

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)

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*

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

Inhalt

Seite

Europäisches Vorwort	5
Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EG-Richtlinie 2006/42/EG	6
Vorwort	7
Einleitung	8
1 Anwendungsbereich	11
2 Normative Verweisungen	11
3 Begriffe, Formelzeichen und Abkürzungen	12
3.1 Begriffe	12
3.2 Formelzeichen und Abkürzungen	19
4 Gestaltungsaspekte	20
4.1 Sicherheitsziele in der Gestaltung	20
4.2 Strategie der Risikominderung	22
4.2.1 Allgemeines	22
4.2.2 Beitrag der Risikominderung durch das Steuerungssystem	22
4.3 Bestimmung des erforderlichen Performance Levels (PL _r)	26
4.4 Entwicklung des SRP/CS	26
4.5 Bewertung des erreichten Performance Levels PL und die Beziehung zum SIL	27
4.5.1 Performance Level PL	27
4.5.2 Mittlere Zeit bis zum gefahrbringenden Ausfall jedes Kanals (MTTF _D)	29
4.5.3 Diagnosedeckungsgrad (DC)	30
4.5.4 Vereinfachtes Verfahren zur Abschätzung der quantifizierbaren Aspekte des PL	31
4.5.5 Beschreibung des Ausgabeteils der SRP/CS nach Kategorien	33
4.6 Software-Sicherheitsanforderungen	34
4.6.1 Allgemeines	34
4.6.2 Sicherheitsbezogene Embedded-Software (SRESW)	35
4.6.3 Sicherheitsbezogene Anwendungssoftware (SRASW)	36
4.6.4 Softwarebasierende Parametrisierung	39
4.7 Verifikation, dass der erreichte PL den PL _r erfüllt	41
4.8 Ergonomische Aspekte der Gestaltung	41
5 Sicherheitsfunktionen	41
5.1 Spezifikation der Sicherheitsfunktionen	41
5.2 Nähere Angaben über die Sicherheitsfunktionen	44
5.2.1 Sicherheitsbezogene Stoppfunktion	44
5.2.2 Manuelle Rückstellungsfunktion	44
5.2.3 Start-/Wiederaufnahmefunktion	45
5.2.4 Lokale Steuerungsfunktion	45
5.2.5 Mutingfunktion	45
5.2.6 Ansprechzeit	46
5.2.7 Sicherheitsbezogene Parameter	46
5.2.8 Schwankungen, Verlust und Wiederkehr der Energiequellen	46

6	Die Kategorien und deren Beziehung zur $MTTF_D$ jedes Kanals, DC_{avg} und CCF	46
6.1	Allgemeines	46
6.2	Spezifikation der Kategorien	47
6.2.1	Allgemeines	47
6.2.2	Vorgesehene Architekturen	47
6.2.3	Kategorie B	48
6.2.4	Kategorie 1	48
6.2.5	Kategorie 2	50
6.2.6	Kategorie 3	51
6.2.7	Kategorie 4	52
6.3	Kombination von SRP/CS, um einen Gesamt-PL zu erreichen	55
7	Berücksichtigung von Fehlern, Fehlerausschluss	57
7.1	Allgemeines	57
7.2	Fehlerbetrachtung	57
7.3	Fehlerausschluss	57
8	Validierung	57
9	Instandhaltung	58
10	Technische Dokumentation	58
11	Benutzerinformation	59
Anhang A (informativ) Bestimmung des erforderlichen Performance Levels (PL_r)		60
A.1	Auswahl des PL_r	60
A.2	Anleitung für die Auswahl der Parameter S, F und P zur Einschätzung des Risikos	60
A.2.1	Schwere der Verletzung S1 und S2	60
A.2.2	Häufigkeit und/oder Dauer der Gefährdungsexposition F1 und F2	61
A.2.3	Möglichkeit zur Vermeidung der Gefährdungsereignisse P1 und P2 und Eintrittswahrscheinlichkeit	61
A.3	Überlagerte Gefährdungen	63
Anhang B (informativ) Blockmethode und sicherheitsbezogenes Blockdiagramm		65
B.1	Blockmethode	65
B.2	Sicherheitsbezogenes Blockdiagramm	65
Anhang C (informativ) Berechnung oder Abschätzung von $MTTF_D$ -Werten für einzelne Bauteile		67
C.1	Allgemeines	67
C.2	Verfahren guter ingenieurmäßiger Praxis	67
C.3	Hydraulische Bauteile	67
C.4	$MTTF_D$ von pneumatischen, mechanischen und elektromechanischen Bauteilen	70
C.4.1	Allgemeines	70
C.4.2	Berechnung der $MTTF_D$ für Bauteile aus B_{10D}	70
C.4.3	Beispiel	72
C.5	$MTTF_D$ -Daten elektrischer Bauteile	72
C.5.1	Allgemeines	72
C.5.2	Halbleiter	73
C.5.3	Passive Bauteile	73
Anhang D (informativ) Vereinfachtes Verfahren zur Abschätzung der $MTTF_D$ für jeden Kanal		76
D.1	Parts-Count-Verfahren	76
D.2	Die $MTTF_D$ für unterschiedliche Kanäle, Symmetrisierung der $MTTF_D$ für jeden Kanal	77
Anhang E (informativ) Abschätzungen des Diagnosedeckungsgrades (DC) für Funktionen und Module		78
E.1	Beispiele für den Diagnosedeckungsgrad (DC)	78
E.2	Abschätzung des durchschnittlichen DC (DC_{avg})	80

