DIN EN ISO 13849-1

ICS 13.110

Ersatz für
DIN EN ISO 13849-1:2008-12

Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze (ISO 13849-1:2015); Deutsche Fassung EN ISO 13849-1:2015

Safety of machinery –
Safety-related parts of control systems –
Part 1: General principles for design (ISO 13849-1:2015);
German version EN ISO 13849-1:2015

Sécurité des machines –
Parties des systèmes de commande relatives à la sécurité –
Partie 1: Principes généraux de conception (ISO 13849-1:2015);
Version allemande EN ISO 13849-1:2015

Gesamtumfang 113 Seiten

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

Preisgruppe 32
www.din.de
www.beuth.de
2300069

Nationales Vorwort

Diese Norm enthält sicherheitstechnische Festlegungen.

Dieses Dokument (EN ISO 13849-1:2015) wurde vom Technischen Komitee ISO/TC 199 „Safety of machinery“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 114 „Sicherheit von Maschinen“, dessen Sekretariat von DIN (Deutschland) gehalten wird, erarbeitet.

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

In dieser Deutschen Ausgabe der EN ISO 13849-1:2015 wurde in Abschnitt 11 „Benutzerinformation“, Absatz 2, erster Spiegelstrich, und im Beispiel am Ende des Abschnittes 11 „ISO 13849-1:2006“ in „ISO 13849-1:2015“ korrigiert.

Für die in Abschnitt 2 dieses Dokuments zitierten Internationalen Normen wird im Folgenden auf die entsprechenden Deutschen Normen hingewiesen:

ISO 12100	siehe	DIN EN ISO 12100
ISO 13849-2	siehe	DIN EN ISO 13849-2
IEC 61508-3	siehe	DIN EN 61508-3 (VDE 0803-3)
IEC 61508-4	siehe	DIN EN 61508-4 (VDE 0803-4)
IEC 62061	siehe	DIN EN 62061 (VDE 0113-50)
ISO/TR 22100-2	siehe	DIN ISO/TR 22100-2 (DIN SPEC 33887)
ISO/TR 23849	siehe	DIN ISO/TR 23849 (DIN SPEC 33883)

Änderungen

Gegenüber DIN EN ISO 13849-1:2008-12 wurden folgende Änderungen vorgenommen:

a) Einarbeitung des Technischen Corrigendums ISO 13849-1:2006/Cor 1:2009;

b) Löschung der früheren Tabelle 1 in der Einleitung;

c) Aktualisierung und Hinzufügen normativer Verweisungen;

d) Änderung von Definitionen der Begriffe „Gefährdungssituation“ und „Betriebsart mit hoher Anforderungsrate oder Betriebsart mit kontinuierlicher Anforderung“;

e) Hinzufügen des neuen Begriffs und der Definition „betriebsbewährt“;

f) Einfügen eines neuen Unterabschnitts 4.5.5 „Beschreibung des Ausgabeteils der SRP/CS nach Kategorien“;

g) Änderungen an den Anhängen, insbesondere bei Anhang I;

h) Dokument redaktionell überarbeitet.

Frühere Ausgaben

DIN EN 954-1: 1997-03
DIN EN 954-1 Beiblatt 1: 2000-01
DIN EN ISO 13849-1: 2007-02, 2007-07, 2008-12

Nationaler Anhang NA
(informativ)

Literaturhinweise

[1] DIN EN ISO 12100, *Sicherheit von Maschinen — Allgemeine Gestaltungsleitsätze — Risikobeurteilung und Risikominderung*

[2] DIN EN ISO 13849-2, *Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen — Teil 2: Validierung*

[3] DIN EN 61508-3 (VDE 0803-3), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 3: Anforderungen an Software*

[4] DIN EN 61508-4 (VDE 0803-4), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 4: Begriffe und Abkürzungen*

[5] DIN EN 62061 (VDE 0113-50), *Sicherheit von Maschinen — Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme*

[6] DIN ISO/TR 22100-2 (DIN SPEC 33887), *Sicherheit von Maschinen — Beziehung zu ISO 12100 — Teil 2: Wie ISO 12100 und ISO 13849-1 zusammenhängen*

[7] DIN ISO/TR 23849 (DIN SPEC 33883), *Leitfaden zur Anwendung von ISO 13849-1 und IEC 62061 bei der Gestaltung von sicherheitsbezogenen Steuerungen für Maschinen*

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN ISO 13849-1

Dezember 2015

ICS 13.110

Ersatz für EN ISO 13849-1:2008

Deutsche Fassung

Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen — Teil 1: Allgemeine Gestaltungsleitsätze (ISO 13849-1:2015)

Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design (ISO 13849-1:2015)

Sécurité des machines — Parties des systèmes de commande relatives à la sécurité — Partie 1: Principes généraux de conception (ISO 13849-1:2015)

Diese Europäische Norm wurde vom CEN am 20. Juni 2015 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-CENELEC 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 Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

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

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

CEN-CENELEC Management-Zentrum: Avenue Marnix 17, B-1000 Brüssel

Ref. Nr. EN ISO 13849-1:2015 D

Inhalt

Seite

Europäisches Vorwort

Dieses Dokument (EN ISO 13849-1:2015) wurde vom Technischen Komitee ISO/TC 199 „Safety of machinery“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 114 „Sicherheit von Maschinen“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Juni 2016, und etwaige entgegenstehende nationale Normen müssen bis Juni 2016 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente 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 13849-1:2008.

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

Zum Zusammenhang mit EU-Richtlinien siehe informativen Anhang ZA, 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, die ehemalige jugoslawische Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO 13849-1:2015 wurde vom CEN als EN ISO 13849-1:2015 ohne irgendeine Abänderung genehmigt.

Anhang ZA
(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.

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

Vorwort

ISO (die Internationale Organisation für Normung) ist eine weltweite Vereinigung von Nationalen Normungsorganisationen (ISO-Mitgliedsorganisationen). Die Erstellung von Internationalen Normen wird normalerweise von ISO Technischen Komitees durchgeführt. Jede Mitgliedsorganisation, die Interesse an einem Thema hat, für welches ein Technisches Komitee gegründet wurde, hat das Recht, in diesem Komitee vertreten zu sein. Internationale Organisationen, staatlich und nicht-staatlich, in Liaison mit ISO, nehmen ebenfalls an der Arbeit teil. ISO arbeitet eng mit der Internationalen Elektrotechnischen Kommission (IEC) bei allen elektrotechnischen Themen zusammen.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der empfangenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname wird als Information zum Nutzen der Anwender angegeben und stellt keine Anerkennung dar.

Eine Erläuterung der Bedeutung ISO-spezifischer Benennungen und Ausdrücke, die sich auf Konformitätsbewertung beziehen, sowie Informationen über die Beachtung der WTO-Grundsätze zu technischen Handelshemmnissen (TBT, en: Technical Barriers to Trade) durch ISO enthält der folgende Link: Foreword - Supplementary information.

Das für dieses Dokument verantwortliche Komitee ist ISO/TC 199, *Safety of machinery*.

Diese dritte Ausgabe ersetzt die zweite Ausgabe (ISO 13849-1:2006), welche technisch überarbeitet wurde. Sie enthält außerdem das Technische Corrigendum ISO 13849-1:2006/Cor 1:2009. Änderungen zur vorherigen Ausgabe umfassen

— das Löschen der früheren Tabelle 1 in der Einleitung,

— das Aktualisieren und Hinzufügen normativer Verweisungen,

— die Änderung von Definitionen der Begriffe Gefährdungssituation und Betriebsart mit hoher Anforderungsrate oder Betriebsart mit kontinuierlicher Anforderung,

— das Hinzufügen eines neuen Begriffs und der Definition, *betriebsbewährt*,

— die editorielle, aber nicht technische Änderung des Bildes 1,

— einen neuen Unterabschnitt 4.5.5, sowie Änderungen an bestehenden Teilen einschließlich der Anhänge, wesentliche Änderungen an Anhang C und einen vollständig erneuerten Anhang I.

ISO 13849 besteht aus den folgenden Teilen, unter dem allgemeinen Titel *Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen*:

— Teil 1: Allgemeine Gestaltungsleitsätze

— Teil 2: Validierung

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 Maschine oder eine Gruppe von Maschinen.

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

Dieses Dokument betrifft im Besonderen die folgenden Interessengruppen, welche die Akteure am Markt im Bereich der Maschinensicherheit repräsentieren:

— Hersteller von Maschinen (kleine, mittlere und große Unternehmen);

— Arbeitsschutz-Institutionen (Aufsichtsbehörden, Unfallverhütungs-Organisationen, Marktaufsicht usw.).

Das Niveau der Maschinensicherheit, das mit Hilfe dieses Dokuments von den oben genannten Interessengruppen erreicht wird, kann weitere Gruppen betreffen:

— Anwender von Maschinen / Arbeitgeber (kleine, mittlere und große Unternehmen);

— Anwender von Maschinen / Arbeitnehmer (z. B. Gewerkschaften, Organisationen für Menschen mit besonderen Bedürfnissen);

— Dienstleister, z. B. für die Instandhaltung (kleine, mittlere und große Unternehmen);

— Verbraucher (wenn die Maschine zur Nutzung durch Verbraucher gedacht ist).

Den oben erwähnten Interessengruppen wurde ermöglicht, am Erarbeitungsprozess dieser Norm mitzuwirken.

Zusätzlich ist dieses Dokument für Normungs-Gremien, die Typ-C-Normen erarbeiten, vorgesehen.

Die Anforderungen in diesem Dokument können durch eine Typ-C-Norm ergänzt oder geändert werden.

Für Maschinen, die durch den Anwendungsbereich einer Typ-C-Norm abgedeckt sind und die entsprechend den Anforderungen dieser Norm gestaltet und konstruiert wurden, haben die Anforderungen dieser Typ-C-Norm Vorrang.

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- oder Typ-C-Normen erarbeiten, mit der Vermutung, mit den wesentlichen Sicherheitsanforderungen des Anhangs I der Richtlinie 2006/42/EG über Maschinen, 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 2).

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 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.

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 ISO 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 die Gestaltung und die Implementierung sicherheitsbezogener Steuerungen von Maschinen fest. Durch die Anwendung einer der beiden Internationalen Normen kann in Übereinstimmung mit deren Anwendungsbereichen angenommen werden, dass die relevanten und erforderlichen Sicherheitsanforderungen erfüllt sind. ISO/TR 23849 enthält Hinweise zur Anwendung von diesem Teil der ISO 13849 und IEC 62061 bei der Gestaltung von sicherheitsbezogenen Steuerungen für Maschinen.

Wie ISO/TR 23849 wurde auch ISO/TR 22100-2 zur Liste der normativen Verweisungen in Abschnitt 2 hinzugefügt — der letztgenannte wegen seiner Bedeutung für das Verständnis des Zusammenhangs zwischen diesem Teil der ISO 13849 und ISO 12100.

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 mit Betriebsart mit hoher Anforderungsrate und Betriebsart mit kontinuierlicher Anforderung, 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 programmierbar elektronischem(n) System(en) 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.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, 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 12100:2010, *Safety of machinery — General principles for design — Risk assessment and risk reduction*

ISO 13849-2:*2012*, *Safety of machinery — Safety-related parts of control systems — Part 2: Validation*

IEC 60050-191:1990, *International electrotechnical vocabulary — Chapter 191: Dependability and quality of service.* Amended by IEC 60050-191-am1:1999 and IEC 60050-191-am2:2002:1999

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements.* Corrected by IEC 61508-3/Cor.1:1999

IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviation.* Corrected by IEC 61508-4/Cor.1:1999

IEC 62061:2012, *Safety of machinery — Functional safety of safety–related electrical, electronic and programmable electronic control systems*

ISO/TR 22100-2:2013, *Safety of machinery — Relationship with ISO 12100 — Part 2: How ISO 12100 relates to ISO 13849-1*

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

3 Begriffe, Formelzeichen und Abkürzungen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO 12100 und 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 zum Begriff: 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 zum Begriff: 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 zum Begriff: Ein Fehler ist oft das Resultat eines Ausfalls der Einheit selbst, kann aber ohne vorherigen Ausfall bestehen.

Anmerkung 2 zum Begriff: In diesem Teil der ISO 13849 bedeutet der Begriff „Fehler“ *zufälliger Fehler*.

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

3.1.4
Ausfall
Beendigung der Fähigkeit einer Einheit, eine geforderte Funktion zu erfüllen

Anmerkung 1 zum Begriff: Nach einem Ausfall hat die Einheit einen Fehler.

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

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

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

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

3.1.5
gefahrbringender Ausfall
Ausfall der das Potential hat, das SRP/CS in einen gefährlichen Zustand oder eine Fehlfunktion zu bringen

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

Anmerkung 2 zum Begriff: [QUELLE: IEC 61508-4, 3.6.7, modifiziert.]

3.1.6
Ausfall infolge gemeinsamer Ursache
CCF
Ausfälle verschiedener Einheiten aufgrund eines einzelnen Ereignisses, wobei diese Ausfälle nicht auf gegenseitiger Ursache beruhen

Anmerkung 1 zum Begriff: Ausfälle infolge gemeinsamer Ursache sollten nicht verwechselt werden mit gleichartigen Ausfällen (siehe ISO 12100:2010, 3.36).

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

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 zugehörenden Faktoren, beseitigt werden kann

Anmerkung 1 zum Begriff: Instandsetzung ohne Änderung wird üblicherweise den Grund des Ausfalls nicht beseitigen.

Anmerkung 2 zum Begriff: Ein systematischer Ausfall kann hervorgerufen werden durch Simulation der Ausfallursache.

Anmerkung 3 zum Begriff: 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.

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

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

[QUELLE: ISO 12100:2010, 3.5.]

3.1.11
Gefährdung
potentielle Schadensquelle

Anmerkung 1 zum Begriff: 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 zum Begriff: 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).

[QUELLE: ISO 12100:2010, 3.6, modifiziert.]

3.1.12
Gefährdungssituation
Sachlage, bei der eine Person mindestens einer Gefährdung ausgesetzt ist

Anmerkung 1 zum Begriff: Diese Situation kann unmittelbar oder über einen Zeitraum hinweg zu einem Schaden führen.

[QUELLE: ISO 12100:2010, 3.10.]

3.1.13
Risiko
Kombination der Wahrscheinlichkeit des Eintritts eines Schadens und seines Schadensausmaßes

[QUELLE: ISO 12100:2010, 3.12.]

3.1.14
Restrisiko
verbleibendes Risiko, nachdem Schutzmaßnahmen ergriffen wurden

Anmerkung 1 zum Begriff: Siehe Bild 2.

[QUELLE: ISO 12100:2010, 3.13, modifiziert.]

3.1.15
Risikobeurteilung
Gesamtheit des Verfahrens, das eine Risikoanalyse und Risikobewertung umfasst

[QUELLE: ISO 12100:2010, 3.17.]

3.1.16
Risikoanalyse
Kombination aus Festlegung der Grenzen der Maschine, Identifizierung der Gefährdung und Risikoeinschätzung

[QUELLE: ISO 12100:2010, 3.15.]

3.1.17
Risikobewertung
auf der Risikoanalyse beruhende Beurteilung, ob die Ziele zur Risikominderung erreicht wurden

[QUELLE: ISO 12100:2010, 3.16.]

3.1.18
bestimmungsgemäße Verwendung einer Maschine
Verwendung einer Maschine in Übereinstimmung mit den in der Benutzerinformation bereitgestellten Informationen

[QUELLE: ISO 12100:2010, 3.23.]

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

[QUELLE: ISO 12100:2010, 3.24.]

3.1.20
Sicherheitsfunktion
Funktion einer Maschine, wobei ein Ausfall der Funktion zur unmittelbaren Erhöhung des Risikos (der Risiken) führen kann

[QUELLE: ISO 12100:2010, 3.30.]

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

[QUELLE: IEC 61508-4:1998, 3.3.2, modifiziert.]

3.1.23
Performance Level
PL
diskreter Level, der die Fähigkeit von sicherheitsbezogenen Teilen einer Steuerung spezifiziert, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen

Anmerkung 1 zum Begriff: 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 1 zum Begriff: 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

[QUELLE: IEC 62061:2005, 3.2.34, modifiziert.]

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 zum Begriff: 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.

[QUELLE: IEC 61508-4:1998, 3.8.6, modifiziert.]

3.1.27
Schutzmaßnahme
vorgesehene Maßnahme zur 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, Betriebserlaubnis zur Ausführung von Arbeiten), Bereitstellung und Anwendung zusätzlicher Schutzeinrichtungen (persönliche Schutzausrüstung, Ausbildung).

[QUELLE: ISO 12100:2010, 3.19, modifiziert.]

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 Reparatur oder nach System-/ Bauteilaustausch.

Anmerkung 1 zum Begriff: 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 1 zum Begriff: 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

[QUELLE: 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 zum Begriff: Typische Beispiele von LVL (Kontaktplan, Funktions-Blockdiagramm) sind in IEC 61131-3 angegeben.

Anmerkung 2 zum Begriff: Ein typisches Beispiel von einem System, das die LVL verwendet: PLC.

[QUELLE: IEC 61511-1:2003, 3.2.80.1.2, modifiziert.]

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 zum Begriff: Ein typisches Beispiel von Systemen für die Verwendung von FVL: Embedded-Systeme.

Anmerkung 2 zum Begriff: Im Bereich der Maschinen wird FVL in Embedded-Software und gelegentlich in Anwendungssoftware eingesetzt.

