

DIN EN ISO 13849-1



ICS 13.110

Ersatz für
DIN EN ISO 13849-1:2007-07

**Sicherheit von Maschinen –
Sicherheitsbezogene Teile von Steuerungen –
Teil 1: Allgemeine Gestaltungsleitsätze (ISO 13849-1:2006);
Deutsche Fassung EN ISO 13849-1:2008**

Safety of machinery –
Safety-related parts of control systems –
Part 1: General principles for design (ISO 13849-1:2006);
German version EN ISO 13849-1:2008

Sécurité des machines –
Parties des systèmes de commande relatives à la sécurité –
Partie 1: Principes généraux de conception (ISO 13849-1:2006);
Version allemande EN ISO 13849-1:2008

Gesamtumfang 102 Seiten

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

© DIN Deutsches Institut für Normung e.V. · Jede Art der Vervielfältigung, auch auszugsweise,
nur mit Genehmigung des DIN Deutsches Institut für Normung e.V., Berlin, gestattet.
Alleinverkauf der Normen durch Beuth Verlag GmbH, 10772 Berlin

Preisgruppe 31
www.din.de
www.beuth.de



1454006

Beginn der Gültigkeit

Diese Norm gilt ab 2008-12-01.

Daneben dürfen DIN EN 954-1:1997-03 und DIN EN 954-1 Bbl 1:2000-01 noch bis zum 30.11.2009 und DIN EN ISO 13849-1:2007-07 noch bis zum 28.12.2009 angewendet werden.

Nationales Vorwort

Diese Norm enthält sicherheitstechnische Festlegungen im Sinne des Gesetzes über technische Arbeitsmittel und Verbraucherprodukte (Geräte- und Produktsicherheitsgesetz (GPSG)).

Sie beinhaltet die Deutsche Fassung der vom Technischen Komitees CEN/TC 114 „Sicherheit vom Maschinen und Geräten“, dessen Sekretariat vom DIN (Deutschland) gehalten wird, im Europäischen Komitee für Normung (CEN) erarbeiteten EN ISO 13849-1:2008.

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

Diese Europäische Norm konkretisiert einschlägige Anforderungen von Anhang I der EG-Maschinenrichtlinie 98/37/EG (gültig bis 28. Dezember 2009) sowie mit Wirkung vom 29. Dezember 2009 der neuen EG-Maschinenrichtlinie 2006/42/EG an erstmals im EWR in Verkehr gebrachte Maschinen, um den Nachweis der Übereinstimmung mit diesen Anforderungen zu erleichtern.

Ab dem Zeitpunkt ihrer Bezeichnung als Harmonisierte Norm im Amtsblatt der Europäischen Gemeinschaften kann der Hersteller bei ihrer Anwendung davon ausgehen, dass er die von der Norm behandelten Anforderungen der Maschinenrichtlinie eingehalten hat (so genannte Vermutungswirkung).

Für die im Abschnitt 2 und in den Literaturhinweisen angegebenen Internationalen Normen wird im Folgenden auf die entsprechenden Deutschen Normen hingewiesen:

Im Abschnitt 2 angegebenen Normen

ISO 12100-1	siehe	DIN EN ISO 12100-1
ISO 12100-2	siehe	DIN EN ISO 12100-2
ISO 13849-2	siehe	DIN EN ISO 13849-2
ISO 14121	siehe	DIN EN 1050
IEC 60050-191	siehe	IEV 191
IEC 61508-3	siehe	DIN EN 61508-3
IEC 61508-4	siehe	DIN EN 61508-4