Anhang F (informativ) Abschätzungen der Ausfälle aufgrund gemeinsamer Ursache (CCF).....	82
F.1 Anforderungen an CCF.....	82
F.2 Abschätzung der Auswirkung des CCF.....	82
Anhang G (informativ) Systematischer Ausfall	84
G.1 Allgemeines	84
G.2 Maßnahmen zur Beherrschung systematischer Ausfälle	84
G.3 Maßnahmen zur Vermeidung systematischer Ausfälle.....	85
G.4 Maßnahmen zur Vermeidung systematischer Ausfälle während der Integration des SRP/CS	86
Anhang H (informativ) Beispiel der Kombination von verschiedenen sicherheitsbezogenen Teilen einer Steuerung	87
Anhang I (informativ) Beispiele	90
I.1 Allgemeines	90
I.2 Sicherheitsfunktion und erforderlicher Performance Level (PL _r).....	90
I.3 Beispiel A, einkanalgiges System	91
I.3.1 Identifikation der sicherheitsbezogenen Teile	91
I.3.2 Quantifizierung von MTTF _D , DC _{avg} , Maßnahmen gegen den Ausfall infolge gemeinsamer Ursache (CCF), Kategorie, PL	92
I.4 Beispiel B, redundantes System	93
I.4.1 Identifikation der sicherheitsbezogenen Teile	93
I.4.2 Quantifizierung der MTTF _D für jeden Kanal, DC _{avg} , Maßnahmen gegen den Ausfall infolge gemeinsamer Ursache (CCF), Kategorie und PL	95
Anhang J (informativ) Software	99
J.1 Beschreibung des Beispiels	99
J.2 Anwendung des V-Modells des Software-Sicherheitslebenszyklus	99
J.3 Verifikation der Softwarespezifikation.....	100
J.4 Beispiel von Programmierregeln	101
Anhang K (informativ) Numerische Darstellung von Bild 5.....	103
Literaturhinweise.....	107

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

gefährbringender 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 zugehörigen 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