[QUELLE: IEC 61511-1:2003, 3.2.80.1.3, modifiziert.]

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 1 zum Begriff: Üblicherweise wird Embedded-Software in FVL geschrieben.

3.1.38
Betriebsart mit hoher Anforderungsrate oder Betriebsart mit kontinuierlicher Anforderung
Betriebsart, in der die Häufigkeit von Anforderungen an ein SRP/CS mehr als einmal pro Jahr beträgt oder die sicherheitsbezogenen Teile des Steuersystems die Maschine als Teil des Normalbetriebs in einem sicheren Zustand halten

[QUELLE: IEC 62061:2012, 3.2.27, modifiziert.]

3.1.39
betriebsbewährt
Nachweis, basierend auf einer Analyse der betrieblichen Erfahrung für eine spezielle Konfiguration eines Elements, dass die Wahrscheinlichkeit gefahrbringender systematischer Fehler niedrig genug ist, damit jede Sicherheitsfunktion, die das Element verwendet, ihren erforderlichen Performance Level (PL_r) erreicht

[QUELLE: IEC 61508-4:2010, 3.8.18, modifiziert]

3.2 Formelzeichen und Abkürzungen

Siehe Tabelle 1.

Tabelle 1 — Formelzeichen und Abkürzungen

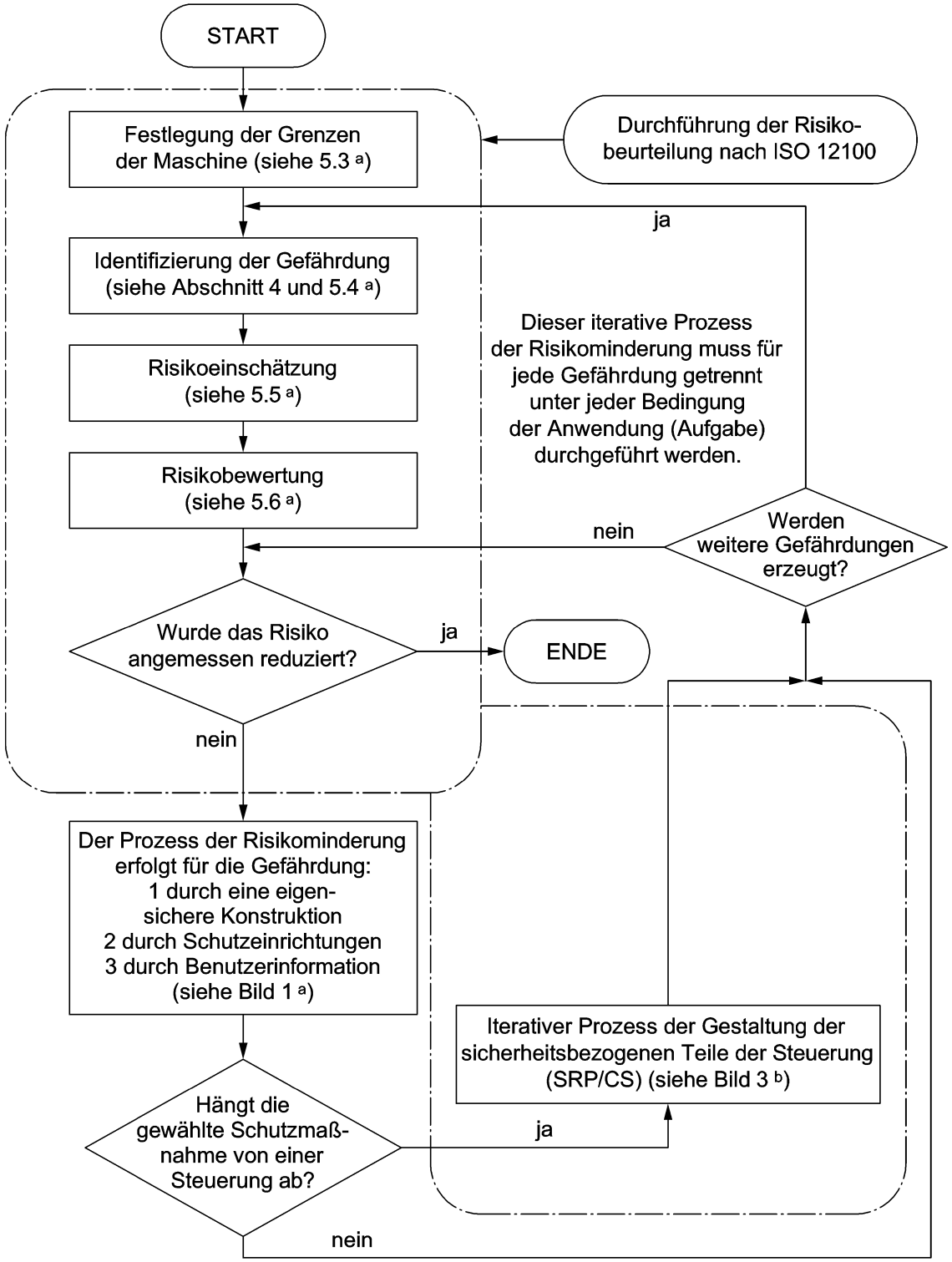
Formelzeichen oder Abkürzung	Beschreibung	Definition oder Fundort
a, b, c, d, e	Bezeichnung für die Performance Level	Tabelle 3
AOPD	aktive opto-elektronische Schutzeinrichtungen (z. B. Lichtschranke)	Anhang H
B, 1, 2, 3, 4	Bezeichnung für die Kategorien	Tabelle 7
B_{10D}	Anzahl von Zyklen, bis 10 % 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
n_{op}	mittlere Anzahl der jährlichen Betätigungen	Anhang C
O, O1, O2, OTE	Ausgabegerät, z. B. Betätigungselement	6.2
P, P1, P2	Möglichkeit zur Vermeidung der Gefährdung	A.2.3

Formelzeichen oder Abkürzung	Beschreibung	Definition oder Fundort
PES	programmierbares elektronisches System	3.1.22
PFH_D	durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde	Tabelle 3 und Tabelle K.1
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
r_t	Testrate	3.1.29
RS	Drehgeber	Anhang I
S, S1, S2	Schwere der Verletzung	A.2.1
SW1A, SW1B, SW2	Positionsschalter	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
T_{10D}	mittlere Zeit bis 10 % der Bauteile gefährlich ausfallen	Anhang C

4 Gestaltungsaspekte

4.1 Sicherheitsziele in der Gestaltung

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



a Bezieht sich auf ISO 12100:2010

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 12100:2010, 6.1 genannt, weitere Anleitungen finden sich in der ISO 12100:2010, 6.2 (Inhärent sichere Konstruktion) und 6.3 (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 Risikominderung durch Konstruktion (siehe ISO 12100:2010, 6.2);

— Risikominderung durch Schutzeinrichtungen und mögliche ergänzende Schutzmaßnahmen (siehe ISO 12100:2010, 6.3);

— Risikominderung durch Bereitstellung einer Benutzerinformation über das Restrisiko (siehe ISO 12100:2010, 6.4).

4.2.2 Beitrag der Risikominderung durch das Steuerungssystem

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 verriegelten trennenden 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.

ANMERKUNG Es ist nicht notwendig, diese Strategie der Risikominderung auf nicht sicherheitsrelevante Teile des Steuerungssystems oder auf rein funktionale Bauteile der Maschine anzuwenden (siehe ISO TR 22100-2:2013, Abschnitt 3).

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 sind festgelegt, vom niedrigsten PL a bis zum höchsten PL e, mit definierten Bereichen der Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (siehe Tabelle 2).

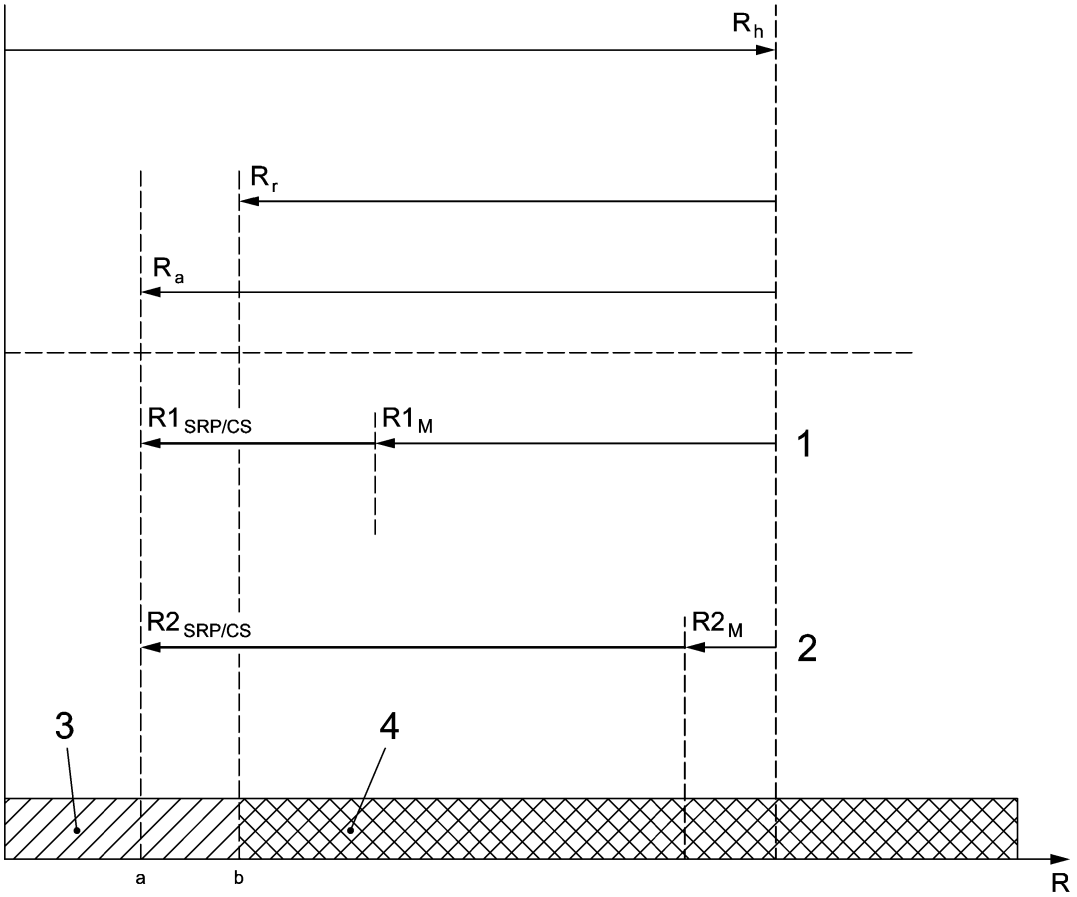
Um einen PL zu erhalten, müssen neben den quantifizierbaren Aspekten auch die qualitativen Aspekte in Bezug auf die Anforderungen der PL erfüllt werden (siehe 4.5).

Tabelle 2 —Performance Level (PL)

Performance Level (PL)	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (PFH_D) 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 $< 10^{-7}$

Nach der Risikobeurteilung (siehe ISO 12100) an der Maschine, muss der Konstrukteur entscheiden, welchen Beitrag der Risikominderung von jeder relevanten Sicherheitsfunktion benötigt wird, die das/die SRP/CS ausführt/ausführen. 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 Schutzeinrichtung 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).

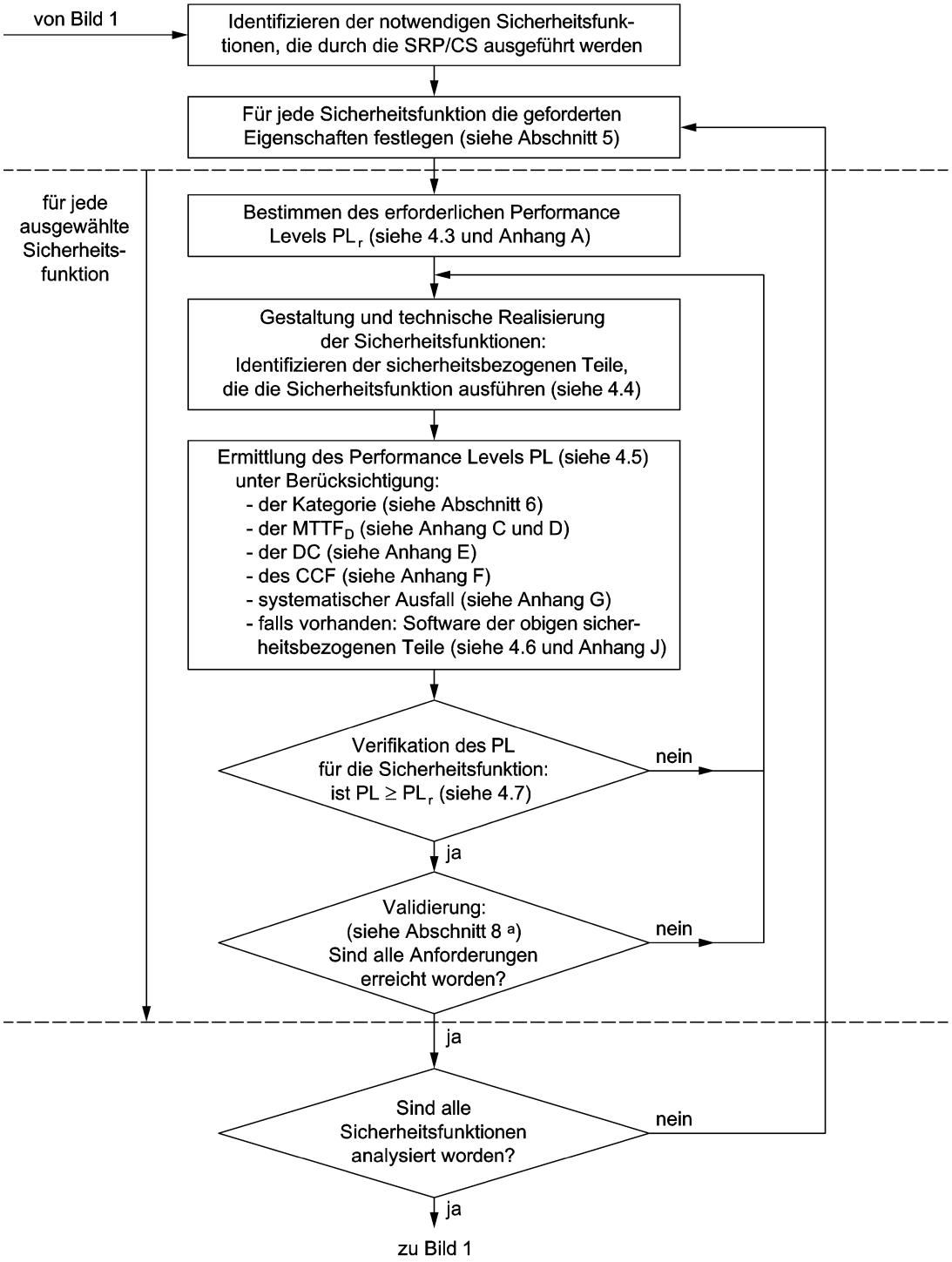


Legende

R_h	Risiko einer speziellen Gefährdungssituation, bevor Schutzmaßnahmen angewendet werden
R_r	geforderte Risikominderung durch Schutzmaßnahmen
R_a	tatsächliche, 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)
3	angemessen vermindertes Risiko
4	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



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 als Leitlinie zur Bestimmung des PL_r). 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

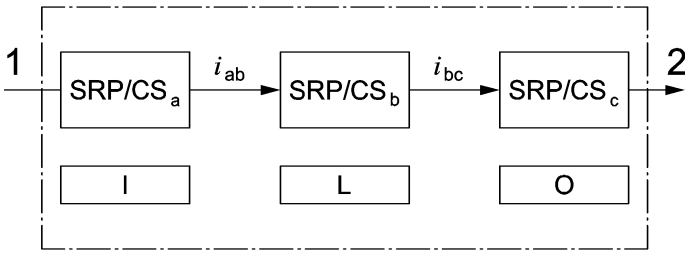
— Verbindungen (i_{ab}, i_{bc}) (z. B. elektrisch, optisch).

ANMERKUNG 1 Es ist wichtig, innerhalb der gleichen Maschinenanlage zwischen den Sicherheitsfunktionen und deren zugehörigem SRP/CS zu unterscheiden, welches eine bestimmte Sicherheitsfunktion ausführt.

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.



Legende
I Eingang (z. B. Endschalter, Sensor, AOPD)
L Logik
O Ausgang (z. B. Ventil, Kontakt, Stromrichtergerät)
1 Startereignis (z. B. manuelle Betätigung eines Tasters, Öffnung einer trennenden Schutzeinrichtung, Unterbrechung des Strahls einer AOPD)
2 Antriebselement der Maschine (z. B. Motor, Zylinder)

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 gefahrbringenden 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 (siehe auch 4.5.5).

ANMERKUNG 2 Für den Entwurf komplexer Steuerungssysteme, wie z. B. PES zur Durchführung von Sicherheitsfunktionen, kann die Anwendung anderer einschlägiger Normen angemessen sein (z. B. IEC 61508 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 3 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 3 — 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

Wurde eine sicherheitsrelevante Steuerungsfunktion unter Verwendung eines oder mehrerer SRP/CS entworfen, muss jedes SRP/CS entweder nach diesem Teil der ISO 13489 oder nach IEC 62061/IEC 61508 (siehe auch ISO/TR 23849) entworfen sein, obwohl es eine Übereinstimmung zwischen den PL dieses Teils der ISO 13489 und den SIL der Normen IEC 61508 und IEC 62061 gibt. SRP/CS können nach 6.3 zusammengefasst werden.