Im Verzeichnis „Literaturhinweise“ angegebenen Normen

ISO 4413	siehe	DIN ISO 4413
ISO 4414	siehe	DIN ISO 4414
ISO 7731	siehe	DIN EN ISO 7731
ISO 9355-1	siehe	DIN EN 894-1
ISO 9355-2	siehe	DIN EN 894-2
ISO 9355-3	siehe	DIN EN 894-3
ISO 11428	siehe	DIN EN 842
ISO 11429	siehe	DIN EN 981
ISO 13850	siehe	DIN EN 418
ISO 13855	siehe	DIN EN 999
ISO 13856-1	siehe	DIN EN 1760-1
ISO 13856-2	siehe	DIN EN 1760-2
ISO 14118	siehe	DIN EN 1037
IEC 60204-1	siehe	DIN IEC 60204-1
IEC 60447	siehe	DIN EN 60447
IEC 60529	siehe	DIN EN 60529
IEC 60812	siehe	DIN IEC 60812
IEC 60957-5-1	keine nationale Entsprechung	
IEC 61000-4-4	siehe	DIN EN 61000-4-4
IEC 61496-1	siehe	DIN EN 61496-1
IEC 61496-2	keine nationale Entsprechung	
IEC 61496-3	siehe	DIN EN 61496-3
IEC 61508-1	siehe	DIN EN 61508-1
IEC 61508-2	siehe	DIN EN 61508-2
IEC 61508-5	siehe	DIN EN 61508-5
IEC 61508-6	siehe	DIN EN 61508-6
IEC 61508-7	siehe	DIN EN 61508-7

Die Anhänge A bis K sind informativ.

Änderungen

Gegenüber DIN EN ISO 13849-1:2007-07 wurden folgende Änderungen vorgenommen:

- Anpassung des informativen Anhangs ZA über den Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EG-Maschinenrichtlinie 98/37/EG;
- Aufnahme des informativen Anhangs ZB über den Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EG-Maschinenrichtlinie 2006/42/EG.

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

Nationaler Anhang NA (informativ)

Literaturhinweise

Im Abschnitt 2 angegebenen Normen

IEV 191:2002, *Internationales Elektrotechnisches Wörterbuch — Kapitel 191: Zuverlässigkeit und Dienstgüte* (Konsolidiert mit IEC 60050-191/A1:1993-03 und IEC 60050-191/A2:2002-01)

DIN EN 61508-3:2002-12, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 3: Anforderungen an Software* (IEC 61508-3:1998 + Corrigendum 1999); Deutsche Fassung EN 61508-3:2001

DIN EN 61508-4:2002-11, *Funktionale Sicherheit elektrischer/elektronischer/programmierbarer elektronischer sicherheitsbezogener Systeme — Teil 4: Begriffe und Abkürzungen* (IEC 61508-4:1998 + Corrigendum 1999); Deutsche Fassung EN 61508-4:2001

DIN EN ISO 12100-1:2004-04, *Sicherheit von Maschinen — Grundbegriffe, allgemeine Gestaltungsleitsätze — Teil 1: Grundsätzliche Terminologie, Methodologie* (ISO 12100-1:2003); Deutsche Fassung EN ISO 12100-1:2003

DIN EN ISO 12100-2:2004-04, *Sicherheit von Maschinen — Grundbegriffe, allgemeine Gestaltungsleitsätze — Teil 2: Technische Leitsätze* (ISO 12100-2:2003); Deutsche Fassung EN ISO 12100-2:2003

Im Verzeichnis „Literaturhinweise“ angegebenen Normen

DIN EN 418, *Sicherheit von Maschinen — NOT-AUS-Einrichtung — Funktionelle Aspekte — Gestaltungsleitsätze*

DIN EN 842, *Sicherheit von Maschinen — Optische Gefahrensignale — Allgemeine Anforderungen, Gestaltung und Prüfung*

DIN EN 894-1, *Sicherheit von Maschinen — Ergonomische Anforderungen an die Gestaltung von Anzeigen und Stellteilen — Teil 1: Allgemeine Leitsätze für Benutzer-Interaktion mit Anzeigen und Stellteilen*

DIN EN 894-2, *Sicherheit von Maschinen — Ergonomische Anforderungen an die Gestaltung von Anzeigen und Stellteilen — Teil 2: Anzeigen*