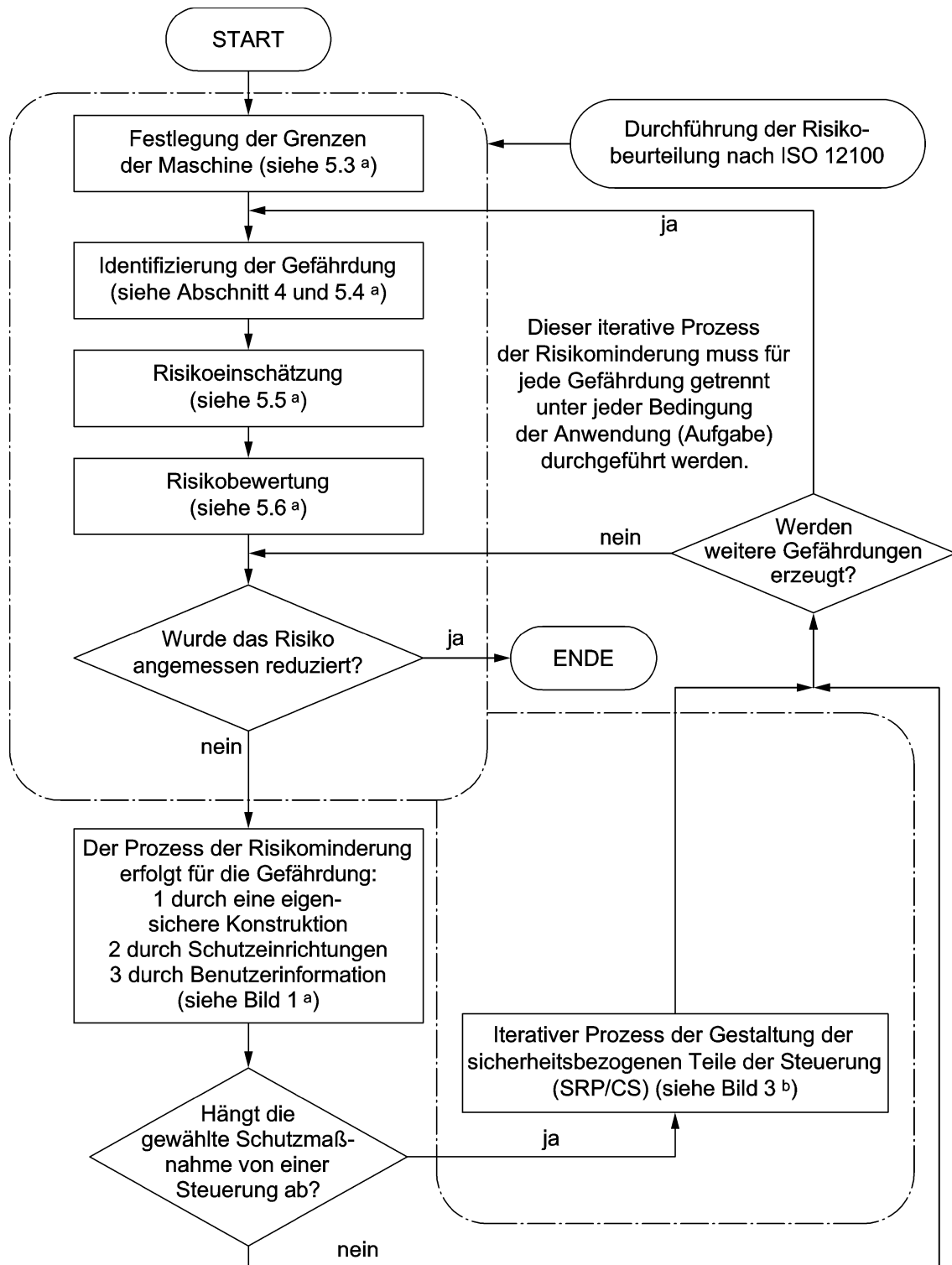
Formelzeichen oder Abkürzung	Beschreibung	Definition oder Fundort
a, b, c, d, e	Bezeichnung für die Performance Level	Tabelle 3
AOPD	aktive opto-elektronische Schutzeinrichtungen (z. B. Lichtschranke)	Anhang H
B, 1, 2, 3, 4	Bezeichnung für die Kategorien	Tabelle 7
B_{10D}	Anzahl von Zyklen, bis 10 % 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).

