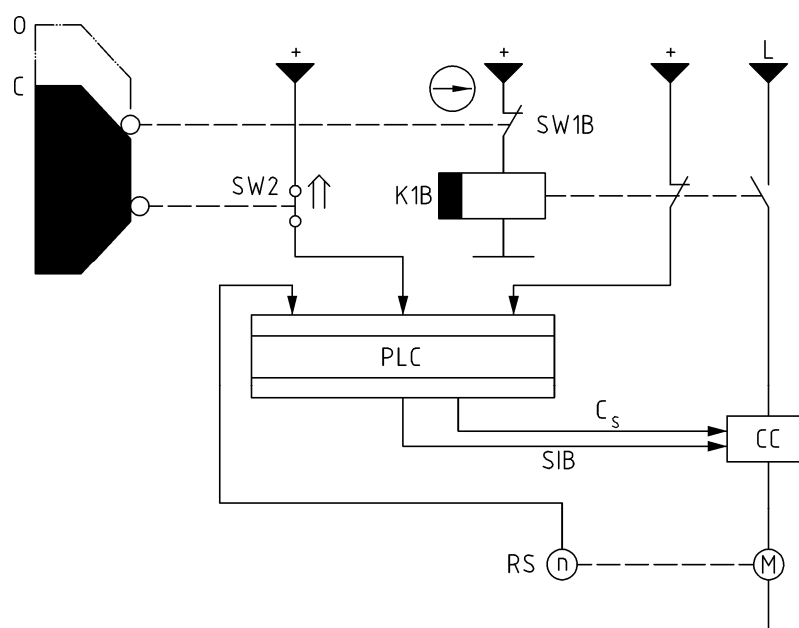
Eingangsdaten für Bild 5: $MTTF_d$ für jeden Kanal ist „mittel“ (14,3 Jahre), DC_{avg} ist „kein“ und die Kategorie ist B.

Dies kann als Performance Level b interpretiert werden.

Dieses Ergebnis entspricht nicht dem erforderlichen Performance Level c nach I.2. Die Schaltung muss deshalb neu gestaltet und bewertet werden, bis der Performance Level c erreicht wird, um die Anforderungen zur Risikominderung der Beispielanwendung von I.2 zu erreichen.

I.4 Beispiel B, redundantes System**I.4.1 Identifikation der sicherheitsbezogenen Teile**

Alle Bauteile, die zur Sicherheitsfunktion beitragen, sind in Bild I.3 dargestellt. Funktionale Details, die nichts zur Sicherheitsfunktion der Verriegelung beitragen (wie Start- und Stopp-Schalter oder die Abfallverzögerung von K1B), sind weggelassen.

**Legende**

PLC speicherprogrammierbare Steuerung
 CC Stromrichter
 M Motor
 RS Drehgeber
 o offen
 c geschlossen

C_s Stopp-Funktion (normale)
 SIB sichere Impulssperre
 K1B Hilfsschütz
 SW1B Schalter (NC)
 SW2 Schalter (NO)

Bild I.3 — Schaltplan B zur Ausführung der Sicherheitsfunktion

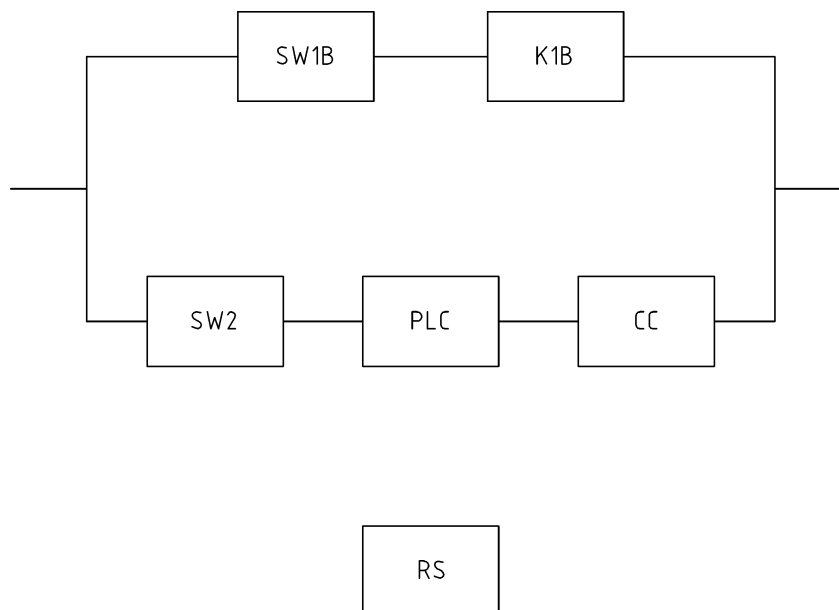
Im zweiten Beispiel werden zwei Kanäle, die Redundanz bereitstellen, verwendet. Der erste Kanal verwendet einen Türschalter mit zwangsöffnenden Kontakten in zwangsläufiger Betätigung, ähnlich dem in Beispiel A. Dieser Türschalter ist mit einem Hilfsschütz verbunden, das die Energiezuführung eines Motors abschalten kann. Im zweiten Kanal werden zusätzlich (programmierbare) elektronische Bauteile verwendet. Ein zweiter Türschalter ist mit einer speicherprogrammierbaren Steuerung verbunden, die den Stromrichter ansteuern kann, um die Energie zum Motor zu unterbrechen:

- redundante Kanäle, einer elektromechanisch und der andere programmierbar elektronisch;
- Schalter SW1B hat zwangsöffnende Kontakte, SW2 hat eine mittlere MTTF_d;
- Hilfsschütz K1B hat eine mittlere MTTF_d, das gewählte Hilfsschütz in diesem Beispiel ist *kein* bewährtes Bauteil;
- die MTTF_d der elektronischen Bauteile ist „mittel“.

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

ANMERKUNG Im Hinblick auf die zusätzliche Diversität werden Anforderungen an den PLC-Pfad nach 4.6 als nicht relevant betrachtet.

EN ISO 13849-1:2008 (D)



SW1B und K1B bilden den ersten Kanal, SW2, PLC und CC bilden den zweiten Kanal; RS wird nur verwendet, um den Stromrichter zu testen.

Legende

SW1B	Verriegelungseinrichtung
K1B	Hilfsschütz
SW2	Schalter
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 aufgrund gemeinsamer Ursache, Kategorie und PL

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

Der Schalter SW1B hat einen zwangsöffnenden Kontakt und eine zwangsläufige Betätigung. Deshalb wird ein Fehlerrückmeldung angenommen bezogen auf Nicht-Öffnen der Kontakte und Nicht-Betätigung des Schalters aufgrund mechanischer Ausfälle (z. B. Bruch des Stößels, Verschleiß des Schalthebels, Dejustage).

ANMERKUNG Diese Annahmen sind zulässig für Hilfsschalter nach IEC 60957-5-1:1997, Anhang K und bei ausreichender Fixierung und Betätigung des Schalters nach den Herstellerangaben (siehe ISO 13849-2).

— $MTTF_d$

Das Hilfsschütz K1B ist das einzige Element, das zur $MTTF_d$ des einen Kanals beiträgt. Es wird angenommen, dass die $MTTF_{dK1B}$ von 30 Jahren vom Hersteller angegeben wird. Das „Parts-Count“-Verfahren von D.1 ergibt für die $MTTF_d$ des einen Kanals

$$\frac{1}{MTTF_{dC1}} = \frac{1}{MTTF_{dK1B}} \quad (I.2)$$

was zu einer $MTTF_d = 30$ Jahren für den Kanal führt.

Im zweiten Kanal tragen SW2, PLC und CC zur $MTTF_{dC2}$ bei. Für diese drei Bauteile und auch für den RS wird eine $MTTF_d$ von 20 Jahren als vom Hersteller angegeben angenommen. Das „Parts-Count“-Verfahren von D.1 ergibt für die $MTTF_{dC2}$ des zweiten Kanals

$$\frac{1}{MTTF_{dC2}} = \frac{1}{MTTF_{dSW2}} + \frac{1}{MTTF_{dPLC}} + \frac{1}{MTTF_{dCC}} = \frac{1}{20 \text{ Jahre}} + \frac{1}{20 \text{ Jahre}} + \frac{1}{20 \text{ Jahre}} = \frac{0,15}{\text{Jahre}} \quad (I.3)$$

was zu einer $MTTF_d = 6,7$ Jahren für den Kanal führt.

Da beide Kanäle eine unterschiedliche $MTTF_d$ haben, kann die Gleichung von D.2 verwendet werden, um den Ersatzwert für $MTTF_d$ für einen Kanal eines symmetrischen zweikanaligen Systems zu erhalten. Diese Gleichung liefert $MTTF_d = 20$ Jahre oder „mittel“ für einen Kanal nach 4.5.2, Tabelle 5.