DIN EN 894-3, *Sicherheit von Maschinen — Ergonomische Anforderungen an die Gestaltung von Anzeigen und Stellteilen — Teil 3: Stellteile*

DIN EN 981, *Sicherheit von Maschinen — System akustischer und optischer Gefahrensignale und Informationssignale*

DIN EN 999, *Sicherheit von Maschinen — Anordnung von Schutzeinrichtungen im Hinblick auf Annäherungsgeschwindigkeiten von Körperteilen*

DIN EN 1037, *Sicherheit von Maschinen — Vermeidung von unerwartetem Anlauf*

DIN EN 1760-1, *Sicherheit von Maschinen — Druckempfindliche Schutzeinrichtungen — Teil 1: Allgemeine Leitsätze für die Gestaltung und Prüfung von Schalmatten und Schaltplatten*

DIN EN 1760-2, *Sicherheit von Maschinen — Druckempfindliche Schutzeinrichtungen — Teil 2: Allgemeine Leitsätze für die Gestaltung und Prüfung von Schaltleisten und Schaltstangen*

DIN EN 60447, *Grund- und Sicherheitsregeln für die Mensch-Maschine-Schnittstelle — Kennzeichnung — Bedienungsgrundsätze*

DIN EN 60529, *Schutzarten durch Gehäuse (IP-Code)*

DIN EN 61000-4-4, *Elektromagnetische Verträglichkeit (EMV) — Teil 4-4: Prüf- und Messverfahren — Prüfung der Störfestigkeit gegen schnelle transiente elektrische Störgrößen/Burst*

DIN EN 61496-1, *Sicherheit von Maschinen — Berührungslos wirkende Schutzeinrichtungen — Teil 1: Allgemeine Anforderungen und Prüfungen*

DIN EN 61496-3, *Sicherheit von Maschinen — Berührungslos wirkende Schutzeinrichtungen — Teil 3: Besondere Anforderungen an aktive opto-elektronische diffuse Reflektion nutzende Schutzeinrichtungen (AOPDDR)*

DIN EN 61508-1, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/ programmierbarer elektronischer Systeme — Teil 1: Allgemeine Anforderungen*

DIN EN 61508-2, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/ programmierbarer elektronischer Systeme — Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/ programmierbare elektronische Systeme*

DIN EN 61508-5, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/ programmierbarer elektronischer Systeme — Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level)*

DIN EN 61508-6, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/ programmierbarer elektronischer Systeme — Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3*

DIN EN 61508-7, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/ programmierbarer elektronischer Systeme — Teil 7: Anwendungshinweise über Verfahren und Maßnahmen*

DIN EN ISO 7731, *Ergonomie — Gefahrensignale für öffentliche Bereiche und Arbeitsstätten — Akustische Gefahrensignale*

DIN IEC 60204-1, *Sicherheit von Maschinen — Elektrische Ausrüstung von Maschinen — Teil 1: Allgemeine Anforderungen*

DIN IEC 60812, *Analysetechniken für die Funktionsfähigkeit von Systemen — Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA)*

— Leerseite —

Deutsche Fassung

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

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

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

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

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

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

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



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

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

© 2008 CEN Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den nationalen Mitgliedern von CEN vorbehalten.