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 überwachtes 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 4) und muss für jeden Kanal individuell berücksichtigt werden (z. B. einzelner Kanal, jeder Kanal eines redundanten Systems).

Für jedes SRP/CS (Teilsystem) nach Tabelle 5 beträgt der maximale Wert der $MTTF_D$ für jeden Kanal 100 Jahre. Für SRP/CS (Teilsysteme) der Kategorie 4 erhöht sich der maximale Wert der $MTTF_D$ für jeden Kanal auf 2 500 Jahre.

ANMERKUNG Dieser höhere Wert ist dadurch begründet, dass sich in Kategorie 4 die anderen quantifizierbaren Aspekte, Struktur und DC auf ihrem Höchststand befinden, was es erlaubt, in Kategorie 4 mehr als drei Teilsysteme (SRP/CS) seriell zu kombinieren und PL e nach 6.3 zu erreichen.

Tabelle 4 — 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

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).

ANMERKUNG 2 Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Zur Abschätzung der $MTTF_D$ eines Bauteils muss folgendes abgestuftes 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) Wählen von zehn Jahren.

4.5.3 Diagnosedeckungsgrad (DC)

Der Wert für den DC wird in vier Stufen angegeben (siehe Tabelle 5).

Zur Abschätzung des DC kann in den meisten Fällen die Ausfallarten und Effekt-Analyse (FMEA, siehe IEC 60812) oder ähnliche Verfahren verwendet werden. In diesem Fall sollten alle relevanten Fehler und/oder Ausfallarten berücksichtigt werden. Für einen vereinfachten Ansatz zur Abschätzung des DC, siehe Anhang E.

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

Tabelle 5 — Diagnosedeckungsgrad (DC)

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	99 % ≤ DC

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.

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.

4.5.4 Vereinfachtes Verfahren zur Abschätzung der quantifizierbaren Aspekte des 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 die quantifizierbaren Aspekte des 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.

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 leistungssteuernden Elemente (siehe auch ISO 12100:2010, 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 ≤ 1/100 der Testrate (siehe auch die Anmerkung in Anhang K); oder die Prüfung erfolgt unmittelbar bei Anforderung der Sicherheitsfunktion und die Gesamtzeit zum Erkennen des Ausfalls und zur Überführung der Maschine in einen nicht gefahrbringenden Zustand (in der Regel wird die Maschine angehalten) ist kürzer als die Zeit bis zum Erreichen der Gefährdung (siehe auch ISO 13855);

— für Kategorie 2, ist $MTTF_D$ des Testkanals größer als die Hälfte der $MTTF_D$ des Funktionskanals.

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 (Hilfestellung hierzu siehe Anhang F).

Enthalten die SRP/CS Software, müssen die Anforderungen nach 4.6 angewandt werden.

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 12100:2010, Abschnitt 3 und IEC 60204-1:2005).

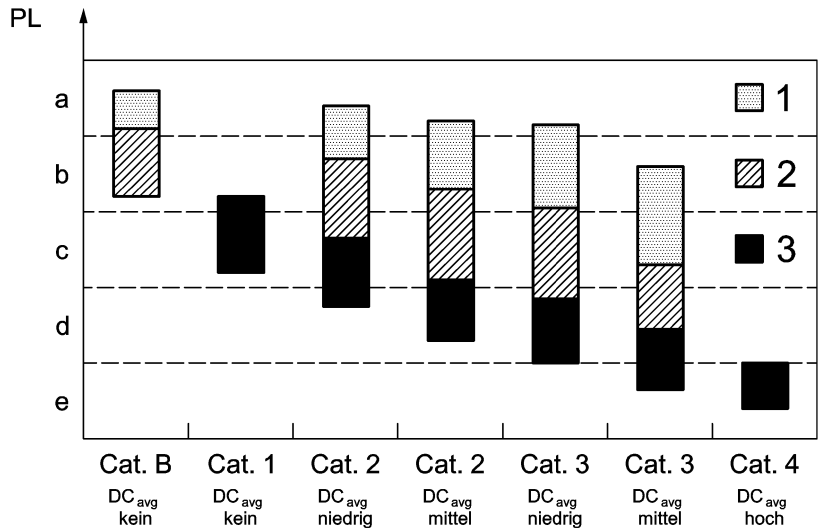
Bild 5 zeigt das Verfahren zur Auswahl der Kategorien in Kombination mit $MTTF_D$ für jeden Kanal und der DC_{avg}, um den erforderlichen PL für jede Sicherheitsfunktion zu erreichen.

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 (Hilfestellung hierzu 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 6 angegeben. Für eine genauere Auswahl des PL auf der Basis des genauen Wertes der $MTTF_D$ jedes Kanals, siehe Anhang K.



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

Tabelle 6 — 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

4.5.5 Beschreibung des Ausgabeteils der SRP/CS nach Kategorien

Wenn für mechanische, hydraulische oder pneumatische Bauteile (oder Bauteile, die eine Mischung von Technologien enthalten) keine anwendungsspezifischen Zuverlässigkeitsdaten vorhanden sind, darf der Hersteller der Maschine die quantifizierbaren Aspekte des PL ohne eine $MTTF_D$-Berechnung abschätzen.

In diesen Fällen wird der sicherheitsbezogene Performance Level (PL) durch die Architektur, die Diagnose und die Maßnahmen gegen CCF implementiert.

Tabelle 7 zeigt den Zusammenhang zwischen erreichbarem PL (wie in Bild 5) und den Kategorien. PL a und PL b können mit Kategorie B implementiert werden. PL c kann mit Kategorie 1 oder Kategorie 2 implementiert werden, wenn bewährte Bauteile und bewährte Sicherheitsprinzipien benutzt werden.

Wird eine PL c Sicherheitsfunktion mit Kategorie 1 implementiert, werden die T_{10D}-Werte der sicherheitsrelevanten Bauteile, die während des Prozesses nicht überwacht werden, bestimmt. Diese T_{10D}-Werte können durch betriebsbewährte Daten des Maschinenherstellers bestimmt werden.

Die $MTTF_D$ des Testkanals in Kategorie 2 muss mindestens 10 Jahre betragen.

PL d kann mit Kategorie 3 implementiert werden, wenn bewährte Bauteile und bewährte Sicherheitsprinzipien benutzt werden. PL e kann mit Kategorie 4 implementiert werden, wenn bewährte Bauteile und bewährte Sicherheitsprinzipien benutzt werden.

Grundsätzlich: Bei der Implementierung der Sicherheitsfunktion mit Kategorie 2, Kategorie 3 oder Kategorie 4 müssen Ausfälle infolge gemeinsamer Ursache (CCF) und ein ausreichender Diagnosedeckungsgrad (DC) berücksichtigt werden (niedrig, mittel für Kategorie 2 und 3, hoch für Kategorie 4).

In diesem Fall wird die Berechnung des DC_{avg} auf den arithmetischen Mittelwert der einzelnen DCs aller Bauteile in dem Funktionskanal reduziert.

Tabelle 7 — PL und PFH_D als Abschätzung des ungünstigsten Falls basierend auf Kategorie, DC_{avg} und der Verwendung von bewährten Bauteilen

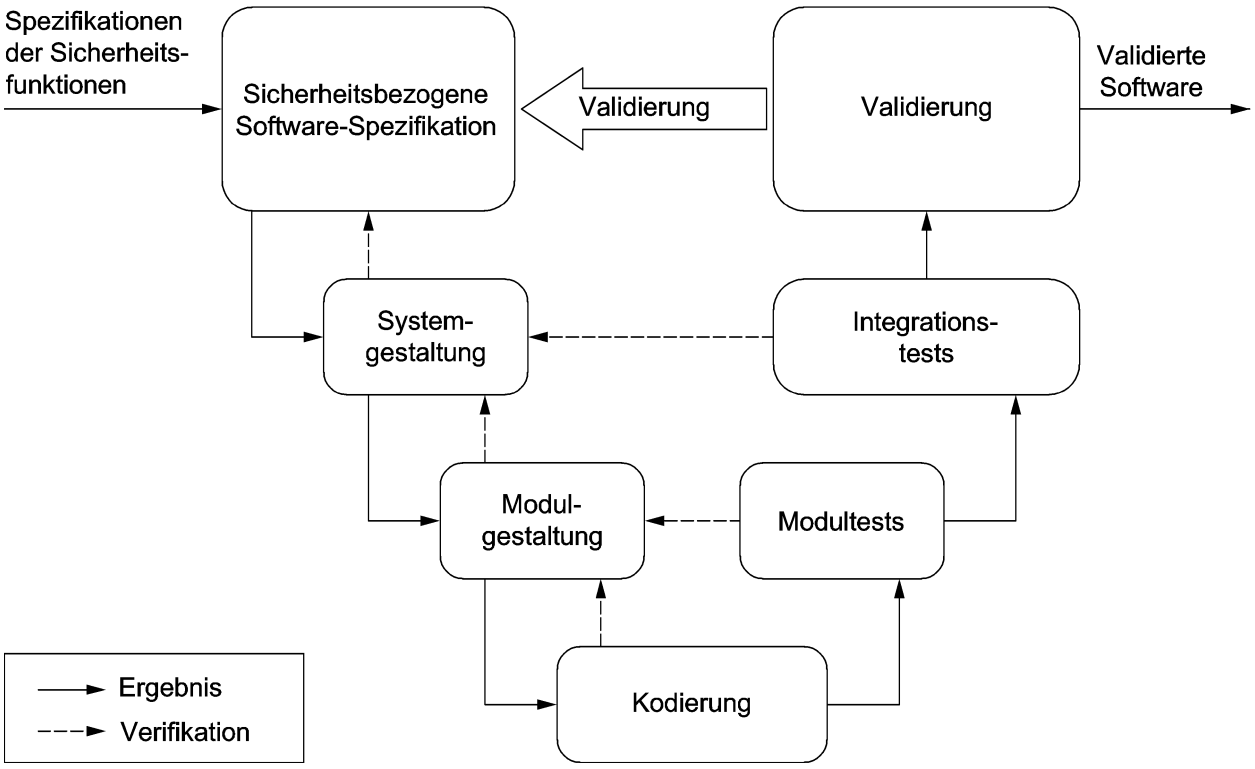
	PFH_D (1/h)	Kat. B	Kat. 1	Kat. 2	Kat. 3	Kat. 4
PL a	2*10-5	●	O	O	O	O
PL b	5*10-6	●	O	O	O	O
PL c	1,7*10-6	-	●2*	●1*	O	O
PL d	2,9*10-7	-	-	-	●1*	O
PL e	4,7*10-8	-	-	-	-	●1*

●	Angewandte Kategorie wird empfohlen
O	Angewandte Kategorie ist optional
-	Kategorie ist nicht zulässig
1*	Betriebsbewährte (siehe 3.1.39) oder bewährte (Eignung für diese bestimmte Anwendung durch den Bauteilhersteller bestätigt) Bauteile und bewährte Sicherheitsprinzipien müssen benutzt werden
2*	Bewährte Bauteile und bewährte Sicherheitsprinzipien müssen benutzt werden. Für die sicherheitsbezogenen Bauteile, die im Prozess nicht überwacht werden, können die T_{10D} Werte durch den Maschinenhersteller basierend auf Daten zur Betriebsbewährung bestimmt werden.

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 Empfehlungen für Tätigkeiten des Lebenszyklus.

Bild 6 — Vereinfachtes V-Modell des Software-Sicherheitslebenszyklus

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 von nicht sicherheitsbezogener 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 durch zu treffende Maßnahmen, 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.

Bauteile, für die die SRESW-Anforderungen nicht erfüllt sind, z. B. PLC(en) ohne Sicherheitsbewertung durch den Hersteller, dürfen unter folgenden alternativen Bedingungen verwendet werden:

— das SRP/CS ist auf PL a oder PL b begrenzt und verwendet Kategorie B, 2 oder 3;

— das SRP/CS ist auf PL c oder PL d begrenzt und darf mehrere Bauteile für zwei Kanäle in Kategorie 2 oder 3 verwenden. Die Bauteile dieser beiden Kanäle verwenden diversitäre Technologien.

4.6.3 Sicherheitsbezogene Anwendungssoftware (SRASW)

Der Software-Sicherheitslebenszyklus (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,

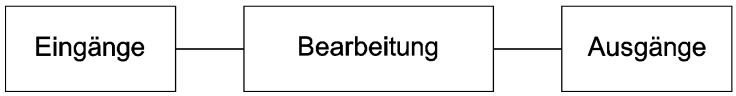
3) Funktionsblöcke mit minimierter Codelänge,

4) Innerhalb des Funktionsblocks sollte die Ausführung des Codes mit einem Eingangssprung und einem Ausgangssprung erfolgen,

5) Architektur des Modells in drei Stufen: Eingänge ⇒ Verarbeitung ⇒ Ausgänge (siehe Bild 7 und Anhang J),

6) Zuordnung des Sicherheitsausgangs zu nur einem Programmteil, und

7) Verwendung von Techniken zur Detektion externer Ausfälle und zur defensiven Programmierung innerhalb von Eingangs-, Verarbeitungs- und Ausgangsblöcken, die zum sicheren Zustand führen.



Eingangsblöcke	**Verarbeitungsblock**	**Ausgangsblöcke**
Erfassung der Information der verschiedenen Sicherheitssensoren durch die Sicherheitseingänge	Erforderliche Verarbeitung, um die Sicherheitsfunktionen zu realisieren, die zu einem sichern Zustand führen	Ansteuerung der Betätigungselemente durch Sicherheitsausgänge

Bild 7 — Allgemeines Architekturmodell für Software

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

1) SRASW und nicht-SRASW 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 nicht sicherheitsbezogenen 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.

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/Anweisung und Deklarationszeilen.

h) Verifikation[1)]:

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, dass 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.

---

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

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

— Kontrolle des Bereiches gültiger Eingaben;

— 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. Personal Computer 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. Personal Computer 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.

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

4.8 Ergonomische Aspekte der Gestaltung

Die Schnittstelle zwischen Benutzer und den SRP/CS 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, EN 614-1, ISO 9355-1, ISO 9355-2, ISO 9355-3, EN 1005-3, IEC 60204-1:2005, 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 12100:2010, 6.2.8 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 verweisen, deren Anforderungen sich auf die Sicherheitsfunktion, Eigenschaft oder Parameter beziehen. Der Konstrukteur (oder Typ-C-Normensetzer) muss sicherstellen, dass alle anwendbaren Anforderungen für die in den Tabellen aufgelisteten relevanten 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 Maschinen-Sicherheitsfunktionen und einige ihrer Eigenschaften anwendbar sind

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

[a] Einschließlich verriegelter trennender Schutzeinrichtungen und Grenzwertüberwachung (z. B. Höchstdrehzahl, Übertemperatur, Überdruck).

[b] Ergänzende Schutzmaßnahme, siehe ISO 12100:2010.

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

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

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

   ANMERKUNG In einigen Fällen kann es notwendig sein, das Verhalten der Maschine bei Energieverlust zu berücksichtigen, wenn es beispielsweise notwendig ist, eine vertikale Achse zu halten, um ein Absenken durch Schwerkraft zu verhindern. Das kann zwei getrennte Sicherheitsfunktionen erfordern: mit Energie verfügbar und ohne Energie verfügbar.

g) Bedingung(en) (z. B. Betriebsart) der Maschine, in der sie aktiv oder gesperrt ist;

h) der Häufigkeit der Betätigung;

i) 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 dieser ein 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 ein sicherer 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 Betätigungselements 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 Betätigungselement zum Rücksetzen muss außerhalb des Gefahrbereichs und an einer sicheren Position mit guter Einsicht zur Überprüfung, dass sich keine Person im Gefahrbereich befindet, angebracht werden.

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

ANMERKUNG Eine Lösung ist die Verwendung eines zweiten Betätigungselements zum Rücksetzen. Die Rückstellfunktion wird innerhalb des Gefahrbereichs durch das erste Betätigungselement in Kombination mit einem zweiten Betätigungselement zum Rücksetzen außerhalb des Gefahrbereichs (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 trifft ISO 12100:2010, 6.3.3.2.5 bei einer verriegelten trennenden Schutzeinrichtung mit Startfunktion zu.

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

ANMERKUNG Die Rückmeldung eines Sensorsignals an die Steuerung kann einen automatischen Start auslösen.

BEISPIEL Beim automatischen Maschinenablauf wird die Rückmeldung eines Sensorsignals an die Steuerung häufig zur Steuerung des Prozessablaufs verwendet. Wenn ein Werkstück seine Position verlässt, wird der Ablauf gestoppt. Wenn die Überwachung der verriegelnden trennenden Schutzeinrichtung der automatischen Steuerung nicht übergeordnet ist, könnte eine Gefahr bestehen, dass die Maschine wieder anläuft, wenn die Bedienperson der Maschine die Lage des Werkstücks korrigiert. Deshalb sollte der ferngesteuerte Wiederanlauf nicht erlaubt werden, bis die trennende 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 Gefahrbereichs 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 den Anforderungen einer oder mehrerer 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).