— DC

Im Steuerstromkreis B werden vier der sicherheitsbezogenen Teile durch die PLC getestet: SW2 und K1B werden zurückgelesen durch die PLC, die PLC führt Selbsttests durch und CC wird durch RS in die PLC zurückgelesen. Die zugehörigen DC jedes getesteten Teils sind:

- 1) $DC_{SW2} = 60 \%$, „niedrig“ aufgrund der Überwachung der Eingangssignale ohne dynamischen Test, siehe Tabelle E.1 (dritte Zeile des Teils der „Eingabeeinheit“),
- 2) $DC_{K1B} = 99 \%$, „hoch“ aufgrund der zwangsgeführten Öffner-/Schließer-Kombination, siehe Tabelle E.1 (zweite Zeile des Teils der „Eingabeeinheit“),
- 3) $DC_{PLC} = 30 \%$, „kein“ aufgrund der niedrigen Wirksamkeit der Selbsttests (es wird angenommen, dass der Hersteller diesen Wert durch eine FMEA berechnet hat), und
- 4) $DC_{CC} = 90 \%$, „mittel“ aufgrund des redundanten Abschaltweges mit Überwachung des Antriebselements durch die Steuerung, siehe Tabelle E.1 (sechste Zeile des Teils der „Ausgabeeinheit“) — wenn die PLC einen Ausfall des CC bemerkt, ist es möglich, die Bewegung durch die sichere Impulssperre zu blockieren (zusätzlicher Abschaltpfad).

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

$$\begin{aligned} DC_{avg} &= \frac{\frac{DC_{SW2}}{MTTF_{dSW2}} + \frac{DC_{K1B}}{MTTF_{dK1B}} + \frac{DC_{PLC}}{MTTF_{dPLC}} + \frac{DC_{CC}}{MTTF_{dCC}}}{\frac{1}{MTTF_{dSW2}} + \frac{1}{MTTF_{dK1B}} + \frac{1}{MTTF_{dPLC}} + \frac{1}{MTTF_{dCC}}} \\ &= \frac{\frac{0,6}{20 \text{ J}} + \frac{0,99}{30} + \frac{0,3}{20 \text{ J}} + \frac{0,9}{20 \text{ J}}}{\frac{1}{20 \text{ J}} + \frac{1}{30 \text{ J}} + \frac{1}{20 \text{ J}} + \frac{1}{20 \text{ J}}} = \frac{0,123}{0,183} = 67,1\% \end{aligned} \quad (I.4)$$

Demnach ist die DC_{avg} „niedrig“ nach 4.5.3 und Tabelle 6.

— CCF

Es wird angenommen, dass die Abschätzung der Maßnahmen gegen CCF für die Steuerung nach F.2 durchgeführt wurde. Die erreichten Ergebnisse sind in Tabelle I.1 angegeben.

EN ISO 13849-1:2008 (D)

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

Nr	Betrachtungseinheit	Punktezahl für den Steuerstromkreis	Maximal mögliches Ergebnis
1	Trennung/Abtrennung		
	Physikalische Trennung zwischen den Signalwegen	15	15
2	Diversität		
	Unterschiedliche Technologien/Gestaltung oder physikalische Prinzipien werden verwendet	20	20
3	Gestaltung/Anwendung/Erfahrung		
3.1	Schutz gegen Überspannung, Überdruck, Überstrom usw.	kein	15
3.2	Verwendung bewährter Bauteile	5	5
4	Beurteilung/Analyse		
	Sind die Ergebnisse einer Ausfallart und Effektanalyse berücksichtigt worden, um Ausfälle aufgrund gemeinsamer Ursache in der Entwicklung zu vermeiden?	5	5
5	Kompetenz/Ausbildung		
	Sind Konstrukteure geschult worden, um die Gründe und Auswirkungen von Ausfällen infolge gemeinsamer Ursache zu verstehen?	kein	5
6	Umgebung		
6.1	Schutz vor Verunreinigung und elektromagnetischer Beeinflussung (EMC) gegen CCF in Übereinstimmung mit den angemessenen Normen	25	25
6.2	Andere Einflüsse Wurden alle Anforderungen hinsichtlich Unempfindlichkeit gegenüber allen relevanten Umgebungsbedingungen wie Temperatur, Schock, Vibration, Feuchte (z. B. wie in den zutreffenden Normen festgelegt) berücksichtigt?	10	10
	Gesamt	80	Max. 100

Ausreichende Maßnahmen gegen CCF erfordern ein Ergebnis von mindestens 65. Im Beispiel B ist ein Wert von 80 ausreichend, um die Anforderungen gegen CCF zu erfüllen.

Ein einzelner Fehler in irgendeinem der Teile führt nicht zum Verlust der Sicherheitsfunktion. 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. Diese Eigenschaften sind typisch für Kategorie 3.

Eingangsdaten für Bild 5: $MTTF_d$ für den Kanal ist „mittel“ (20 Jahre), DC_{avg} ist „niedrig“ und die Kategorie ist 3.

Dies kann als Performance Level c interpretiert werden.

Dieses Ergebnis entspricht dem erforderlichen Performance Level c von I.2. Somit erfüllt der Steuerstromkreis B die Anforderungen zur Risikominderung der Beispielanwendung von I.2.