Ref. Nr. EN ISO 13849-1:2008 D

Inhalt

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

	Seite
8 Validierung	50
9 Instandhaltung	51
10 Technische Dokumentation	51
11 Benutzerinformation	52
Anhang A (informativ) Bestimmung des erforderlichen Performance Levels (PL_r).....	53
Anhang B (informativ) Blockmethode und sicherheitsbezogenes Blockdiagramm.....	56
Anhang C (informativ) Berechnung oder Abschätzung von MTTF_d-Werten für einzelne Bauteile.....	58
Anhang D (informativ) Vereinfachtes Verfahren zur Bestimmung der MTTF_d für jeden Kanal.....	66
Anhang E (informativ) Abschätzungen des Diagnosedeckungsgrades (DC) für Funktionen und Module	68
Anhang F (informativ) Abschätzungen der Ausfälle aufgrund gemeinsamer Ursache (CCF)	72
Anhang G (informativ) Systematischer Ausfall.....	74
Anhang H (informativ) Beispiel der Kombination von verschiedenen sicherheitsbezogenen Teilen einer Steuerung	77
Anhang I (informativ) Beispiele	80
Anhang J (informativ) Software	87
Anhang K (informativ) Numerische Darstellung von Bild 5.....	90
Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EG-Richtlinie 98/37/EG geändert durch Richtlinie 98/79/EG	92
Anhang ZB (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EG-Richtlinie 2006/42/EG.....	93
Literaturhinweise	94

Vorwort

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

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

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

Dieses Dokument ersetzt EN ISO 13849-1:2006.

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

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

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

Anerkennungsnotiz

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

Einleitung

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 Anwendungsbereich

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

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

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

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

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

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

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

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

ANMERKUNG 5 Siehe auch Tabelle 1.

2 Normative Verweisungen

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

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

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

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

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

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

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

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

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

3 Begriffe, Formelzeichen und Abkürzungen

3.1 Begriffe

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

3.1.1

sicherheitsbezogenes Teil einer Steuerung

SRP/CS

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

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

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

3.1.2

Kategorie

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

3.1.3

Fehler

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

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

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

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

3.1.4

Ausfall

Beendigung der Fähigkeit einer Einheit, eine geforderte Funktion zu erfüllen

ANMERKUNG 1 Nach einem Ausfall hat die Einheit einen Fehler.

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

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

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

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

3.1.5

gefährbringender Ausfall

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

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

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

3.1.6

Ausfall infolge gemeinsamer Ursache

CCF

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

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

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

3.1.7

systematischer Ausfall

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

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

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

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

ANMERKUNG 3 Beispielursachen systematischer Ausfälle beinhalten menschliches Versagen in:

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

3.1.8

Muting

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

3.1.9

manuelle Rückstellung

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

3.1.10

Schaden

physische Verletzung oder Schädigung der Gesundheit

[ISO 12100-1:2003, 3.5]

3.1.11

Gefährdung

potentielle Schadensquelle

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

ANMERKUNG 2 Die Gefährdung im Sinne dieser Definition

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

[ISO 12100-1:2003, 3.6]

3.1.12

Gefährdungssituation

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

[ISO 12100-1:2003, 3.9]

3.1.13

Risiko

Kombination der Wahrscheinlichkeit des Eintritts eines Schadens und seines Schadensausmaßes

[ISO 12100-1:2003, 3.11]

3.1.14

Restrisiko

verbleibendes Risiko, nachdem Schutzmaßnahmen ergriffen wurden

(Siehe Bild 2)

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

3.1.15

Risikobeurteilung

Gesamtheit des Verfahrens, das eine Risikoanalyse und Risikobewertung umfasst

[ISO 12100-1:2003, 3.13]

3.1.16

Risikoanalyse

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

[ISO 12100-1:2003, 3.14]

3.1.17

Risikobewertung

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

[ISO 12100-1:2003, 3.16]

3.1.18

bestimmungsgemäße Verwendung einer Maschine

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

[ISO 12100-1:2003, 3.22]

3.1.19

vernünftigerweise vorhersehbare Fehlanwendung

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

[ISO 12100-1:2003, 3.23]

3.1.20

Sicherheitsfunktion

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

[ISO 12100-1:2003, 3.28]

3.1.21

Überwachung

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

3.1.22

programmierbares elektronisches System

PES

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

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

3.1.23

Performance Level

PL

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

ANMERKUNG Siehe 4.5.1.

3.1.24

erforderlicher Performance Level

PL_r

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

ANMERKUNG Siehe Bilder 2 und A.1.