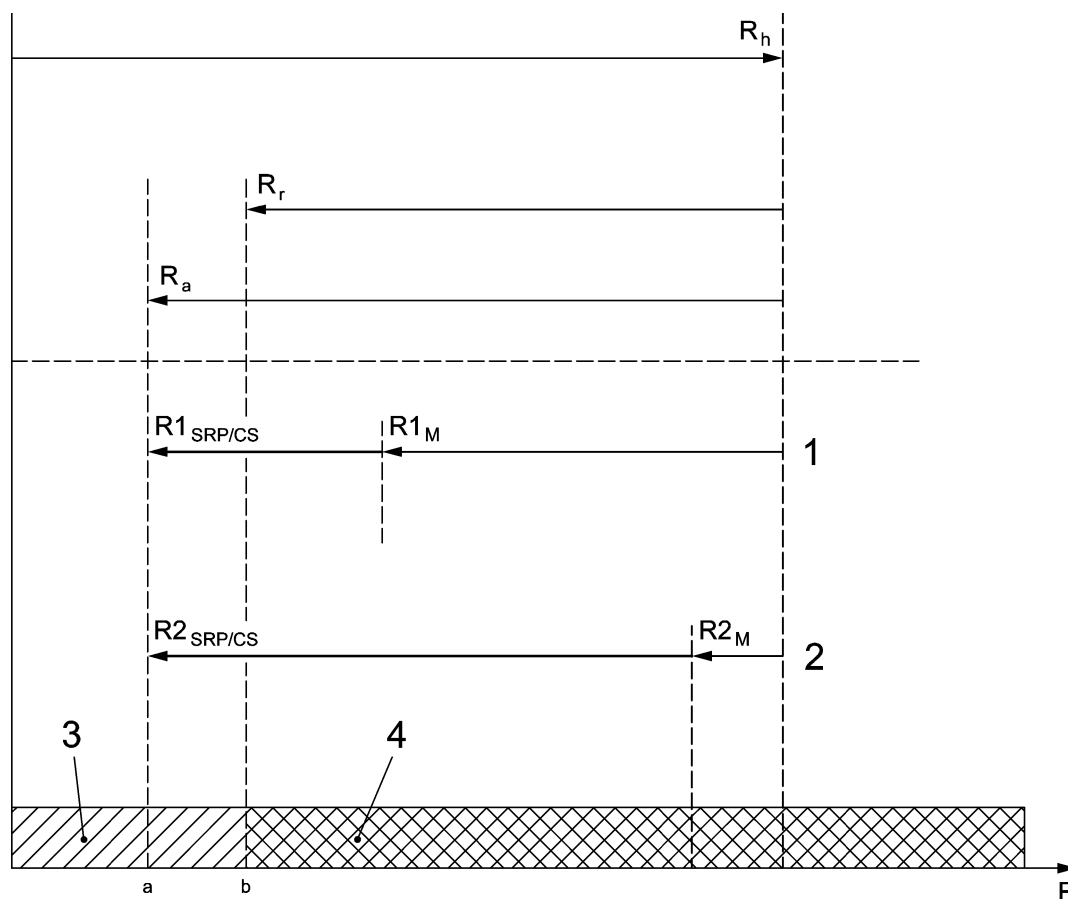
Um einen PL zu erhalten, müssen neben den quantifizierbaren Aspekten auch die qualitativen Aspekte in Bezug auf die Anforderungen der PL erfüllt werden (siehe 4.5).

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).