Anhang J (informativ)

Software

J.1 Beschreibung des Beispiels

In diesem Anhang werden exemplarisch die Tätigkeiten dargelegt, um die SRESW einer SRP/CS für einen $PL_r = d$ umzusetzen. Das SRP/CS ist mit der Maschinenausrüstung verbunden. Dies stellt sicher

- die Erfassung der Informationen von den verschiedenen Sensoren,
- die notwendige Bearbeitung für den Betrieb der Steuerungselemente unter Berücksichtigung der Sicherheitsanforderungen und
- die Ansteuerung der Antriebe.

Der Entwurf der SRESW für diese Anwendung auf der Ebene eines Funktionsblockschaltbildes ist wie in Bild J.1 gezeigt.

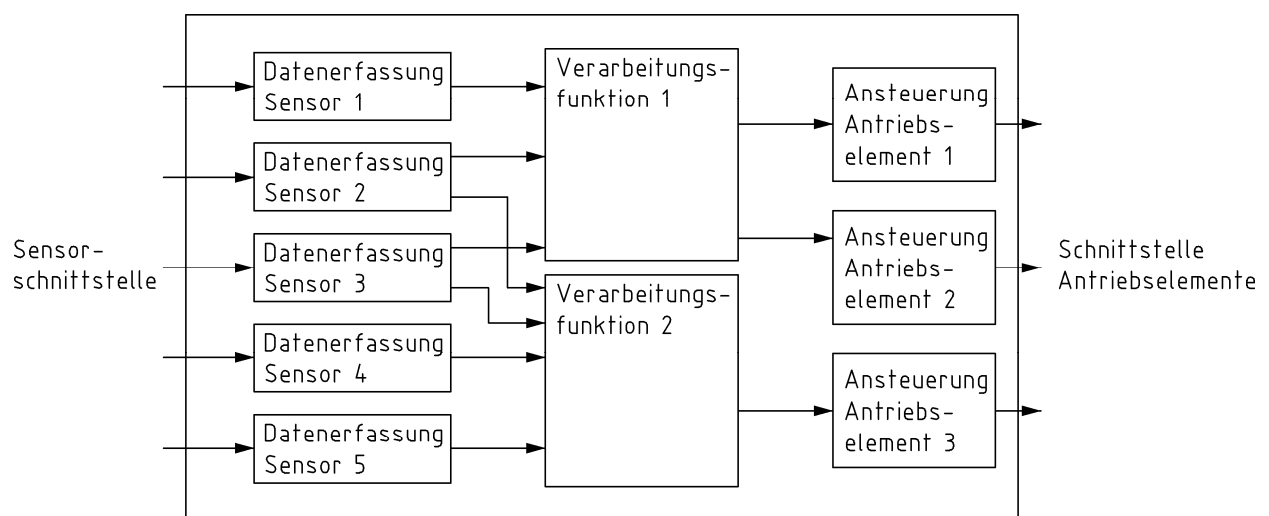


Bild J.1 — Entwurf eines Softwarebeispiels als Funktionsblockschaltbild

J.2 Anwendung des V-Modells des Software-Sicherheitslebenszyklus

Tabelle J.1 zeigt eine beispielhafte Zusammenstellung von Aktivitäten und Dokumenten zur Anwendung des V-Modells des Software-Sicherheitslebenszyklus für eine Maschinensteuerung.

EN ISO 13849-1:2008 (D)**Tabelle J.1 — Aktivitäten und Dokumente innerhalb des Software-Sicherheitslebenszyklus**

Entwicklungsaktivität	Verifikationsaktivität	Zugehörige Dokumentation
Maschinenaspekt: Identifikation der mit dem SRP/CS verbundenen Funktionen	Identifikation der „sicherheitsbezogenen“ Funktionen	„Sicherheitsbezogene Spezifikation der Maschinensteuerung“
Architektur-aspekt: Definition der Steuerungsarchitektur mit Sensoren und Antriebselementen	Erläuterungen zu den Sicherheitsmerkmalen der gewählten Bauteile	„Definition der Steuerungsarchitektur“
Aspekt der Softwarespezifikation: Umsetzen der Maschinenfunktionen in Softwarefunktionen	Erneutes Lesen der Beschreibungen (siehe J.3)	„Softwarebeschreibung“
Aspekt der Softwarearchitektur: Zuweisung der Funktionen zu Funktionsblöcken	Definition der kritischen Blöcke, die mit größerem Aufwand geprüft und validiert werden	„Funktionsblockmodellierung“
Codierungsaspekt: Codierung nach den Programmierregeln (siehe J.4)	Erneutes Lesen des Codes, Verifikation der Funktionen und Übereinstimmung mit den Regeln	„Kommentierung der Codes“ „Codierung der erneut gelesenen Blätter“
Validierungsaspekt: Aufstellen von Testszenarien: Betriebsaspekt der Funktionen Aspekt des Verhaltens bei Ausfällen	Verifikation der Testabdeckung, Verifikation der Testergebnisse	„Übereinstimmungsmatrix“ der Querverweise zu Paragraphen der Spezifikation und der Tests „Testblätter“, bestehend aus Testszenarien und Kommentaren zu erreichten Ergebnissen