3.1.25

mittlere Zeit bis zum gefahrbringenden Ausfall

MTTF_d

Erwartungswert der mittleren Zeit bis zum gefahrbringenden Ausfall

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

3.1.26

Diagnosedeckungsgrad

DC

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

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

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

3.1.27

Schutzmaßnahme

Maßnahme zur vorgesehenen Minderung des Risikos

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

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

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

3.1.28

Gebrauchsdauer

T_M

Zeitraum, der die vorgegebene Verwendung der SRP/CS abdeckt

3.1.29

Testrate

r_t

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

3.1.30

Anforderungsrate

r_d

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

3.1.31

Reparaturrate

r_r

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

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

3.1.32

Maschinensteuerung

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

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

3.1.33

Sicherheits-Integritätslevel

SIL

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

[IEC 61508-4:1998, 3.5.6]

3.1.34

Programmiersprache mit eingeschränktem Sprachumfang

LVL

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

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

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

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

3.1.35

Programmiersprache mit nicht eingeschränktem Sprachumfang

FVL

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

BEISPIEL C, C++, Assembler.

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

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

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

3.1.36

Anwendungssoftware

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

3.1.37

Embedded-Software

Firmware

Systemsoftware

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

ANMERKUNG Üblicherweise wird Embedded-Software in FVL geschrieben.

3.2 Formelzeichen und Abkürzungen

Siehe Tabelle 2.

Tabelle 2 — Formelzeichen und Abkürzungen

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

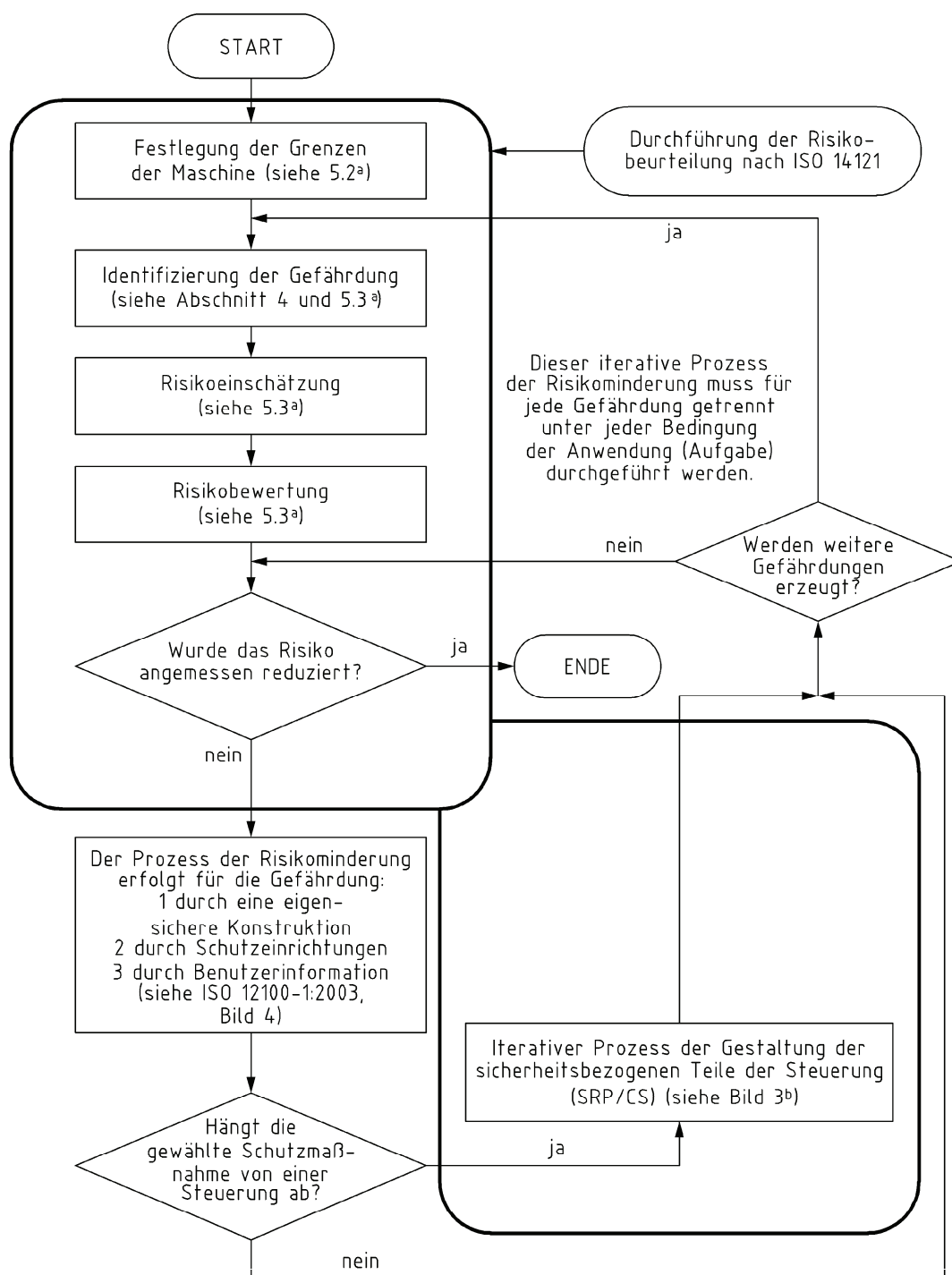
Tabelle 2 (fortgesetzt)