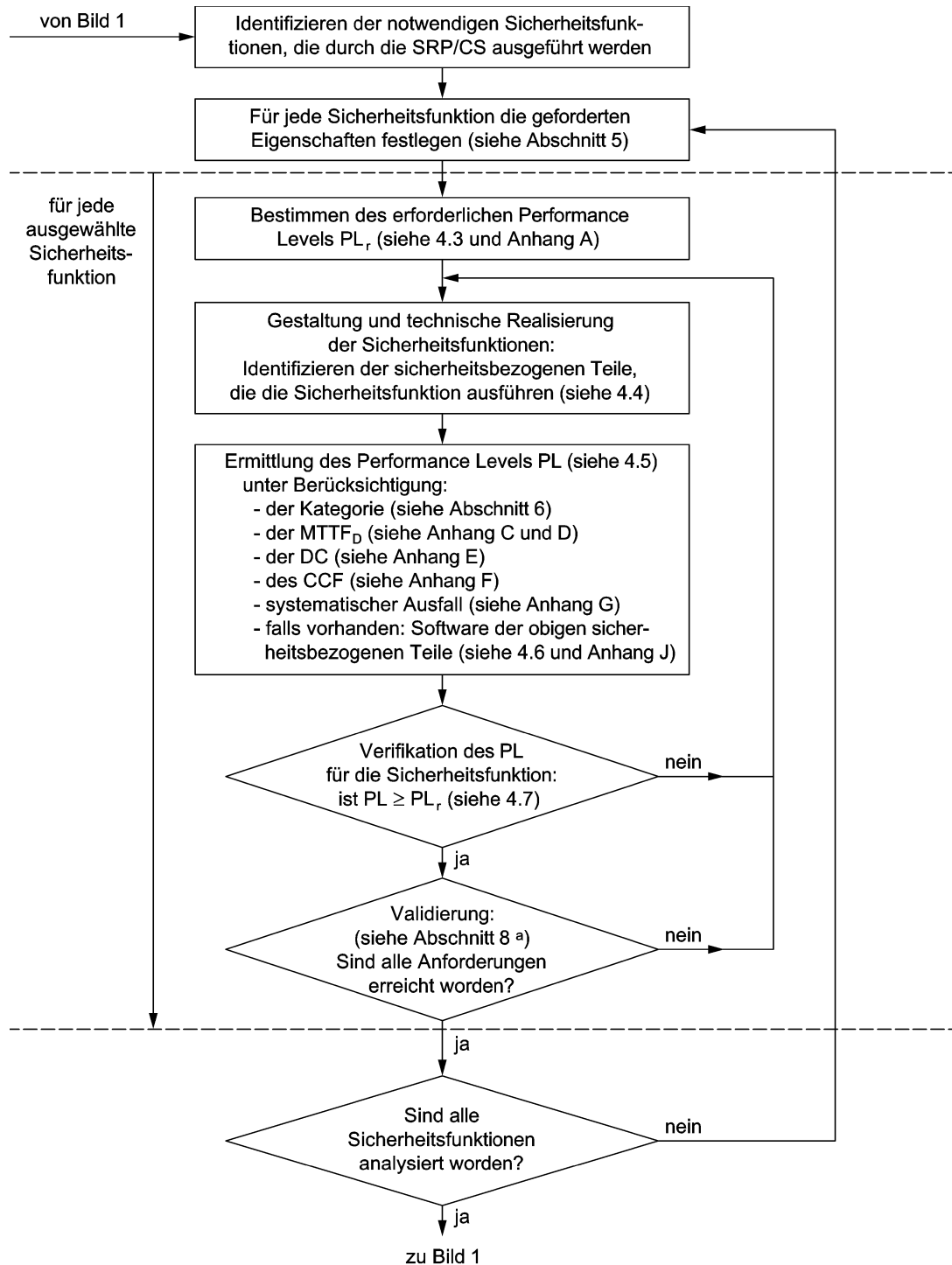


Legende

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:

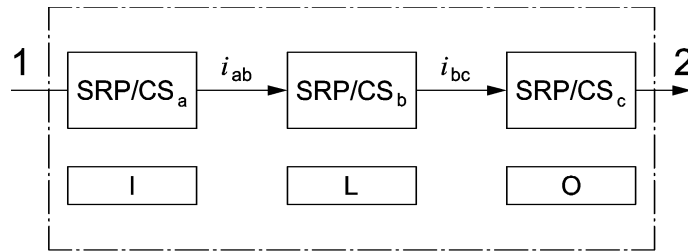
- Eingang (SRP/CS_a),
- Logik/Bearbeitung (SRP/CS_b),
- Ausgang/Energieübertragungselementen (SRP/CS_c), und
- Verbindungen (i_{ab}, i_{bc}) (z. B. elektrisch, optisch).

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 13849 oder nach IEC 62061/IEC 61508 (siehe auch ISO/TR 23849) entworfen sein, obwohl es eine Übereinstimmung zwischen den PL dieses Teils der ISO 13849 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 überwacht System erforderlich sein. Zusätzlich müssen Ausfälle infolge gemeinsamer Ursache (CCF) mit in Betracht gezogen werden (siehe Bild 3).

Zu Einschränkungen aufgrund der Architektur, siehe Abschnitt 6.

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

Der Wert der MTTF_D jedes Kanals wird in drei Stufen angegeben (siehe Tabelle 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:

- Verwendung von Herstellerdaten;
- Verwendung der Verfahren in den Anhängen C und D;
- 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.