J.3 Verifikation der Softwarespezifikation

Als Teil des Software-Sicherheitslebenszyklus besteht die Verifikationsaktivität auf der Basis der Software-spezifikation im Lesen der Beschreibungen, um nachzuweisen, dass alle sensiblen Punkte beschrieben sind. Das Folgende sollte bei der Verifikation jeder Funktion betrachtet werden:

- Begrenzen der Fälle fehlerhafter Interpretation der Systemspezifikation;
- Vermeiden von Lücken in der Spezifikation, resultierend aus von vornherein unbekanntem Verhalten der SRP/CS;
- genaue Definition der Bedingungen zur Aktivierung und Deaktivierung von Funktionen;
- Garantie, dass alle möglichen Fälle behandelt sind;
- Konsistenzprüfungen;
- unterschiedliche Fälle der Parametrisierung;
- Reaktion nach einem Ausfall.

J.4 Beispiel von Programmierregeln

Im Allgemeinen sollte es für die CCF möglich sein, ein Programm durch den Autor, dem Datum des Ladens, der Version und dem letzten Zugriff authentifizieren zu können. Hinsichtlich der Programmierregeln kann zwischen den folgenden Regeln unterschieden werden.

a) Programmierregeln auf Ebene der Programmstruktur

Die Programmierung sollte strukturiert werden, um so ein konsistentes und verständliches allgemeines Gerüst zu zeigen, in dem die verschiedenen Abläufe leicht lokalisiert werden können. Dies beinhaltet:

- 1) Verwenden von Vorlagen für typische Programm- und Funktionsblöcke,
- 2) Aufteilen des Programms in Teilabschnitte, um die wichtigen entsprechenden Teile zu kennzeichnen, die zu „Eingaben“, „Verarbeitungen“ und „Ausgaben“ gehören,
- 3) Kommentierung jedes Programmabschnittes des Quellcodes, um eine Aktualisierung der Kommentierung im Fall einer Änderung zu erleichtern,
- 4) Beschreibung, welche Aufgabe ein Funktionsblock bei einem Aufruf hat,
- 5) dass die Verwendung eines Speicherbereichs nur durch einen einzelnen Datentyp mit eindeutigen Kennzeichnungen erfolgen sollte und
- 6) dass der Programmablauf nicht abhängig sein sollte von Variablen wie Sprungadressen, die während der Laufzeit berechnet werden. Bedingungsabhängige Sprünge sind erlaubt.

b) Programmierregeln bezüglich der Verwendung von Variablen

- Die Ansteuerung oder Absteuerung jedes Ausgangs sollte nur einmalig erfolgen (zentralisierte Bedingungen).
- Das Programm sollte so strukturiert sein, dass die Gleichungen zum Aktualisieren einer Variablen zentralisiert sind.
- Jede globale Variable, Eingabe oder Ausgabe, sollte einen eindeutigen mnemonischen Namen erhalten und eine Beschreibung im Kommentar des Quelltextes.

c) Programmierregeln auf der Ebene des Funktionsblocks

- Vorzugsweise Verwendung von Funktionsblöcken, die durch den Lieferanten des SRP/CS validiert worden sind, prüfen, dass die angenommenen Betriebsbedingungen für diese validierten Blöcke mit den Bedingungen des Programms übereinstimmen.
- Die Größe des kodierten Blocks sollte nach folgenden Richtwerten begrenzt werden:
 - i) Parameter — maximal 8 digitale und 2 Integer-Eingänge, 1 Ausgang;
 - ii) Funktionaler Code — maximal 10 lokale Variable, maximal 20 boolsche Gleichungen.
- Die Funktionsblöcke sollten die globalen Variablen nicht verändern.
- Ein digitaler Wert sollte durch einen vorgegebenen Vergleichstest kontrolliert werden, um den Gültigkeitsbereich sicherzustellen.
- Ein Funktionsblock sollte versuchen, Widersprüchlichkeiten der zu verarbeitenden Variablen aufzudecken.
- Der Fehlercode eines Blocks sollte zugänglich sein, um den Fehler von anderen unterscheiden zu können.
- Der Fehlercode und der Zustand des Blocks nach Bemerken eines Fehlers sollte durch Kommentare beschrieben sein.
- Das Rücksetzen des Blocks oder die Wiederherstellung des normalen Zustands sollten durch Kommentare beschrieben sein.

Anhang K (informativ)

Numerische Darstellung von Bild 5

Siehe Tabelle K.1.