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 (von) Fehlers(n) in diesem Teil,

— den Möglichkeiten, Fehler in diesem Teil zu vermeiden (systematische Fehler),

— der Wahrscheinlichkeit des Auftretens eines (von) Fehlers(n) 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 dass 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.

6.2.3 Kategorie B

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

— 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

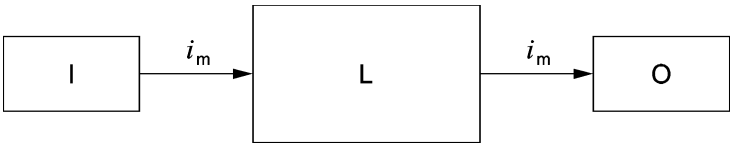
— anderen relevanten äußeren Einflüssen, z. B. mechanische Schwingungen, elektromagnetischen Störungen, Unterbrechungen oder Störungen der Energieversorgung.

In Systemen der Kategorie B gibt es keinen Diagnosedeckungsgrad (DC_{avg} = 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.

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 Diagnosedeckungsgrad (DC_{avg} = kein). In solchen Strukturen (einkanalige 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 ist 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

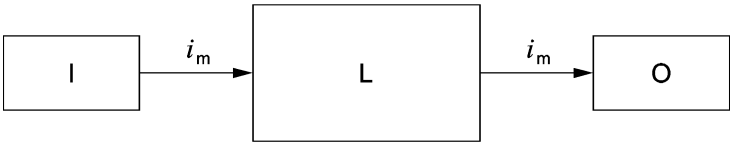
— Mittel, um die Befestigung des Schalters nach der Justierung zu sichern,

— 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 Funktion(en) in angemessenen Zeitabständen durch die Maschinensteuerung getestet wird (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, sobald die Sicherheitsfunktion benötigt wird 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

— eine Ausgabe für die Einleitung geeigneter Steuerungsmaßnahmen erzeugen (OTE), wenn ein Fehler erkannt wurde.

Für $PL_r = d$ muss die Ausgabe (OTE) einen sicheren Zustand einleiten, der bis zur Behebung des Fehlers beibehalten wird.

Für PL_r bis zu einschließlich $PL_r = c$ muss die Ausgabe (OTE) wenn möglich einen sicheren Zustand einleiten, der bis zur Behebung des Fehlers beibehalten wird. Wenn das Einleiten eines sicheren Zustands nicht möglich ist (z. B. durch Verschweißen des Kontakts des finalen Schaltglieds), kann es ausreichen, wenn der Ausgang der Testeinrichtung, OTE, nur eine Warnung bereitstellt.

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 Diagnosedeckungsgrad (DC_{avg}) des Funktionskanals muss mindestens 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/des die 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.

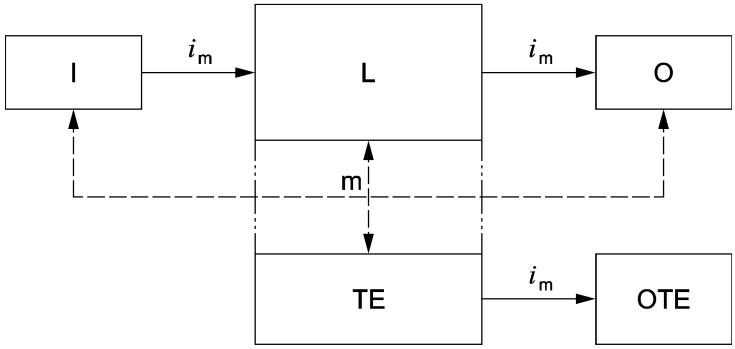
ANMERKUNG 2 Das Systemverhalten der Kategorie 2 ist dadurch gekennzeichnet, dass

— 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 technischen Festlegungen, z. B. die Wahl der Testhäufigkeit, die Wahrscheinlichkeit des Auftretens einer Gefährdungssituation verringert.

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



Legende

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

Die gestrichelten Linien zeigen die vernünftigerweise durchführbare Fehlererkennung.

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}) des gesamten SRP/CS muss mindestens 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, hat der Normensetzer von Typ-C-Normen weitere Einzelheiten zur Fehlererkennung zu nennen.

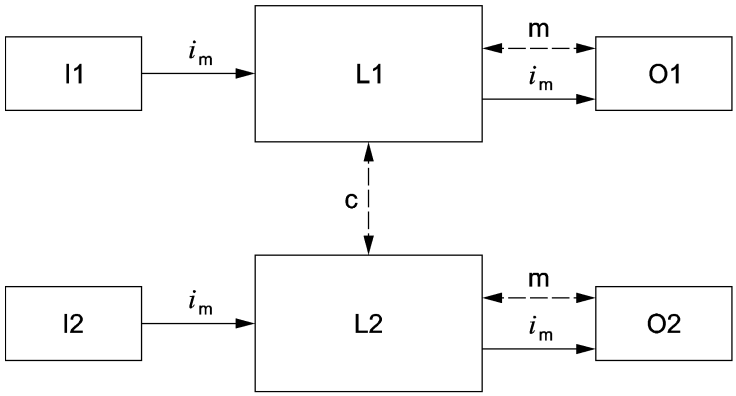
ANMERKUNG 3 Das Systemverhalten der Kategorie 3 ist dadurch gekennzeichnet, dass

— bei Auftreten eines einzelnen Fehlers die Sicherheitsfunktion immer ausgeführt wird,

— einige, aber nicht alle Fehler erkannt werden,

— durch die Anhäufung unerkannter Fehler die Sicherheitsfunktion verloren gehen kann.

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



Legende

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

Die gestrichelten Linien zeigen die vernünftigerweise durchführbare Fehlererkennung.

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 ist dadurch gekennzeichnet, dass

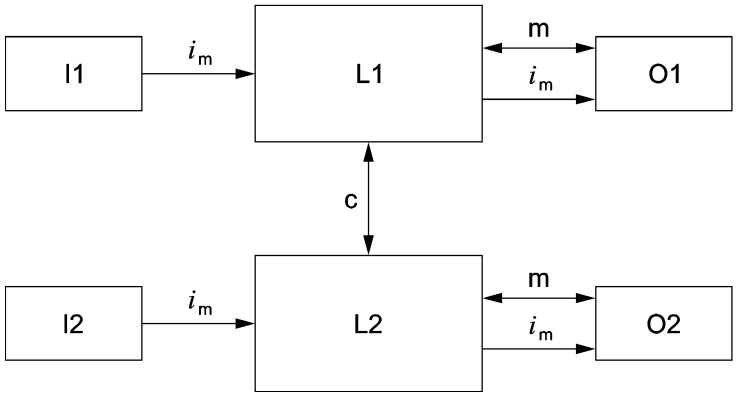
— bei Auftreten eines einzelnen Fehlers die Sicherheitsfunktion immer ausgeführt wird,

— 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 $MTTF_D$ jedes Kanals von nur „hoch“.

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



Legende

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

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

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 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 Sicherheits-prinzipien müssen erfüllt sein. Die Sicherheitsfunktion muss in geeigneten Zeitabständen durch die Maschinensteuerung getestet werden (siehe 4.5.4).	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 Sicherheits-prinzipien 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	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

Kategorie	Zusammenfassung der Anforderungen	Systemverhalten	Prinzip zum Erreichen der Sicherheit	$MTTF_D$ jedes Kanals	DC_{avg}	CCF
	durchführbar, der einzelne Fehler erkannt wird.					
4 (siehe 6.2.7)	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 — der einzelne Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt wird, aber wenn diese Erkennung nicht möglich ist, darf eine Anhäufung von unerkannten Fehlern nicht zum Verlust der Sicherheitsfunktion führen.	Wenn ein einzelner Fehler auftritt, bleibt die Sicherheitsfunktion immer erhalten. Die Erkennung von Fehleranhäufungen reduziert die Wahrscheinlichkeit des Verlustes der Sicherheitsfunktion (hohe DC). Die Fehler werden rechtzeitig erkannt, um einen Verlust der Sicherheitsfunktion zu verhindern.	Überwiegend durch die Struktur charakterisiert.	hoch	hoch, einschließlich 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, Signalverarbeitungseinheit, Ausgangssystem. Diese SRP/CS können 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 ein Gesamt-PL nach den Verfahren dieses Abschnitts 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 serielle Kombination folgende Abschätzungen gezeigt.

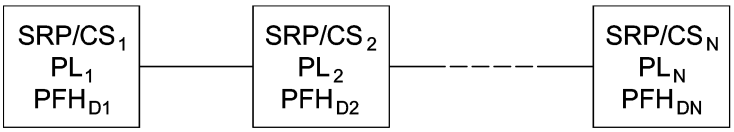
Es werden *N* separate SRP/CS_i in einer Reihenschaltung angenommen, die zusammen eine Sicherheitsfunktion ausführen. Für jedes SRP/CS_i wurde bereits ein PL_i festgelegt. Diese Situation wird in Bild 13 dargestellt (siehe auch Bild 4 und Bild H.2).

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

— den niedrigsten PL eines einzelnen SRP/CS_i, das an der Durchführung der Sicherheitsfunktion beteiligt ist (da der PL auch durch nicht quantifizierbare Aspekte bestimmt wird) und

— den PL, der dem PFH_D des kombinierten SRP/CS nach Tabelle 2 entspricht.

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



SRP/CS
PL
$$\mathbf{PFH_D = PFH_{D1} + PFH_{D2} + \ldots + PFH_{DN}}$$

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

Wenn die PFH_D-Werte aller einzelnen SRP/CS_i nicht bekannt sind, dann darf, als ungünstigster Fall zum vorstehenden Verfahren, der PL des gesamten kombinierten SRP/CS, das die Sicherheitsfunktion ausführt, mithilfe von Tabelle 11 wie folgt berechnet werden:

a) Bestimmen des niedrigsten PL_i, dies ist $PL_{niedrig}$.

b) Bestimmen der Anzahl $N_{niedrig} \leq N$ der SRP/CS_i mit $PL_i = PL_{niedrig}$.

c) Nachschlagen des PL in Tabelle 11.

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

$PL_{niedrig}$	$N_{niedrig}$	⇒	PL
a	> 3	⇒	kein, nicht erlaubt
	≤ 3	⇒	a
b	> 2	⇒	a
	≤ 2	⇒	b
c	> 2	⇒	b
	≤ 2	⇒	c
d	> 3	⇒	c
	≤ 3	⇒	d
e	> 3	⇒	d
	≤ 3	⇒	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 wichtigen Fehler und Ausfälle für verschiedene Technologien auf. Die Fehlerlisten sind nicht vollständig, 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 Ausfallarten und Effekt-Analyse (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 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 des/der sicherheitsbezogenen Teils(e) einer Steuerung muss denen in ISO 12100:2010, 6.2.7 folgen. Alle Informationen der Instandhaltung müssen mit ISO 12100:2010, 6.4.5.1 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 das/die sicherheitsbezogene(n) Teil(e) beginnt/beginnen und endet/enden;

— die Umgebungsbedingungen;

— den Performance Level (PL);

— die ausgewählte Kategorie oder die ausgewählten Kategorien;

— die auf die Zuverlässigkeit bezogenen Parameter ($MTTF_D$, DC, CCF und Gebrauchsdauer);

— 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 12100:2010, 6.4.5.2 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 der/den ausgewählten Kategorie(n) und einem Fehlerausschluss;

— die Grenzen der SRP/CS und einen 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 des/der Fehlerausschlusses/-schlüsse 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 13849-1:2015");

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 13849-1:2015 Kategorie B PL a

Anhang A
(informativ)

Bestimmung des erforderlichen Performance Levels (PL_r)

A.1 Auswahl des PL_r

Anhang A 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.

ANMERKUNG Dieses Verfahren zur Abschätzung des PL_r ist nicht verbindlich. Es ist ein generischer Ansatz, der die ungünstigste Eintrittswahrscheinlichkeit eines Gefährdungsereignisses annimmt (d. h. die Eintrittswahrscheinlichkeit ist 100 %). Andere geeignete Methoden zur Risikoabschätzung für bestimmte Arten von Maschinen können verwendet werden und Erfahrungen im erfolgreichen Umgang mit ähnlichen Maschinen/Gefährdungen sollten bei der Abschätzung von PL_r berücksichtigt werden. Daher kann der erforderliche PL in einer Typ-C-Norm vom demjenigen abweichen, der durch den generischen Ansatz in Bild A.1 ermittelt wird.

Der Graph in Bild A.1 basiert auf der Situation vor Festlegung der beabsichtigten Sicherheitsfunktion (siehe ISO/TR 22100-2:2013). Eine Risikominderung durch technische Maßnahmen unabhängig vom Steuerungssystem (z. B. mechanischer Schutz) oder zusätzliche Sicherheitsfunktionen müssen bei der Bestimmung des PL_r der beabsichtigten Sicherheitsfunktion berücksichtigt werden; in diesem Fall wird der Startpunkt in Bild A.1 nach der Implementierung dieser Maßnahmen gewählt (siehe auch Bild 2).

Die Schwere der Verletzung (gekennzeichnet durch S) ist nur annäherungsweise abgeschätzt (z. B. Fleischwunde, Amputation, Todesfall). Für die Häufigkeit des Auftretens werden Hilfsparameter benutzt, um die Abschätzung 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 nach der Häufigkeit und Dauer des Zugangs zur Gefährdung ausgewählt werden.

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.

Liegt keine andere Rechtfertigung vor, sollte F2 gewählt werden, wenn die Häufigkeit höher als einmal je 15 Minuten ist.

F1 darf gewählt werden, wenn die gesamte Expositionsdauer 1/20 der gesamten Betriebsdauer nicht überschreitet und die Häufigkeit nicht höher als einmal je 15 Minuten ist.

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

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

Wenn die Eintrittswahrscheinlichkeit eines Gefährdungsereignisses als niedrig bewertet werden kann, darf der PL_r um einen Level verringert werden, siehe A.2.3.2.

A.2.3.1 Möglichkeit zur Vermeidung der Gefährdung

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

— Geschwindigkeit, mit der die Gefährdung auftritt (z. B. schnell oder langsam);

— Möglichkeit zur Vermeidung der Gefährdung, (z. B. durch Flucht);

— praktische Erfahrungen mit der Sicherheit in Bezug zum Prozess;

— Betrieb durch ausgebildete und geeignete Bedienungspersonen;

— Betrieb mit oder ohne Beaufsichtigung.

A.2.3.2 Eintrittswahrscheinlichkeit eines Gefährdungsereignisses

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

— Zuverlässigkeitsdaten;

— Unfallgeschichte an vergleichbaren Maschinen.

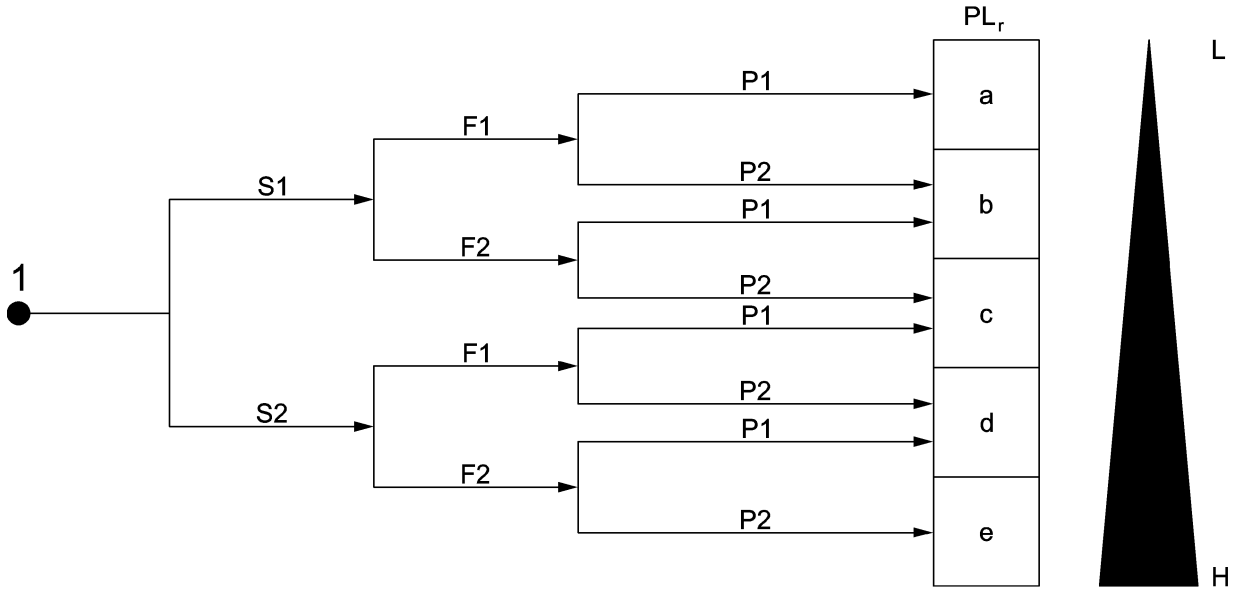
ANMERKUNG Eine geringe Zahl an Unfällen muss nicht zwingend bedeuten, dass das Eintreten von Gefährdungssituationen gering ist, sondern dass die Sicherheitseinrichtungen der Maschine ausreichend sind.