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

4 Gestaltungsaspekte

4.1 Sicherheitsziele in der Gestaltung

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



- a Bezieht sich auf ISO 12100-1:2003
b Bezieht sich auf diesen Teil der ISO 13849

Bild 1 — Übersicht über die Risikobeurteilung/Risikominderung

4.2 Strategie der Risikominderung

4.2.1 Allgemeines

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

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

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

4.2.2 Beitrag der Risikominderung durch das Steuerungssystem

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

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

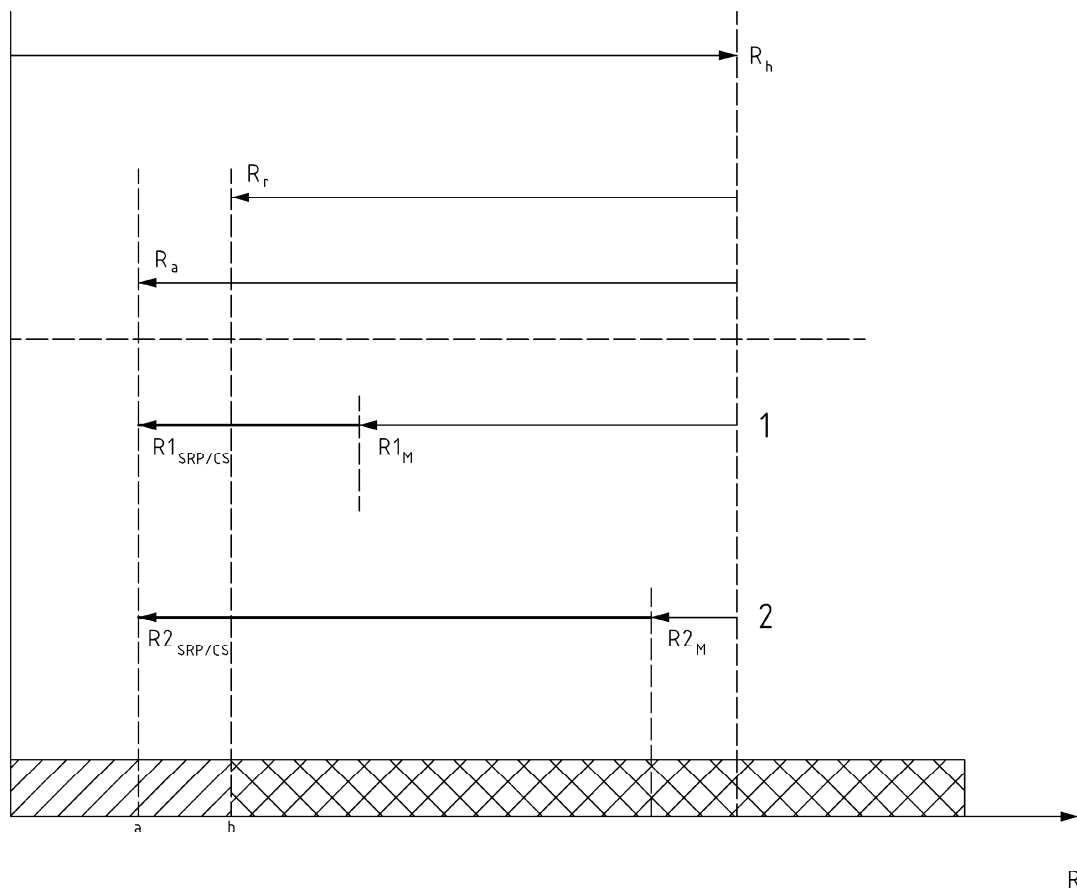
In diesem Teil der ISO 13849 werden die Performance Level definiert in Form der Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde. Fünf Performance Level (a bis e) sind festgelegt mit definierten Bereichen der Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (siehe Tabelle 3).