Tabelle K.1 — Numerische Darstellung von Bild 5

Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (1/h) und der zugehörige Performance Level (PL)													
MTTF _d für jeden Kanal Jahre	Kat. B DC _{avg} = kein	PL	Kat. 1 DC _{avg} = kein	PL	Kat. 2 DC _{avg} = niedrig	PL	Kat. 2 DC _{avg} = mittel	PL	Kat. 3 DC _{avg} = niedrig	PL	Kat. 3 DC _{avg} = mittel	PL	Kat. 4 DC _{avg} = hoch
3	3,80 × 10 ⁻⁵	a			2,58 × 10 ⁻⁵	a	1,99 × 10 ⁻⁵	a	1,26 × 10 ⁻⁵	a	6,09 × 10 ⁻⁶	b	
3,3	3,46 × 10 ⁻⁵	a			2,33 × 10 ⁻⁵	a	1,79 × 10 ⁻⁵	a	1,13 × 10 ⁻⁵	a	5,41 × 10 ⁻⁶	b	
3,6	3,17 × 10 ⁻⁵	a			2,13 × 10 ⁻⁵	a	1,62 × 10 ⁻⁵	a	1,03 × 10 ⁻⁵	a	4,86 × 10 ⁻⁶	b	
3,9	2,93 × 10 ⁻⁵	a			1,95 × 10 ⁻⁵	a	1,48 × 10 ⁻⁵	a	9,37 × 10 ⁻⁶	b	4,40 × 10 ⁻⁶	b	
4,3	2,65 × 10 ⁻⁵	a			1,76 × 10 ⁻⁵	a	1,33 × 10 ⁻⁵	a	8,39 × 10 ⁻⁶	b	3,89 × 10 ⁻⁶	b	
4,7	2,43 × 10 ⁻⁵	a			1,60 × 10 ⁻⁵	a	1,20 × 10 ⁻⁵	a	7,58 × 10 ⁻⁶	b	3,48 × 10 ⁻⁶	b	
5,1	2,24 × 10 ⁻⁵	a			1,47 × 10 ⁻⁵	a	1,10 × 10 ⁻⁵	a	6,91 × 10 ⁻⁶	b	3,15 × 10 ⁻⁶	b	
5,6	2,04 × 10 ⁻⁵	a			1,33 × 10 ⁻⁵	a	9,87 × 10 ⁻⁶	b	6,21 × 10 ⁻⁶	b	2,80 × 10 ⁻⁶	c	
6,2	1,84 × 10 ⁻⁵	a			1,19 × 10 ⁻⁵	a	8,80 × 10 ⁻⁶	b	5,53 × 10 ⁻⁶	b	2,47 × 10 ⁻⁶	c	
6,8	1,68 × 10 ⁻⁵	a			1,08 × 10 ⁻⁵	a	7,93 × 10 ⁻⁶	b	4,98 × 10 ⁻⁶	b	2,20 × 10 ⁻⁶	c	
7,5	1,52 × 10 ⁻⁵	a			9,75 × 10 ⁻⁶	b	7,10 × 10 ⁻⁶	b	4,45 × 10 ⁻⁶	b	1,95 × 10 ⁻⁶	c	
8,2	1,39 × 10 ⁻⁵	a			8,87 × 10 ⁻⁶	b	6,43 × 10 ⁻⁶	b	4,02 × 10 ⁻⁶	b	1,74 × 10 ⁻⁶	c	
9,1	1,25 × 10 ⁻⁵	a			7,94 × 10 ⁻⁶	b	5,71 × 10 ⁻⁶	b	3,57 × 10 ⁻⁶	b	1,53 × 10 ⁻⁶	c	
10	1,14 × 10 ⁻⁵	a			7,18 × 10 ⁻⁶	b	5,14 × 10 ⁻⁶	b	3,21 × 10 ⁻⁶	b	1,36 × 10 ⁻⁶	c	
11	1,04 × 10 ⁻⁵	a			6,44 × 10 ⁻⁶	b	4,53 × 10 ⁻⁶	b	2,81 × 10 ⁻⁶	c	1,18 × 10 ⁻⁶	c	
12	9,51 × 10 ⁻⁶	b			5,84 × 10 ⁻⁶	b	4,04 × 10 ⁻⁶	b	2,49 × 10 ⁻⁶	c	1,04 × 10 ⁻⁶	c	
13	8,78 × 10 ⁻⁶	b			5,33 × 10 ⁻⁶	b	3,64 × 10 ⁻⁶	b	2,23 × 10 ⁻⁶	c	9,21 × 10 ⁻⁷	d	
15	7,61 × 10 ⁻⁶	b			4,53 × 10 ⁻⁶	b	3,01 × 10 ⁻⁶	b	1,82 × 10 ⁻⁶	c	7,44 × 10 ⁻⁷	d	
16	7,13 × 10 ⁻⁶	b			4,21 × 10 ⁻⁶	b	2,77 × 10 ⁻⁶	c	1,67 × 10 ⁻⁶	c	6,76 × 10 ⁻⁷	d	

Tabelle K.1 (fortgesetzt)

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

Anhang ZA (informativ)

Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EG-Richtlinie 98/37/EG geändert durch Richtlinie 98/79/EG

Diese Europäische Norm wurde im Rahmen eines Mandates, das CEN von der Europäischen Kommission und der Europäischen Freihandelszone erteilt wurde, erarbeitet, um ein Mittel zur Erfüllung der grundlegenden Anforderungen der Richtlinie nach der neuen Konzeption 98/37/EG, ergänzt durch Richtlinie 98/79/EG, bereitzustellen.