Wobei vergleichbare Maschinen

— dasselbe/dieselben Risiko/Risiken umfassen, die die maßgebliche Sicherheitsfunktion verringern soll,

— den gleichen Prozess und dieselbe Betätigung durch die Bedienungsperson erfordern,

— die gleichen Techniken anwenden, die die Gefährdung verursachen.



Legende

1 Startpunkt zur Bewertung des Sicherheitsfunktionsbeitrags zur 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 oder 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 — Graph zur Bestimmung des erforderlichen PL_r für Sicherheitsfunktion

Bild A.1 gibt eine Anleitung für die Bestimmung des sicherheitsbezogenen PL_r, abhängig von der Risikobeurteilung für die gesamte Maschine. Das Verfahren der Risikobeurteilung basiert auf ISO 12100 (siehe Bild 1 und auch ISO/TR 22100-2). Der Graph sollte für jede Sicherheitsfunktion berücksichtigt werden.

A.3 Überlagerte Gefährdungen

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

Wenn es offenbar eine Kombination direkt verbundener Gefährdungen gibt, die immer gleichzeitig eintreten, dann sollten sie zur Risikoabschätzung zusammengefasst werden.

Die Bewertung, ob Gefährdungen einzeln oder zusammengefasst betrachtet werden sollten, sollte während der Risikobewertung der Maschine getroffen werden.

BEISPIEL 1 Ein kontinuierlich arbeitender Schweißroboter kann gleichzeitig verschiedene Gefährdungssituationen erzeugen, wie z. B. Quetschen durch Bewegen und Verbrennen durch den Schweißvorgang. Diese können als eine Kombination direkt verbundener Gefährdungen betrachtet werden.

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

BEISPIEL 3 Infolge der Risikobeurteilung kann es ausreichend sein, am Rundschalttisch mit Klemmvorrichtungen jede Klemmvorrichtung einzeln zu betrachten.

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 Effekt-Analyse oder die „Parts-Count"-Verfahren (siehe 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 Hardwareeinheiten 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

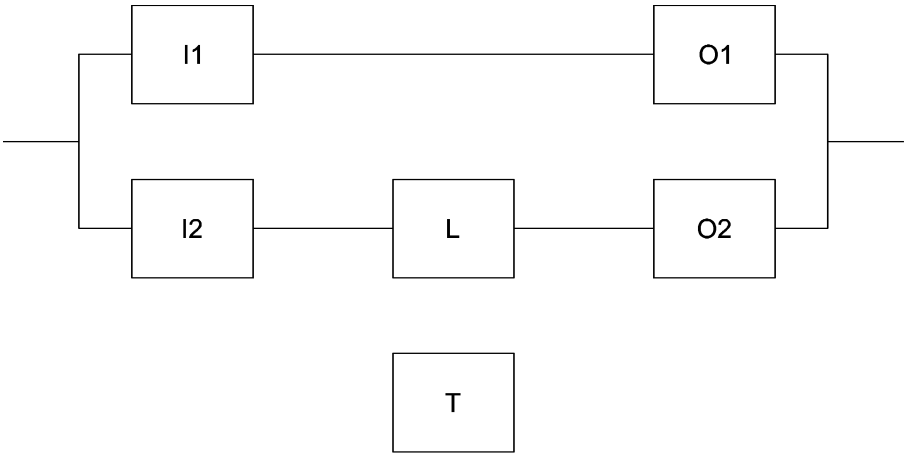
Die durch die Blockmethode definierten Blöcke können verwendet werden, um die logische Struktur der SRP/CS in einem sicherheitsbezogenen Blockdiagramm darzustellen. Für die grafische Darstellung kann folgende Anleitung verwendet werden:

— der Ausfall eines Blocks in einer Serienschaltung von Blöcken führt zu einem Ausfall des gesamten Kanals (z. B. wenn eine Hardwareeinheit in einem Kanal des SRP/CS 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, wenn sie gefährlich ausfallen, können von Blöcken in den verschiedenen Kanälen getrennt werden.

Siehe Bild B.1 als Beispiel.



Legende
I1, I2 Eingabeeinheit, z. B. Sensor
L Logik
O1, O2 Ausgabeeinheiten, z. B. Hauptschütz
T Testeinrichtung
I1 und O1 bilden den ersten Kanal (Serienschaltung).
I2, L und O2 bilden den zweiten Kanal (Serienschaltung), mit beiden Kanälen wird die Sicherheitsfunktion redundant ausgeführt (Parallelschaltung).
T wird nur für die Testung verwendet.

Bild B.1 — Beispiel eines sicherheitsbezogenen Blockdiagramms

Anhang C
(informativ)

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

C.1 Allgemeines

Anhang C 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, mechanische und elektromechanische Bauteile 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 abgeschätzt werden.

a) Die Bauteile werden nach den grundlegenden und bewährten Sicherheitsprinzipien nach ISO 13849-2:2012 hergestellt 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.

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

c) Die Gestaltung des SRP/CS erfüllt die grundlegenden und bewährten Sicherheitsprinzipien nach ISO 13849-2:2012, 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.

a) Die hydraulischen Bauteile werden nach den grundlegenden und bewährten Sicherheitsprinzipien nach ISO 13849-2:2012 hergestellt, 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.

b) Der Hersteller des hydraulischen Bauteils legt die geeignete Anwendung und die Betriebsbedingungen für den SRP/CS-Konstrukteur fest. Der SRP/CS-Konstrukteur muss seiner Verantwortung entsprechend informieren, die grundlegenden und bewährten Sicherheitsprinzipien nach ISO 13849-2:2012, Tabellen C.1 und C.2, für die Implementierung und den Betrieb des hydraulischen Bauteils zu erfüllen.

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

Wenn aber entweder a) oder b) nicht erreicht wird, muss der $MTTF_D$-Wert für das einzelne hydraulische Bauteil durch den Hersteller angegeben werden. Anstatt einen festen Wert für $MTTF_D$ zu verwenden, wie vorstehend beschrieben, ist es zulässig, das B_{10D}-Verfahren für $MTTF_D$ von pneumatischen, mechanischen und elektromechanischen Bauteilen und auch für hydraulische Bauteile zu verwenden, wenn der Hersteller die Daten liefern kann.

Tabelle C.1 — Internationale Normen, die sich mit $MTTF_D$ oder B_{10D} für Bauteile befassen

	Grundlegende und bewährte Sicherheitsprinzipien nach ISO 13849-2:2012	**Relevante Normen**	**Typische Werte:** $MTTF_D$ (Jahre) B_{10D} (Zyklen)
Mechanische Bauteile	Tabellen A.1 und A.2	–	$MTTF_D = 150$
Hydraulische Bauteile mit $n_{op} \geq$ 1 000 000 Zyklen pro Jahr	Tabellen C.1 und C.2	ISO 4413	$MTTF_D = 150$
Hydraulische Bauteile mit 1 000 000 Zyklen pro Jahr $> n_{op} \geq$ 500 000 Zyklen pro Jahr	Tabellen C.1 und C.2	ISO 4413	$MTTF_D = 300$
Hydraulische Bauteile mit 500 000 Zyklen pro Jahr $> n_{op} \geq$ 250 000 Zyklen pro Jahr	Tabellen C.1 und C.2	ISO 4413	$MTTF_D = 600$
Hydraulische Bauteile mit 250 000 Zyklen pro Jahr $> n_{op}$	Tabellen C.1 und C.2	ISO 4413	$MTTF_D = 1\,200$
Pneumatische Bauteile	Tabellen B.1 und B.2	ISO 4414	$B_{10D} = 20\,000\,000$
Relais und Hilfsschütze mit geringer Last	Tabellen D.1 und D.2	EN 50205 IEC 61810 IEC 60947	$B_{10D} = 20\,000\,000$
Relais und Hilfsschütze mit nominaler Last	Tabellen D.1 und D.2	EN 50205 IEC 61810 IEC 60947	$B_{10D} = 400\,000$
Näherungsschalter mit geringer Last	Tabellen D.1 und D.2	IEC 60947 ISO 14119	$B_{10D} = 20\,000\,000$
Näherungsschalter mit nominaler Last	Tabellen D.1 und D.2	IEC 60947 ISO 14119	$B_{10D} = 400\,000$
Schütze mit geringer Last	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	$B_{10D} = 1\,300\,000$ (siehe Anmerkung 1)
Positionsschalter[a]	Tabellen D.1 und D.2	IEC 60947 ISO 14119	$B_{10D} = 20\,000\,000$
Positionsschalter (mit separatem Betätiger, Zuhaltung)[a]	Tabellen D.1 und D.2	IEC 60947 ISO 14119	$B_{10D} = 2\,000\,000$
Not-Halt-Geräte[a]	Tabellen D.1 und D.2	IEC 60947 ISO 13850	$B_{10D} = 100\,000$
Druck-Taster (z. B. Zustimmungsschalter)[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 abgeschätzt als zweimal B_{10} (50 % gefährlicher Ausfall), wenn keine anderen Angaben vorliegen (z. B. Produktnorm).

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

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

[a] Falls Fehlerausschluss 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 und in diesem Teil der ISO 13849 benötig 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 alle folgenden Merkmale erfüllt sind, kann der $MTTF_D$-Wert für ein einzelnes pneumatisches, elektromechanisches oder mechanisches Bauteil nach C.4.2 abgeschätzt werden.

a) Die Bauteile wurden unter Verwendung grundlegender Sicherheitsprinzipien nach ISO 13849-2:2012, Tabelle A.1, Tabelle B.1 oder Tabelle D.1. entworfen und hergestellt.

   ANMERKUNG Diese Information kann im Datenblatt des Bauteilherstellers gefunden werden.

b) Die Bauteile, die in Kategorie 1, 2, 3 oder 4 verwendet werden sollen, wurden unter Verwendung bewährter Sicherheitsprinzipien nach ISO 13849-2:2012, Tabelle A.2, Tabelle B.2 oder Tabelle D.2. entworfen und hergestellt.

   ANMERKUNG Diese Information kann im Datenblatt des Bauteilherstellers gefunden werden.

c) Der Hersteller des Bauteils legt die geeignete Anwendung und die Betriebsbedingungen für den SRP/CS-Konstrukteur fest. Der SRP/CS-Konstrukteur muss seiner Verantwortung entsprechend informieren, die grundlegenden Sicherheitsprinzipien nach ISO 13849-2:2012, Tabellen B.1 oder D.1 für die Implementierung und den Betrieb des Bauteils zu erfüllen. Für Kategorie 1, 2, 3 oder 4 ist der Anwender über seine Verantwortung zu informieren, die bewährten Sicherheitsprinzipien nach ISO 13849-2:2012, 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})[2)], sollte durch den Hersteller des Bauteils in Übereinstimmung mit den entsprechenden Produktnormen für die Prüfung bestimmt werden (z. B. IEC 60957-5-1, 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* gefährlich ausgefallen sind, durchgeführt werden.

Mit B_{10D} und n_{op}, der mittleren Anzahl jährlicher Betätigungen, kann die $MTTF_D$ für Bauteile wie folgt berechnet werden

$$MTTF_D = \frac{B_{10D}}{0{,}1 \times n_{op}} \qquad \text{(C.1)}$$

2) Wenn der gefährliche Anteil des B_{10} nicht angegeben ist (z. B. durch den Hersteller), dürfen 50 % des B_{10} verwendet werden, deshalb wird $B_{10D} = 2\ B_{10}$ empfohlen.

wobei

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

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} die mittlere Betriebszeit zwischen dem Beginn zweier aufeinander folgender 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.

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

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:

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

Die Verfahren der Zuverlässigkeit in diesem Teil der ISO 13849 setzen voraus, dass die Ausfälle von Bauteilen exponentiell über der Zeit verteilt sind: $F(t) = 1 - \exp(-\lambda dt)$. 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

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

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:

$$F(T_{10D}) = 1 - \exp(-\lambda_D T_{10D}) = 10\,\% \text{ bedeutet } \lambda_D = -\frac{\ln(0{,}9)}{T_{10D}} = \frac{0{,}10\,536}{T_{10D}} \approx \frac{0{,}1}{T_{10D}} \quad (C.6)$$

Mit $MTTF_D = 1/\lambda_D$ für eine exponentielle Verteilung ergibt dies

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

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

C.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:

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

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

$$\text{MTTF}_D = \frac{23{,}7\ \text{Jahre}}{0{,}1} = 237\ \text{Jahre} \tag{C.10}$$

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 [46] 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 die Verwendung dieser speziellen Daten anstelle der anderen Daten dringend empfohlen.

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.

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 **Typisch**	**Bemerkungen**
Bipolar	TO18, TO92, SOT23	38 052	76 104	50 % gefahrbringende Ausfälle
Bipolar, niedrige Leistung	TO5, TO39	5 708	11 416	50 % gefahrbringende Ausfälle
Bipolar, Leistung	TO3, TO220, D-Pack	1 903	3 806	50 % gefahrbringende Ausfälle
FET	J-MOS	22 831	45 662	50 % gefahrbringende Ausfälle
MOS, Leistung	TO3, TO220, D-Pack	1 903	3 806	50 % gefahrbringende Ausfälle

Tabelle C.3 — Dioden, Leistungshalbleiter und integrierte Schaltungen

Diode	**Beispiel**	**MTTF für Bauteile** Jahre	**$MTTF_D$ für Bauteile** Jahre **Typisch**	**Bemerkungen**
Allgemeine Anwendung	–	114 155	228 311	50 % gefahrbringende Ausfälle
Entstörgerät	–	16 308	32 616	50 % gefahrbringende Ausfälle
Zenerdiode $P_{tot} < 1$ W	–	114 155	228 311	50 % gefahrbringende Ausfälle
Gleichrichterdioden	–	57 078	114 155	50 % gefahrbringende Ausfälle
Gleichrichterbrücken	–	11 415	22 831	50 % gefahrbringende Ausfälle
Thyristoren	–	2 283	4 566	50 % gefahrbringende Ausfälle
Triacs, Diacs	–	1 522	3 044	50 % gefahrbringende Ausfälle
Integrierte Schaltungen (programmierbar und nicht programmierbar)	Herstellerdaten verwenden			50 % gefahrbringende Ausfälle

C.5.3 Passive Bauteile

Siehe Tabellen C.4 bis C.7.

Tabelle C.4 — Kondensatoren

Kondensator	Beispiel	MTTF für Bauteile Jahre	$MTTF_D$ für Bauteile Jahre Typisch	Bemerkungen
Standard, keine Leistung	KS, KP, KC, KT, MKT, MKC, MKP, MKU, MP, MKV	57 078	114 155	50 % gefahrbringende Ausfälle
Keramik	–	22 831	45 662	50 % gefahrbringende Ausfälle
Aluminiumelektrolyt	flüssiges Elektrolyt	22 831	45 662	50 % gefahrbringende Ausfälle
Aluminiumelektrolyt	festes Elektrolyt	38 052	76 104	50 % gefahrbringende Ausfälle
Tantalelektrolyt	flüssiges Elektrolyt	11 415	22 831	50 % gefahrbringende Ausfälle
Tantalelektrolyt	festes Elektrolyt	114 155	228 311	50 % gefahrbringende Ausfälle

Tabelle C.5 — Widerstände

Widerstand	Beispiel	MTTF für Bauteile Jahre	$MTTF_D$ für Bauteile Jahre Typisch	Bemerkungen
Kohleschicht	–	114 155	228 311	50 % gefahrbringende Ausfälle
Metallfilm	–	570 776	1 141 552	50 % gefahrbringende Ausfälle
Metalloxid und gewendelt	–	22 831	45 662	50 % gefahrbringende Ausfälle
Variabel	–	3 805	7 618	50 % gefahrbringende Ausfälle

Tabelle C.6 — Induktivitäten

Induktivität	Beispiel	MTTF für Bauteile Jahre	$MTTF_D$ für Bauteile Jahre Typisch	Bemerkungen
Für MC-Anwendung	–	38 052	76 104	50 % gefahrbringende Ausfälle
Niederfrequenz-Induktivitäten und Transformatoren	–	22 831	45 662	50 % gefahrbringende Ausfälle
Leistungstransformatoren und Transformatoren für Schaltanwendungen und Netzteile	–	11 415	22 831	50 % gefahrbringende Ausfälle

Tabelle C.7 — Optokoppler

Optokoppler	**Beispiel**	**MTTF für Bauteile** Jahre	**$MTTF_D$ für Bauteile** Jahre **Typisch**	**Bemerkungen**
Bipolar Ausgang	SFH 610	7 610	15 220	50 % gefahrbringende Ausfälle
FET Ausgang	LH 1056	2 854	5 708	50 % gefahrbringende Ausfälle

Anhang D
(informativ)

Vereinfachtes Verfahren zur Abschätzung 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 verwendet[3)].

Die allgemeine Gleichung ist

$$\frac{1}{\mathrm{MTTF_D}} = \sum_{i=1}^{\tilde{N}} \frac{1}{\mathrm{MTTF_{D}}i} = \sum_{j=1}^{\tilde{N}} \frac{n_\mathrm{j}}{\mathrm{MTTF_{D}}j} \tag{D.1}$$

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 22,4 Jahren, was „mittel“ nach Tabelle 5 entspricht.

Tabelle D.1 — Beispiel der Teileliste auf einer Platine

j	**Bauteil**	**Anzahl** n_j	**$MTTF_{Dj}$ typisch** Jahre	**$1/MTTF_{Dj}$ typisch** 1/Jahr	$n_j/MTTF_{Dj}$ **typisch** 1/Jahr
1	Transistoren, Bipolar, Kleinleistung (siehe Tabelle C.2)	2	11 416	0,000 087 6	0,000 175 2
2	Widerstand, Kohlefilm (siehe Tabelle C.5)	5	228 311	0,000 004 4	0,000 021 9
3	Kondensator, Standard, keine Leistung (siehe Tabelle C.4)	4	114 155	0,000 008 8	0,000 035 0
4	Relais, vom Hersteller angegebener Wert (B10D = 20 000 000 Zyklen, nop = 633 600 Zyklen pro Jahr)	4	315,7	0,003 167 6	0,012 670 3

3) 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.

j	Bauteil	Anzahl n_j	$MTTF_{Dj}$ typisch Jahre	$1/MTTF_{Dj}$ typisch 1/Jahr	$n_j/MTTF_{Dj}$ typisch 1/Jahr
5	Schütz, vom Hersteller angegebener Wert (B10D = 2 000 000 Zyklen, nop = 633 600 Zyklen pro Jahr)	1	31,6	0,031 645 6	0,031 645 6
$\Sigma (n_j/MTTF_{Dj})$					0,044 548 0
$MTTF_D = 1/\Sigma (n_j/MTTF_{Dj})$ [Jahre]					22,4

ANMERKUNG 1 Dieses Verfahren basiert auf der Annahme, dass ein gefährlicher Ausfall irgendeines Bauteils (Abschätzung des ungünstigsten Falls) im Kanal zu einem gefährlichen Ausfall des Kanals führt. Die $MTTF_D$-Berechnung der Tabelle D.1 basiert auf dieser 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 t_{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 einer 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;

— Gleichung D.2 kann zur Einschätzung eines Ersatzwertes für $MTTF_D$ für jeden Kanal verwendet werden:

$$MTTF_D = \frac{2}{3}\left[MTTF_{DC1} + MTTF_{DC2} - \frac{1}{\frac{1}{MTTF_{DC1}} + \frac{1}{MTTF_{DC2}}}\right] \quad \text{(D.2)}$$

wobei $MTTF_{DC1}$ und $MTTF_{DC2}$ die Werte für zwei unterschiedliche redundante Kanäle sind, die jeweils auf einen Höchstwert von 100 Jahren (Kategorien B, 1, 2 und 3) oder 2 500 Jahren (Kategorie 4) begrenzt sind, bevor Gleichung (D.2) angewendet wird.

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 Betätigungselementen)	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 %
Logik	
Indirekte Überwachung (z. B. Überwachung durch Druckschalter, elektrische Positionsüberwachung von Betätigungselementen)	90 % bis 99 %, abhängig von der Anwendung
Direkte Überwachung (z. B. elektrische Überwachung der Steuerungsventile, Überwachung elektromechanischer Einheiten durch Zwangsführung)	99 %

Tabelle E.1 *(fortgesetzt)*

Maßnahme	**DC**
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 Relaistechnik	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 !
Ausgabeeinheit	
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 dynamischen 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 mit Überwachung der Betätigungselemente durch die Logik und Testeinrichtung	99 %
Indirekte Überwachung (z. B. Überwachung durch Druckschalter, elektrische Positionsüberwachung von Betätigungselementen)	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 61508-2:2010, 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 dürfen auch andere Maßnahmen als die in dieser Tabelle aufgelisteten verwendet werden. ANMERKUNG 3 Für Maßnahmen, für die ein Bereich des Diagnosedeckungsgrades angegeben ist (z. B. Fehlererkennung durch den Prozess), kann der richtige DC-Wert durch Betrachten aller gefahrbringenden Ausfälle bestimmt werden und anschließend die Entscheidung getroffen werden, welcher von ihnen durch die DC-Maßnahme erkannt wird. Im Zweifelsfall sollte eine FMEA die Grundlage für die Abschätzung des DC darstellen.	

Für die Anwendung von Tabelle E.1 sind die hinweisenden Beispiele zu beachten.

BEISPIEL 1 Anhang E der ISO 13949-2 zeigt ein vollständiges Beispiel (sehr detailliert) zur Validierung des Fehlerverhaltens und Mittel zur Diagnose einer automatischen Montageanlage.

BEISPIEL 2 ISO/TR 24119 beschreibt ein anwendungsbezogenes Schritt-für-Schritt-Verfahren zur Bestimmung des Diagnosedeckungsgrades für in Reihe geschaltete Verriegelungseinrichtungen.

BEISPIEL 3 Die DC Maßnahme „Fehlererkennung durch den Prozess“ darf nur angewendet werden, wenn das sicherheitsbezogene Bauteil am Fertigungsprozess beteiligt ist, z. B. wenn eine normale PLC oder normale Sensoren für die Fertigung eines Werkstücks benutzt werden, und als Teil von einem von zwei redundanten Funktionskanälen, die die Sicherheitsfunktion ausführen, fungieren. Das geeignete DC Level hängt von der Überschneidung der gewöhnlich verwendeten Ressourcen (Logik, Eingänge/Ausgänge, usw.) ab. Wenn z. B. alle Fehler eines Drehreglers in einer Druckmaschine zu stark sichtbaren Fehlern im Druckvorgang führen, wird der DC für den Sensor der eine sicher begrenzte Geschwindigkeit überwacht zwischen 90 % und 99 % angenommen.

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 Diagnosedeckungsgrad DC_{avg} mit folgender Gleichung abgeschätzt:

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \cdots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \cdots + \frac{1}{MTTF_{DN}}} \quad \text{(E.1)}$$

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/Betätigungselemente und besonders für Steuerelektroniken wird z. B. in IEC 61508-6:2000, Anhang D gegeben. Nicht alle Maßnahmen, die darin gegeben werden, sind für Maschinen 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 — Verfahren zur Punktevergabe und Quantifizierung für Maßnahmen gegen CCF

Nr.	Maßnahme gegen CCF	Punkt-zahl
1	**Trennung/Abtrennung**	
	Physikalische Trennung zwischen den Signalpfaden, z. B.: — Trennung der Verdrahtung/Verrohrung; — Erkennen von Kurzschlüssen und Unterbrechungen in Kabeln durch dynamische Prüfung; — getrennte Abschirmung des Signalpfads jedes Kanals; — ausreichende Luft- und Kriechstrecken auf gedruckten Schaltungen.	**15**
2	**Diversität**	
	Unterschiedliche Technologien/Gestaltung oder physikalische Prinzipien werden verwendet, z. B.: — der erste Kanal elektronisch oder programmierbar elektronisch und der zweite Kanal elektromechanisch fest verdrahtet, — unterschiedliche Initiierung der Sicherheitsfunktion für jeden Kanal (z. B. Position, Druck, Temperatur), und/oder digitale und analoge Messung von Variablen (z. B. Abstand, Druck oder Temperatur) und/oder Bauteile von unterschiedlichen Herstellern.	**20**
3	**Gestaltung/Anwendung/Erfahrung**	
3.1	Schutz gegen Überspannung, Überdruck, Überstrom, Übertemperatur, usw.	**15**
3.2	Verwendung bewährter Bauteile.	**5**
4	**Beurteilung/Analyse**	
	Für jedes Teil von sicherheitsbezogenen Teilen eines Steuerungssystems wurde eine Ausfallarten- und Effekt-Analyse durchgeführt und deren Ergebnisse berücksichtigt, um Ausfälle infolge gemeinsamer Ursache bei der Gestaltung zu vermeiden.	**5**
5	**Kompetenz/Ausbildung**	
	Ausbildung der Konstrukteure, um die Gründe und Auswirkungen von Ausfällen infolge gemeinsamer Ursache zu verstehen.	**5**
6	**Umgebung**	
6.1	Für elektrische/elektronische Systeme, Verhindern von Verunreinigungen und elektromagnetischen Störungen (EMV) zum Schutz vor Ausfällen infolge gemeinsamer Ursache entsprechend den einschlägigen Normen (z. B. IEC 61326-3-1) Fluidische Systeme: Filtrierung des Druckmediums, Verhinderung von Schmutzeintrag, Entwässerung von Druckluft, z. B. in Übereinstimmung mit den Anforderungen des Herstellers für die Reinheit des Druckmediums ANMERKUNG Bei kombinierten fluidischen und elektrischen Systemen sollten beide Aspekte berücksichtigt werden.	**25**
6.2	Andere Einflüsse: Berücksichtigung der Anforderungen hinsichtlich Unempfindlichkeit gegenüber allen relevanten Umgebungsbedingungen wie Temperatur, Schock, Vibration, Feuchte (z. B. wie in den zutreffenden Normen festgelegt).	**10**
	Gesamt	**[max. erreich-bar 100]**

Gesamtpunktzahl	Maßnahmen, um CCF[a] zu vermeiden
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 13849-2:2012, 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 ingenieursmäßiger Praxis.

— Kompatibilität

Verwenden von Bauteilen mit kompatiblen Betriebskenndaten.

ANMERKUNG 1 Bauteile, wie z. B. hydraulische oder pneumatische Ventile, können zyklisches Schalten erfordern, um Ausfälle durch Nicht-Schalten oder inakzeptablen Anstieg der Schaltzeiten zu vermeiden. In diesem Fall ist eine wiederkehrende Prüfung notwendig.

— 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 13849-2:2012, 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).

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).

ANMERKUNG 2 IEC 61508-2:2010, Anhang F legt Techniken und Maßnahmen zur Vermeidung systematischer Ausfälle während des Entwurfs und der Entwicklung von anwendungsspezifischen integrierten Schaltungen (ASIC), feldprogrammierbaren Gate-Arrays (FPGA), programmierbaren Logikbausteinen (PLD), usw. fest.

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-Betätigungselement anzusteuern. Dies ist kein Funktionsschaltbild/Arbeitsdiagramm und wird nur gezeigt, um das Prinzip der Zusammenschaltung der Kategorien und Technologien in dieser einen 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 fluidischen Betätigungselements 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 Betätigungselements.

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.

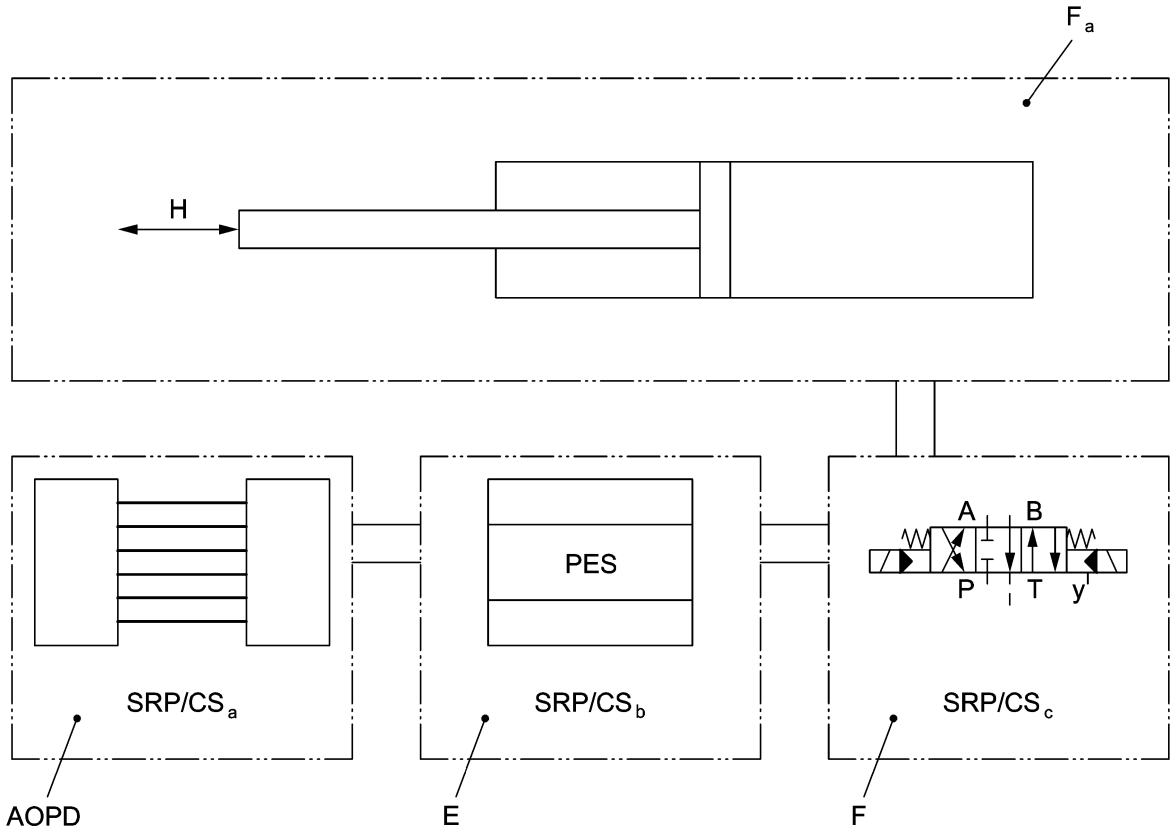
— Kategorie 3, PL = d für die elektronische Steuerung. Um den Beitrag der elektronischen Steuerung zur Sicherheit zu erhöhen, ist die Struktur der SRP/CS redundant und enthält einige Fehlererkennungsmechanismen, sodass die meisten Einzelfehler erkannt werden.

— 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 $PL_{niedrig}$ = c und $N_{niedrig}$ = 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.



Legende

AOPD aktive opto-elektronische Schutzeinrichtung (z. B. Lichtschranke), SRP/CS_a: Kategorie 2 [Typ 2], PL = c

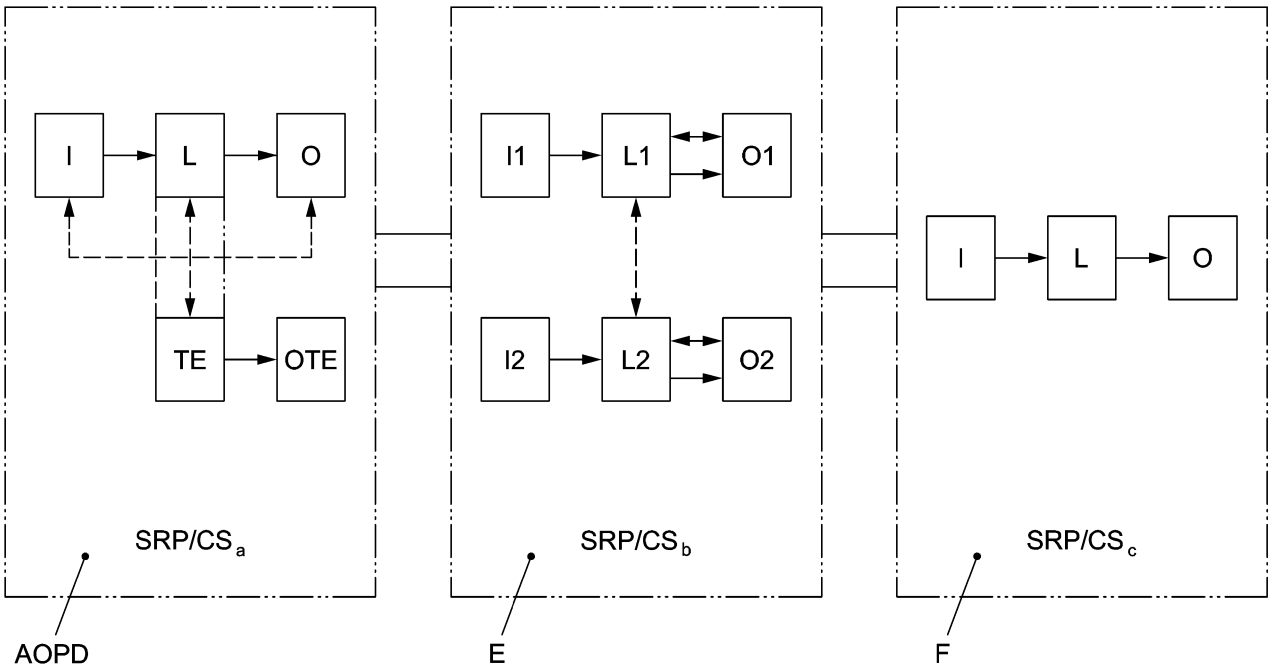
E elektronische Steuerungslogik, SRP/CS_b: Kategorie 3, PL = d

F Fluidtechnik, SRP/CS_c: Kategorie 1, PL = c

F_a fluidtechnischer Betätiger

H gefahrbringende 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	Fluidtechnik
I, l1, 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

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

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

I.2 Sicherheitsfunktion und erforderlicher Performance Level (PL_r)

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

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

ANMERKUNG Für das Beispiel B hat die Risikobeurteilung festgestellt, dass ein Verlust des kontrollierten Abbremsens des Motors infolge einer Fehlfunktion (SW2, CC oder PLC) annehmbar war.

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

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

— Schwere der Verletzung, S = S2, ernst;

— Häufigkeit und/oder Dauer der Gefährdungsexposition, *F* = F1, selten bis weniger häufig und/oder die Gefährdungsexpositionszeit ist kurz;

— Möglichkeit zur Vermeidung der Gefährdung, *P* = P1, möglich unter bestimmten Voraussetzungen.