Sobald diese Norm im Amtsblatt der Europäischen Gemeinschaften im Rahmen der betreffenden Richtlinie in Bezug genommen und in mindestens einem der Mitgliedstaaten als nationale Norm umgesetzt worden ist, berechtigt die Übereinstimmung mit den normativen Abschnitten dieser Norm innerhalb der Grenzen des Anwendungsbereichs dieser Norm zu der Annahme, dass eine Übereinstimmung mit den entsprechenden grundlegenden Anforderungen 1.2.1 und 1.2.7 des Anhangs I der Richtlinie und der zugehörigen EFTA-Vorschriften gegeben ist.

WARNHINWEIS — Für Produkte, die in den Anwendungsbereich dieser Norm fallen, können weitere Anforderungen und weitere EG-Richtlinien anwendbar sein.

Anhang ZB (informativ)

Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EG-Richtlinie 2006/42/EG

Diese Europäische Norm wurde im Rahmen eines Mandates, das CEN von der Europäischen Kommission und der Europäischen Freihandelszone erteilt wurde, erarbeitet, um ein Mittel zur Erfüllung der grundlegenden Anforderungen der Richtlinie nach der neuen Konzeption Maschine 2006/42/EG bereitzustellen.

Sobald diese Norm im Amtsblatt der Europäischen Gemeinschaften im Rahmen der betreffenden Richtlinie in Bezug genommen und in mindestens einem der Mitgliedstaaten als nationale Norm umgesetzt worden ist, berechtigt die Übereinstimmung mit den normativen Abschnitten dieser Norm innerhalb der Grenzen des Anwendungsbereichs dieser Norm zu der Annahme, dass eine Übereinstimmung mit den entsprechenden grundlegenden Anforderungen 1.2.1 des Anhangs I der Richtlinie und der zugehörigen EFTA-Vorschriften gegeben ist.

WARNHINWEIS — Für Produkte, die in den Anwendungsbereich dieser Norm fallen, können weitere Anforderungen und weitere EG-Richtlinien anwendbar sein.

Literaturhinweise

Publikationen über programmierbar elektronische Systeme

- [1] IEC 61000-4-4, *Electromagnetic compatibility (EMC) — Part 4: Testing and measurement techniques — Section 4: Electrical fast transient/burst immunity test*
- [2] IEC 61496-1, *Safety of machinery — Electro-sensitive protective equipment — Part 1: General requirements and tests*
- [3] IEC 61496-2, *Safety of machinery — Electro-sensitive protective equipment — Part 2: Particular requirements for equipment using active opto-electronic protective devices*
- [4] IEC 61496-3, *Safety of machinery — Electro-sensitive protective equipment — Part 3: Particular requirements for active opto-electronic protective devices responsive to diffuse reflection (AOPDDR)*
- [5] IEC 61508-1:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements*
- [6] IEC 61508-2:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*
- [7] IEC 61508-5:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 5: Examples of methods for the determination of safety integrity levels*
- [8] IEC 61508-6:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*
- [9] IEC 61508-7:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures*
- [10] IEC 62061, *Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems*
- [11] HSE Guidelines, *Programmable Electronic Systems in Safety-related Applications — Parts 1 (ISBN 0 11 883906 6) and 2 (ISBN 0 11 883906 3).*
- [12] CECR-184, *Personal Safety in Microprocessor control systems* (Elektronikcentralen, Denmark)

Weitere Publikationen

- [13] ISO/FDIS 13850, *Safety of machinery — Emergency stop — Principles for design*
- [14] ISO 13851, *Safety of machinery — Two-hand control devices — Functional aspects and design principles*
- [15] ISO 13856-1, *Safety of machinery — Pressure-sensitive protective devices — Part 1: General principles for design and testing of pressure-sensitive mats and pressure-sensitive floors*
- [16] ISO 13856-2, *Safety of machinery — Pressure-sensitive protective devices — Part 2: General principles for the design and testing of pressure-sensitive edges and pressure-sensitive bars*
- [17] ISO 11428, *Safety of machinery — Visual danger signals — General requirements, design and testing*
- [18] ISO 9001, *Quality management system — Requirements*