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

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

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

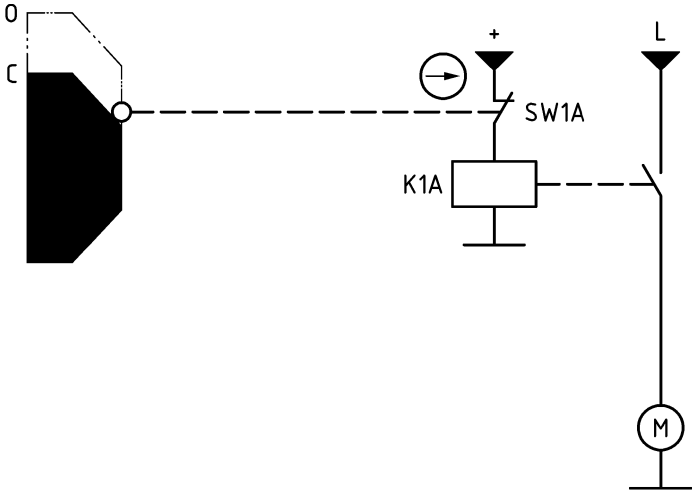
Diese Entscheidungen führen zu einem erforderlichen Performance Level PL_r von „d“.

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

I.3 Beispiel A, einkanaliges System

I.3.1 Identifikation der sicherheitsbezogenen Teile

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



Legende

o	Sicherheitsverriegelung ist offen
c	Sicherheitsverriegelung ist geschlossen
M	Motor
K1A	Hilfsschütz
SW1A	Positionsschalter (NC)
⊖	Zwangsöffnung

Bild I.1 — Schaltplan A zur Ausführung der Sicherheitsfunktion

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

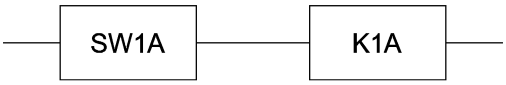
— ein Kanal aus elektromechanischen Bauteilen;

— Positionsschalter SW1A (NC) hat zwangsöffnende Kontakte und hohen B_{10D};

— Hilfsschütz K1A hat hohen B_{10D}.

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

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



Legende
K1A Hilfsschütz
SW1A Positionsschalter

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

I.3.2 Quantifizierung von $MTTF_D$, DC_{avg}, Maßnahmen gegen den Ausfall infolge gemeinsamer Ursache (CCF), Kategorie, PL

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

— **$MTTF_D$**

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

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

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

ANMERKUNG Wenn keine B_{10D}-Informationen zu SW1A oder K1A zur Verfügung stehen, könnte eine Annahme für den ungünstigsten Fall nach C.2 oder C.4 gemacht werden.

— **T_{10D}**

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

— **DC**

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

— **CCF**

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

— **Kategorie**

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

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

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

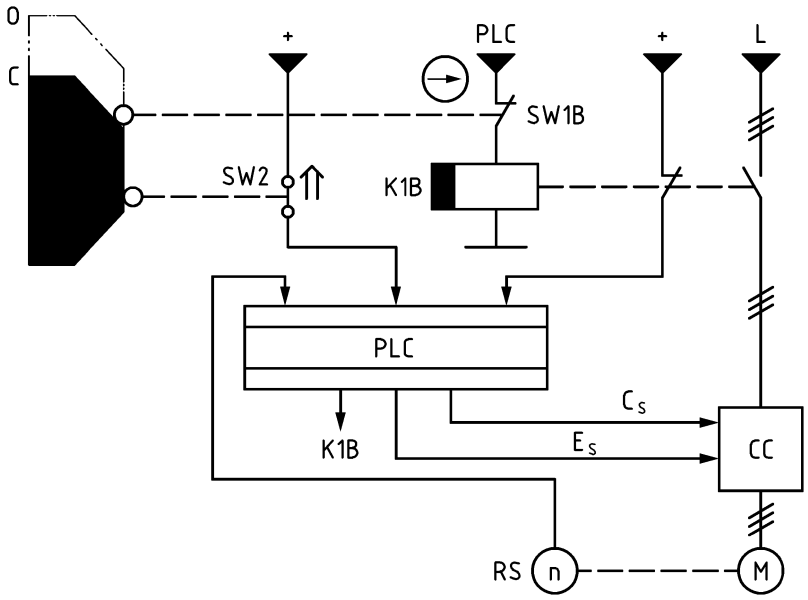
Die Anwendung von Anhang K ergibt eine mittlere Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (PFH_D) von $1{,}14 \times 10^{-6}$/h und PL c.

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

I.4 Beispiel B, redundantes System

I.4.1 Identifikation der sicherheitsbezogenen Teile

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



Legende

PLC	speicherprogrammierbare Steuerung	C_s	Stopp-Signal (normal)
CC	Stromrichter	E_s	Freigabe (normal)
M	Motor	K1B	Hilfsschütz
RS	Drehgeber	SW1B	Positionsschalter (NC)
o	Sicherheitsverriegelung ist offen	SW2	Positionsschalter (NO)
c	Sicherheitsverriegelung ist geschlossen	⇑	Zwangsöffnung

Bild I.3 — Schaltplan B zur Ausführung der Sicherheitsfunktion

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

— redundante Kanäle, ein elektromechanischer und ein programmierbar elektronischer;

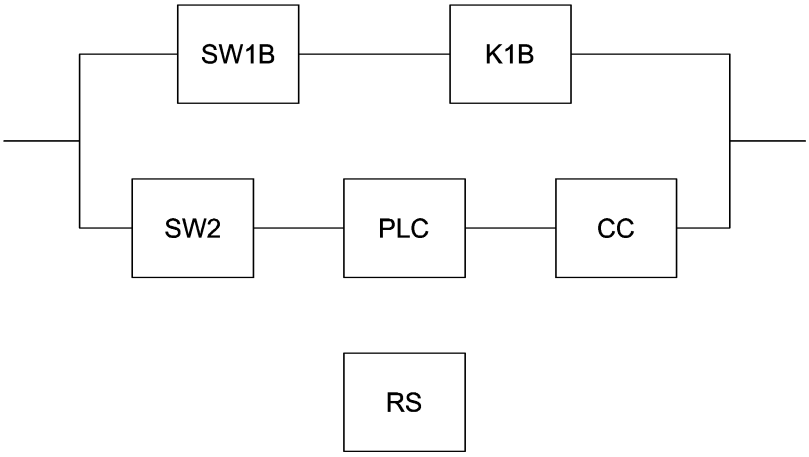
— nur der Positionsschalter SW1B (NC) verfügt über zwangsöffnende Kontakte, aber beide Positionsschalter SW1B und SW2 haben einen hohen B_{10D};

— die $MTTF_D$ des Hilfsschützes K1B ist hoch;

— die $MTTF_D$ der elektronischen Bauteile PLC und CC sind mittel;

— die sicherheitsbezogene Anwendungssoftware der PLC (SRASW), z. B. der mit der Überwachung der Eingangssignale SW2, K1B, RS und der Ausgabeanweisungen an den Stromrichter befasste Teil der Software ist nach 4.6.3 für eine PL_r von „d“ festgelegt, entworfen und geprüft.

Die sicherheitsbezogenen Teile und ihre Aufteilung in Kanäle kann in einem sicherheitsbezogenen Blockdiagram, wie in Bild I.4 gezeigt, dargestellt werden. Der erste Kanal besteht somit aus SW1B und K1B und der zweite Kanal besteht aus SW2, PLC und CC, während RS nur zur Prüfung des Stromrichters verwendet wird.



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

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

I.4.2 Quantifizierung der $MTTF_D$ für jeden Kanal, DC_{avg}, Maßnahmen gegen den Ausfall infolge gemeinsamer Ursache (CCF), Kategorie und PL

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

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

— **$MTTF_D$**

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

$$\frac{1}{MTTF_{D,C1}} = \frac{1}{MTTF_{D,SW1B}} + \frac{1}{MTTF_{D,K1B}} = \frac{1}{2\,778\,\text{Jahre}} + \frac{1}{56\,\text{Jahre}} = \frac{0,0182}{\text{Jahre}} \quad \text{(I.2)}$$

woraus sich $MTTF_D = 55$ Jahre für den Kanal ergibt, der „hoch“ nach 4.5.2, Tabelle 5 ist.

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

$$\frac{1}{\mathrm{MTTF_{D,C2}}} = \frac{1}{\mathrm{MTTF_{D,SW2}}} + \frac{1}{\mathrm{MTTF_{D,PLC}}} + \frac{1}{\mathrm{MTTF_{D,CC}}} = \frac{1}{139\,\mathrm{Jahre}} + \frac{1}{20\,\mathrm{Jahre}} + \frac{1}{20\,\mathrm{Jahre}} = \frac{0,0107}{\mathrm{Jahre}} \qquad \text{(I.3)}$$

woraus sich $\mathrm{MTTF_D} = 9,3$ Jahre für den Kanal ergibt, der „niedrig“ nach 4.5.2 ist.

ANMERKUNG Wenn keine $\mathrm{MTTF_D}$-Informationen für SW1B, SW2 oder K1B zur Verfügung stehen, könnte eine Annahme für den ungünstigsten Fall nach C.2 oder C.4 gemacht werden.

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

— **$\mathrm{T_{10D}}$**

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

— **DC**

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

1) $\mathrm{DC_{SW1B}} = \mathrm{DC_{SW2}} = 99$ %, „hoch“, aufgrund Plausibilitätsprüfung, siehe Tabelle E.1 (zweite Zeile des Teils *Eingabeeinheit*);

2) $\mathrm{DC_{K1B}} = 99$ %, „hoch“, aufgrund der zwangsgeführten Öffner-/Schließer-Kombination, siehe Tabelle E.1 (zweite Zeile des Teils *Eingabeeinheit*);

3) $\mathrm{DC_{PLC}} = 30$ %, „kein“, aufgrund der niedrigen Wirksamkeit der Selbsttests (der Hersteller des PLC gibt den Wert auf Grundlage einer Berechnung durch beispielsweise FMEA an), und

4) $\mathrm{DC_{CC}} = 90$ %, „mittel“, aufgrund indirekter Überwachung der Betätigungselemente durch die Steuerung, siehe Tabelle E.1 (sechste Zeile des Teils *Ausgabeeinheit*) — wenn die PLC einen Ausfall des CC bemerkt, ist es möglich, die Bewegung mit dem Freigabe-Signal (normal) anzuhalten und das Hilfsschütz K1B abzuschalten (zusätzlicher Abschaltpfad).

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

$$\mathrm{DC_{avg}} = \frac{\frac{\mathrm{DC_{SW1B}}}{\mathrm{MTTF_{D,SW1B}}} + \frac{\mathrm{DC_{K1B}}}{\mathrm{MTTF_{D,K1B}}} + \frac{\mathrm{DC_{SW2}}}{\mathrm{MTTF_{D,SW2}}} + \frac{\mathrm{DC_{PLC}}}{\mathrm{MTTF_{D,PLC}}} + \frac{\mathrm{DC_{CC}}}{\mathrm{MTTF_{D,CC}}}}{\frac{1}{\mathrm{MTTF_{D,SW1B}}} + \frac{1}{\mathrm{MTTF_{D,K1B}}} + \frac{1}{\mathrm{MTTF_{D,SW2}}} + \frac{1}{\mathrm{MTTF_{D,PLC}}} + \frac{1}{\mathrm{MTTF_{D,CC}}}} \qquad \text{(I.4)}$$

$$= \frac{\frac{0,99}{2\,778\,\mathrm{Jahre}} + \frac{0,99}{56\,\mathrm{Jahre}} + \frac{0,99}{139\,\mathrm{Jahre}} + \frac{0,3}{20\,\mathrm{Jahre}} + \frac{0,9}{20\,\mathrm{Jahre}}}{\frac{1}{2\,778\,\mathrm{Jahre}} + \frac{1}{56\,\mathrm{Jahre}} + \frac{1}{139\,\mathrm{Jahre}} + \frac{1}{20\,\mathrm{Jahre}} + \frac{1}{20\,\mathrm{Jahre}}} = \frac{0,09}{0,13} = 67,9\ \%$$

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

— **CCF**

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

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

Nr.	Betrachtungseinheit	Punktzahl für den Steuerstromkreis	Maximal mögliches Ergebnis
1	**Trennung/Abtrennung**		
	Physikalische Trennung zwischen den Signalpfaden	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, Übertemperatur, usw.	15	15
3.2	Verwendung bewährter Bauteile	kein (nur teilweise erfüllt, siehe F.2)	5
4	**Beurteilung/Analyse**		
	Für jedes Teil von sicherheitsbezogenen Teilen eines Steuerungssystems wurde eine Ausfallarten- und Effekt-Analyse durchgeführt und deren Ergebnisse berücksichtigt, um Ausfälle infolge gemeinsamer Ursache bei der Gestaltung zu vermeiden.	Kein	5
5	**Kompetenz/Ausbildung**		
	Ausbildung der Konstrukteure, um die Gründe und Auswirkungen von Ausfällen infolge gemeinsamer Ursache zu verstehen.	Kein	5
6	**Umgebung**		
6.1	Für elektrische/elektronische Systeme, Verhindern von Verunreinigungen und elektromagnetischen Störungen (EMV) zum Schutz vor Ausfällen infolge gemeinsamer Ursache entsprechend den einschlägigen Normen (z. B. IEC 61326-3-1)	25	25
6.2	**Andere Einflüsse** Berücksichtigung der Anforderungen hinsichtlich Unempfindlichkeit gegenüber allen relevanten Umgebungsbedingungen wie Temperatur, Schock, Vibration, Feuchte (z. B. wie in den zutreffenden Normen festgelegt).	10	10
	Gesamt	85	Max. 100

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

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

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

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

Die Anwendung von Anhang K (bei 36 Jahren) ergibt eine mittlere Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (PFH_D) von $5{,}16 \times 10^{-7}$/h und PL d.

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

Anhang J
(informativ)

Software

J.1 Beschreibung des Beispiels

In Anhang J 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 Betätiger.

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

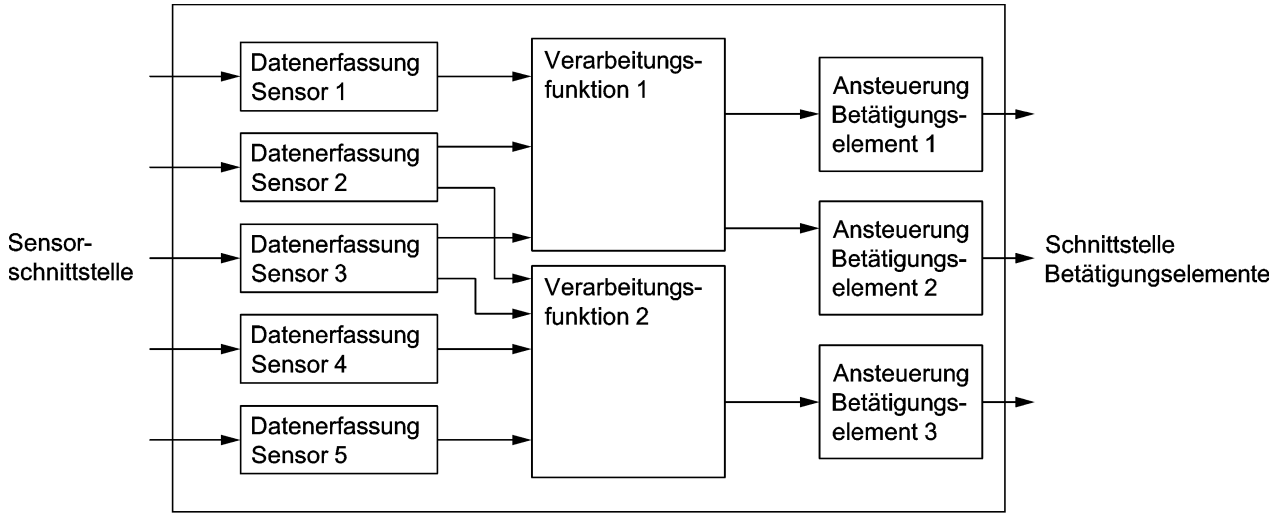


Bild J.1 — Entwurf eines Softwarebeispiels als Funktionsblockschaltbild

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.

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“
Architekturaspekt: Definition der Steuerungsarchitektur mit Sensoren und Betätigungs-elementen	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)	„Softwarebeschreibungen“
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	„Kommentierungen 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 Paragrafen 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 Softwarespezifikation 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 sollten 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, PFH_D (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**
3	$3{,}80 \times 10^{-5}$	a			$2{,}58 \times 10^{-5}$	a	$1{,}99 \times 10^{-5}$	a	$1{,}26 \times 10^{-5}$	a	$6{,}09 \times 10^{-6}$	b		
3,3	$3{,}46 \times 10^{-5}$	a			$2{,}33 \times 10^{-5}$	a	$1{,}79 \times 10^{-5}$	a	$1{,}13 \times 10^{-5}$	a	$5{,}41 \times 10^{-6}$	b		
3,6	$3{,}17 \times 10^{-5}$	a			$2{,}13 \times 10^{-5}$	a	$1{,}62 \times 10^{-5}$	a	$1{,}03 \times 10^{-5}$	a	$4{,}86 \times 10^{-6}$	b		
3,9	$2{,}93 \times 10^{-5}$	a			$1{,}95 \times 10^{-5}$	a	$1{,}48 \times 10^{-5}$	a	$9{,}37 \times 10^{-6}$	b	$4{,}40 \times 10^{-6}$	b		
4,3	$2{,}65 \times 10^{-5}$	a			$1{,}76 \times 10^{-5}$	a	$1{,}33 \times 10^{-5}$	a	$8{,}39 \times 10^{-6}$	b	$3{,}89 \times 10^{-6}$	b		
4,7	$2{,}43 \times 10^{-5}$	a			$1{,}60 \times 10^{-5}$	a	$1{,}20 \times 10^{-5}$	a	$7{,}58 \times 10^{-6}$	b	$3{,}48 \times 10^{-6}$	b		
5,1	$2{,}24 \times 10^{-5}$	a			$1{,}47 \times 10^{-5}$	a	$1{,}10 \times 10^{-5}$	a	$6{,}91 \times 10^{-6}$	b	$3{,}15 \times 10^{-6}$	b		
5,6	$2{,}04 \times 10^{-5}$	a			$1{,}33 \times 10^{-5}$	a	$9{,}87 \times 10^{-6}$	b	$6{,}21 \times 10^{-6}$	b	$2{,}80 \times 10^{-6}$	c		
6,2	$1{,}84 \times 10^{-5}$	a			$1{,}19 \times 10^{-5}$	a	$8{,}80 \times 10^{-6}$	b	$5{,}53 \times 10^{-6}$	b	$2{,}47 \times 10^{-6}$	c		
6,8	$1{,}68 \times 10^{-5}$	a			$1{,}08 \times 10^{-5}$	a	$7{,}93 \times 10^{-6}$	b	$4{,}98 \times 10^{-6}$	b	$2{,}20 \times 10^{-6}$	c		
7,5	$1{,}52 \times 10^{-5}$	a			$9{,}75 \times 10^{-6}$	b	$7{,}10 \times 10^{-6}$	b	$4{,}45 \times 10^{-6}$	b	$1{,}95 \times 10^{-6}$	c		
8,2	$1{,}39 \times 10^{-5}$	a			$8{,}87 \times 10^{-6}$	b	$6{,}43 \times 10^{-6}$	b	$4{,}02 \times 10^{-6}$	b	$1{,}74 \times 10^{-6}$	c		
9,1	$1{,}25 \times 10^{-5}$	a			$7{,}94 \times 10^{-6}$	b	$5{,}71 \times 10^{-6}$	b	$3{,}57 \times 10^{-6}$	b	$1{,}53 \times 10^{-6}$	c		
10	$1{,}14 \times 10^{-5}$	a			$7{,}18 \times 10^{-6}$	b	$5{,}14 \times 10^{-6}$	b	$3{,}21 \times 10^{-6}$	b	$1{,}36 \times 10^{-6}$	c		

	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde, PFH_D (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**
11	$1{,}04 \times 10^{-5}$	a			$6{,}44 \times 10^{-6}$	b	$4{,}53 \times 10^{-6}$	b	$2{,}81 \times 10^{-6}$	c	$1{,}18 \times 10^{-6}$	c		
12	$9{,}51 \times 10^{-6}$	b			$5{,}84 \times 10^{-6}$	b	$4{,}04 \times 10^{-6}$	b	$2{,}49 \times 10^{-6}$	c	$1{,}04 \times 10^{-6}$	c		
13	$8{,}78 \times 10^{-6}$	b			$5{,}33 \times 10^{-6}$	b	$3{,}64 \times 10^{-6}$	b	$2{,}23 \times 10^{-6}$	c	$9{,}21 \times 10^{-7}$	d		
15	$7{,}61 \times 10^{-6}$	b			$4{,}53 \times 10^{-6}$	b	$3{,}01 \times 10^{-6}$	b	$1{,}82 \times 10^{-6}$	c	$7{,}44 \times 10^{-7}$	d		
16	$7{,}13 \times 10^{-6}$	b			$4{,}21 \times 10^{-6}$	b	$2{,}77 \times 10^{-6}$	c	$1{,}67 \times 10^{-6}$	c	$6{,}76 \times 10^{-7}$	d		
18	$6{,}34 \times 10^{-6}$	b			$3{,}68 \times 10^{-6}$	b	$2{,}37 \times 10^{-6}$	c	$1{,}41 \times 10^{-6}$	c	$5{,}67 \times 10^{-7}$	d		
20	$5{,}71 \times 10^{-6}$	b			$3{,}26 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}22 \times 10^{-6}$	c	$4{,}85 \times 10^{-7}$	d		
22	$5{,}19 \times 10^{-6}$	b			$2{,}93 \times 10^{-6}$	c	$1{,}82 \times 10^{-6}$	c	$1{,}07 \times 10^{-6}$	c	$4{,}21 \times 10^{-7}$	d		
24	$4{,}76 \times 10^{-6}$	b			$2{,}65 \times 10^{-6}$	c	$1{,}62 \times 10^{-6}$	c	$9{,}47 \times 10^{-7}$	d	$3{,}70 \times 10^{-7}$	d		
27	$4{,}23 \times 10^{-6}$	b			$2{,}32 \times 10^{-6}$	c	$1{,}39 \times 10^{-6}$	c	$8{,}04 \times 10^{-7}$	d	$3{,}10 \times 10^{-7}$	d		
30			$3{,}80 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}21 \times 10^{-6}$	c	$6{,}94 \times 10^{-7}$	d	$2{,}65 \times 10^{-7}$	d	$9{,}54 \times 10^{-8}$	e
33			$3{,}46 \times 10^{-6}$	b	$1{,}85 \times 10^{-6}$	c	$1{,}06 \times 10^{-6}$	c	$5{,}94 \times 10^{-7}$	d	$2{,}30 \times 10^{-7}$	d	$8{,}57 \times 10^{-8}$	e
36			$3{,}17 \times 10^{-6}$	b	$1{,}67 \times 10^{-6}$	c	$9{,}39 \times 10^{-7}$	d	$5{,}16 \times 10^{-7}$	d	$2{,}01 \times 10^{-7}$	d	$7{,}77 \times 10^{-8}$	e
39			$2{,}93 \times 10^{-6}$	c	$1{,}53 \times 10^{-6}$	c	$8{,}40 \times 10^{-7}$	d	$4{,}53 \times 10^{-7}$	d	$1{,}78 \times 10^{-7}$	d	$7{,}11 \times 10^{-8}$	e
43			$2{,}65 \times 10^{-6}$	c	$1{,}37 \times 10^{-6}$	c	$7{,}34 \times 10^{-7}$	d	$3{,}87 \times 10^{-7}$	d	$1{,}54 \times 10^{-7}$	d	$6{,}37 \times 10^{-8}$	e
47			$2{,}43 \times 10^{-6}$	c	$1{,}24 \times 10^{-6}$	c	$6{,}49 \times 10^{-7}$	d	$3{,}35 \times 10^{-7}$	d	$1{,}34 \times 10^{-7}$	d	$5{,}76 \times 10^{-8}$	e
51			$2{,}24 \times 10^{-6}$	c	$1{,}13 \times 10^{-6}$	c	$5{,}80 \times 10^{-7}$	d	$2{,}93 \times 10^{-7}$	d	$1{,}19 \times 10^{-7}$	d	$5{,}26 \times 10^{-8}$	e
56			$2{,}04 \times 10^{-6}$	c	$1{,}02 \times 10^{-6}$	c	$5{,}10 \times 10^{-7}$	d	$2{,}52 \times 10^{-7}$	d	$1{,}03 \times 10^{-7}$	d	$4{,}73 \times 10^{-8}$	e
62			$1{,}84 \times 10^{-6}$	c	$9{,}06 \times 10^{-7}$	d	$4{,}43 \times 10^{-7}$	d	$2{,}13 \times 10^{-7}$	d	$8{,}84 \times 10^{-8}$	e	$4{,}22 \times 10^{-8}$	e
68			$1{,}68 \times 10^{-6}$	c	$8{,}17 \times 10^{-7}$	d	$3{,}90 \times 10^{-7}$	d	$1{,}84 \times 10^{-7}$	d	$7{,}68 \times 10^{-8}$	e	$3{,}80 \times 10^{-8}$	e
75			$1{,}52 \times 10^{-6}$	c	$7{,}31 \times 10^{-7}$	d	$3{,}40 \times 10^{-7}$	d	$1{,}57 \times 10^{-7}$	d	$6{,}62 \times 10^{-8}$	e	$3{,}41 \times 10^{-8}$	e
82			$1{,}39 \times 10^{-6}$	c	$6{,}61 \times 10^{-7}$	d	$3{,}01 \times 10^{-7}$	d	$1{,}35 \times 10^{-7}$	d	$5{,}79 \times 10^{-8}$	e	$3{,}08 \times 10^{-8}$	e
91			$1{,}25 \times 10^{-6}$	c	$5{,}88 \times 10^{-7}$	d	$2{,}61 \times 10^{-7}$	d	$1{,}14 \times 10^{-7}$	d	$4{,}94 \times 10^{-8}$	e	$2{,}74 \times 10^{-8}$	e
100			$1{,}14 \times 10^{-6}$	c	$5{,}28 \times 10^{-7}$	d	$2{,}29 \times 10^{-7}$	d	$1{,}01 \times 10^{-7}$	d	$4{,}29 \times 10^{-8}$	e	$2{,}47 \times 10^{-8}$	e

	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde, PFH_D (1/h) und der zugehörige Performance Level (PL)						
$MTTF_D$ für jeden Kanal Jahre	**Kat. B** **PL** **DC_{avg} = kein**	**Kat. 1** **PL** **DC_{avg} = kein**	**Kat. 2** **PL** **DC_{avg} = niedrig**	**Kat. 2** **PL** **DC_{avg} = mittel**	**Kat. 3** **PL** **DC_{avg} = niedrig**	**Kat. 3** **PL** **DC_{avg} = mittel**	**Kat. 4** **PL** **DC_{avg} = hoch**
110							$2{,}23 \times 10^{-8}$ e
120							$2{,}03 \times 10^{-8}$ e
130							$1{,}87 \times 10^{-8}$ e
150							$1{,}61 \times 10^{-8}$ e
160							$1{,}50 \times 10^{-8}$ e
180							$1{,}33 \times 10^{-8}$ e
200							$1{,}19 \times 10^{-8}$ e
220							$1{,}08 \times 10^{-8}$ e
240							$9{,}81 \times 10^{-9}$ e
270							$8{,}67 \times 10^{-9}$ e
300							$7{,}76 \times 10^{-9}$ e
330							$7{,}04 \times 10^{-9}$ e
360							$6{,}44 \times 10^{-9}$ e
390							$5{,}94 \times 10^{-9}$ e
430							$5{,}38 \times 10^{-9}$ e
470							$4{,}91 \times 10^{-9}$ e
510							$4{,}52 \times 10^{-9}$ e
560							$4{,}11 \times 10^{-9}$ e
620							$3{,}70 \times 10^{-9}$ e
680							$3{,}37 \times 10^{-9}$ e
750							$3{,}05 \times 10^{-9}$ e
820							$2{,}79 \times 10^{-9}$ e
910							$2{,}51 \times 10^{-9}$ e
1 000							$2{,}28 \times 10^{-9}$ e
1 100							$2{,}07 \times 10^{-9}$ e

Tabelle K.1 *(fortgesetzt)*

	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde, PFH_D (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**
1 200													$1{,}90 \times 10^{-9}$	e
1 300													$1{,}75 \times 10^{-9}$	e
1 500													$1{,}51 \times 10^{-9}$	e
1 600													$1{,}42 \times 10^{-9}$	e
1 800													$1{,}26 \times 10^{-9}$	e
2 000													$1{,}13 \times 10^{-9}$	e
2 200													$1{,}03 \times 10^{-9}$	e
2 300													$9{,}85 \times 10^{-10}$	e
2 400													$9{,}44 \times 10^{-10}$	e
2 500													$9{,}06 \times 10^{-10}$	e

ANMERKUNG 1 Wenn für Kategorie 2 die Anforderungsrate geringer oder gleich 1/25 der Testrate ist (siehe 4.5.4), dann können die Werte für PFH_D in Tabelle K.1 für Kategorie 2 multipliziert mit dem Faktor 1,1 für die Abschätzung des ungünstigsten Falles benutzt werden.

ANMERKUNG 2 Die Berechnung der PFH_D-Werte basiert auf den folgenden DC_{avg}:

— DC_{avg} = niedrig, berechnet mit 60 %;

— DC_{avg} = mittel, berechnet mit 90 %;

— DC_{avg} = hoch, berechnet mit 99 %.

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] Guidelines HSE *Programmable Electronic Systems in Safety-related Applications,* Parts 1 (ISBN 0 11 883906 6) and 2 (ISBN 0 11 883906 3).

[11] CECR-184, *Personal Safety in Microprocessor Control Systems* (Elektronikcentralen, Denmark)

Weitere Publikationen

[12] ISO 13850, *Safety of machinery — Emergency stop — Principles for design*

[13] ISO 13851, *Safety of machinery — Two-hand control devices — Functional aspects and design principles*

[14] 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*

[15] ISO 13856-2, *Safety of machinery — Pressure-sensitive protective devices — Part 2: General principles for design and testing of pressure-sensitive edges and pressure-sensitive bars*

[16] ISO 11428, *Ergonomics — Visual danger signals — General requirements, design and testing*

[17] ISO 9001, *Quality management systems — Requirements*

[18] ISO 9355-1, *Ergonomic requirements for the design of displays and control actuators — Part 1: Human interactions with displays and control actuators*

[19] ISO 9355-2, *Ergonomic requirements for the design of displays and control actuators — Part 2: Displays*

[20] ISO 9355-3, *Ergonomic requirements for the design of displays and control actuators — Part 3: Control actuators*

[21] ISO 11429, *Ergonomics — System of auditory and visual danger and information signals*

[22] ISO 7731, *Ergonomics — Danger signals for public and work areas — Auditory danger signals*

[23] ISO 4413, *Hydraulic fluid power — General rules and safety requirements for systems and their components*

[24] ISO 4414, *Pneumatic fluid power — General rules and safety requirements for systems and their components*

[25] ISO 13855:2010, *Safety of machinery — Positioning of protective equipment with respect to the approach speeds of parts of the human body*

[26] ISO 14118, *Safety of machinery — Prevention of unexpected start–up*

[27] ISO 19973 (alle Teile), *Pneumatic fluid power — Assessment of component reliability by testing*

[28] IEC 60204-1:2005, *Safety of machinery — Electrical equipment of machines — Part 1: General requirements*

[29] IEC 60447, *Basic and safety principles for man–machine interface (MMI) — Actuating principles*

[30] IEC 60529, *Degrees of protection provided by enclosures (IP code)*

[31] IEC 60812, *Analysis techniques for system reliability — Procedure for failure mode and effects analysis (FMEA)*

[32] IEC 60947 (alle Teile), *Low-voltage switchgear and controlgear*

[33] IEC 61000-6-2, *Electromagnetic compatibility (EMC) — Part 6-2: Generic standards — Immunity for industrial environments*

[34] IEC 61800-3, *Adjustable speed electrical power drive systems — Part 3: EMC requirements and specific test methods*

[35] IEC 61810 (alle Teile), *Electromagnetic elementary relays*

[36] IEC 61300 (alle Teile), *Fibre optic interconnecting devices and passive components — Basic test and measurement procedures*

[37] IEC 61310 (alle Teile), *Safety of machinery — Indication, marking and actuation*

[38] IEC 61131-3, *Programmable controllers — Part 3: Programming languages*

[39] EN 457, *Sicherheit von Maschinen; Akustische Gefahrensignale; Allgemeine Anforderungen, Gestaltung und Prüfung (ISO 7731:1986, modifiziert)*

[40] EN 614-1, *Sicherheit von Maschinen — Ergonomische Gestaltungsgrundsätze — Teil 1: Begriffe und allgemeine Leitsätze*

[41] EN 982, *Sicherheit von Maschinen — Sicherheitstechnische Anforderungen an fluidtechnische Anlagen und deren Bauteile — Hydraulik*

[42] EN 983, *Sicherheit von Maschinen — Sicherheitstechnische Anforderungen an fluidtechnische Anlagen und deren Bauteile — Pneumatik*

[43] EN 1005-3, *Sicherheit von Maschinen — Menschliche körperliche Leistung — Teil 3: Empfohlene Kraftgrenzen bei Maschinenbetätigung*

[44] EN 1088, *Sicherheit von Maschinen — Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen — Leitsätze für Gestaltung und Auswahl*

[45] EN 50205, *Relais mit (mechanisch) zwangsgeführten Kontakten*

[46] SN 29500 (alle Teile), *Failure rates of components*

[47] Goble, W.M.: *Control systems — Evaluation and Rehability.* 2nd Edition. Instrument Society of America (ISA), North Carolina, 1998

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

Datenbanken

[49] SN 29500, *Ausfallraten für Bauteile, Edition 1999-11, Siemens AG 1999*

[50] IEC/TR 62380, *Reliability data handbook — Universal model for reliability prediction of electronics components, PCBs and equipment*[4)]

[51] Reliability Prediction of Electronic Equipment, MIL-HDBK-217E, Department of Defense, 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

[54] NPRD-95, *Non-electronic Parts Reliability Data* (RAC-STD-6200), Reliability Analysis Center, 201 Mill Street, Rome, NY 13440

[55] *British Handbook for Reliability Data for Components used in Telecommunication Systems*, British Telecom (HRD5, last issue)

[56] Chinese Military Standard, GJB/z 299B

4) Identisch zu RDF 2000/*Reliability Data Handbook*, UTE C 80-810, Union Technique de l'Electricité et de la Communication.