- [19] ISO 9355-1, *Ergonomic requirements for the design of displays and control actuators — Part 1: Human interactions with displays and control actuators*
- [20] ISO 9355-2, *Ergonomic requirements for the design of displays and control actuators — Part 2: Displays*
- [21] ISO 9355-3, *Ergonomic requirements for the design of displays and control actuators — Part 3: Control actuators*
- [22] ISO 11429, *Safety of machinery — System of auditory and visual danger and information signals*
- [23] ISO 7731, *Ergonomics — Danger signals for public and work areas — Auditory*
- [24] ISO 4413, *Hydraulic fluid power — General rules relating to systems*
- [25] ISO 4414, *Pneumatic fluid power — General rules relating to systems*
- [26] ISO 13855:2000, *Safety of machinery — Positioning of protective equipment with respect to the approach speeds of parts of the human body*
- [27] ISO 14118, *Safety of machinery — Prevention of unexpected start-up*
- [28] ISO 19973 (all parts), *Pneumatic fluid power — Assessment of component reliability by testing*
- [29] IEC 60204-1:2005, *Safety of machinery — Electrical equipment of machines — Part 1: General requirements*
- [30] IEC 60447:1993, *Basic and safety principles for man-machine interface (MMI) — Actuating principles*
- [31] IEC 60529, *Degrees of protection provided by enclosures (IP code)*
- [32] IEC 60812, *Analysis techniques for system reliability — Procedure for failure mode and effects analysis (FMEA)*
- [33] IEC 60947 (all parts), *Low-voltage switchgear and control gear*
- [34] IEC 61000-6-2, *Electromagnetic compatibility (EMC) — Part 6-2: Generic standards — Immunity for industrial environments*
- [35] IEC 61800-3, *Adjustable speed electrical power drive systems — Part 3: EMC requirements and specific test methods*
- [36] IEC 61300 (all parts), *Fibre optic interconnecting devices and passive components — Basic test and measurement procedures*
- [37] IEC 61310 (all parts), *Safety of machinery — Indication, marking and actuation*
- [38] IEC 61131-3, *Programmable controllers — Part 3: Programming languages*
- [39] IEC 61810 (all parts), *Electromagnetic elementary relays*
- [40] EN 457, *Sicherheit von Maschinen; Akustische Gefahrensignale; Allgemeine Anforderungen, Gestaltung und Prüfung (ISO 7731:1986, modifiziert)*
- [41] EN 614-1, *Sicherheit von Maschinen — Ergonomische Gestaltungsgrundsätze — Teil 1: Begriffe und allgemeine Leitsätze*

EN ISO 13849-1:2008 (D)

- [42] EN 982, *Sicherheit von Maschinen — Sicherheitstechnische Anforderungen an fluidtechnische Anlagen und deren Bauteile — Hydraulik*
- [43] EN 983, *Sicherheit von Maschinen — Sicherheitstechnische Anforderungen an fluidtechnische Anlagen und deren Bauteile — Pneumatik*
- [44] EN 1005-3, *Sicherheit von Maschinen — Menschliche körperliche Leistung — Teil 3: Empfohlene Kraftgrenzen bei Maschinenbetätigung*
- [45] EN 1088, *Sicherheit von Maschinen — Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen — Leitsätze für Gestaltung und Auswahl*
- [46] EN 50205, *Relais mit (mechanisch) zwangsgeführten Kontakten*
- [47] SN 29500 (all Parts), *Failure rates of components*
- [48] Goble, W.M.: *Control systems — Evaluation and Reliability. 2nd Edition. Instrument Society of America (ISA), North Carolina, 1998*

Datenbanken

- [49] Siemens Standard SN 29500, *Ausfallraten für Bauteile, Edition 1999-11, Siemens AG 1999* (www.pruefinstitut.de)
- [50] IEC/TR 62380, *Reliability data handbook — Universal model for reliability prediction of electronics components, PCBs and equipment*, identisch zu RDF 2000/Reliability Data Handbook, UTE C 80-810, Union Technique de l'Electricité et de la Communication (www.ute-fr.com)
- [51] *Reliability Prediction of Electronic Equipment*, MIL-HDBK-217E, Department of Défense, Washington DC, 1982
- [52] *Reliability Prediction Procedure for Electronic Equipment*, Telcordia SR-332, Issue 01, May 2001 (telecom-info.telcordia.com), (Bellcore TR-332, Issue 06)
- [53] *EPRD, Electronic Parts Reliability Data* (RAC-STD-6100), Reliability Analysis Center, 201 Mill Street, Rome, NY 13440 (rac.alionscience.com)
- [54] *NPRD-95, Nonelectronic Parts Reliability Data* (RAC-STD-6200), Reliability Analysis Center, 201 Mill Street, Rome, NY 13440 (rac.alionscience.com)
- [55] *British Handbook for Reliability Data for Components used in Telecommunication Systems*, British Telecom (HRD5, last issue)
- [56] Chinese Military Standard, GJB/z 299B