Tabelle 3 — Performance Level (PL)

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

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

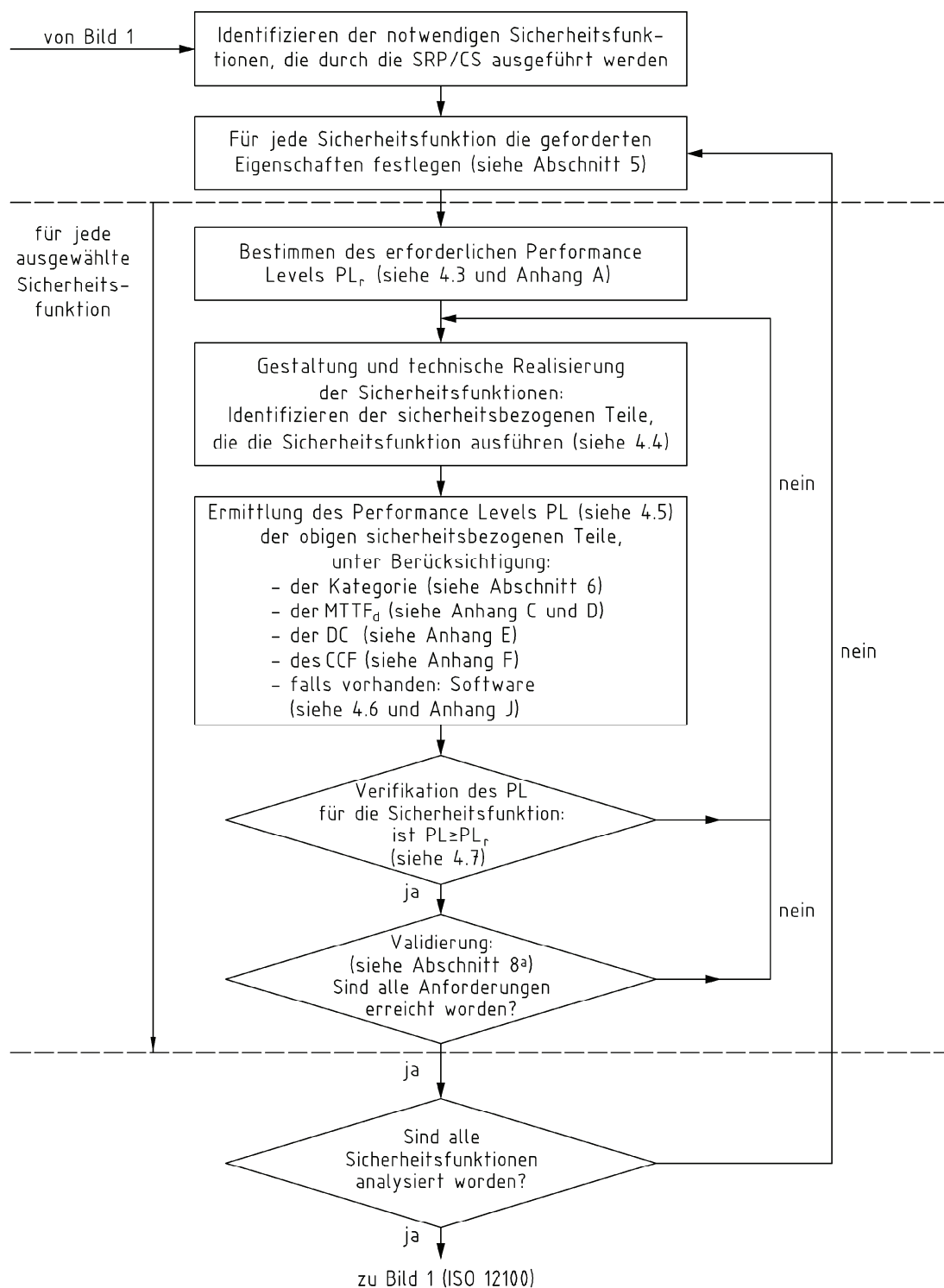


Legende

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

ANMERKUNG Für weitere Informationen zur Risikominderung, siehe ISO 12100.

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



a ISO 13849-2 enthält weitere Hilfe zur Validierung.

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

4.3 Bestimmung des erforderlichen Performance Levels (PL_r)

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

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

4.4 Entwicklung des SRP/CS

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

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

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

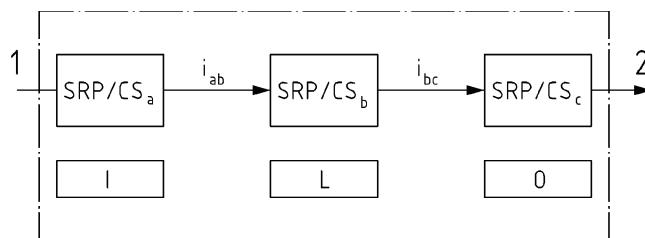
- Eingang (SRP/CS_a),
- Logik/Bearbeitung (SRP/CS_b),
- Ausgang/Energieübertragungselementen (SRP/CS_c), und
- Verbindungen (i_{ab} , i_{bc}) (z. B. elektrisch, optisch).

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

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

ANMERKUNG 2 Vorgesehene Architekturen werden im Abschnitt 6 angegeben.

ANMERKUNG 3 Alle Verbindungen sind in den sicherheitsbezogenen Teilen enthalten.



Legende

I Eingang
L Logik
O Ausgang

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

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

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

4.5.1 Performance Level PL

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

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

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

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

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

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

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

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

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

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

Für ein SRP/CS oder einer Kombination von SRP/CS, welches nach den in Abschnitt 6 gegebenen Anforderungen entworfen wurde, kann die durchschnittliche Wahrscheinlichkeit eines 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.

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

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

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

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

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

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

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

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

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

Zu Einschränkungen aufgrund der Architektur, siehe Abschnitt 6.

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

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

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

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

MTTF _d	
Bezeichnung für jeden Kanal	Bereich für jeden Kanal
niedrig	3 Jahre ≤ MTTF _d < 10 Jahre
mittel	10 Jahre ≤ MTTF _d < 30 Jahre
hoch	30 Jahre ≤ MTTF _d ≤ 100 Jahre

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 der Tabelle 5 wird eine Genauigkeit von 5 % angenommen.

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

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

4.5.3 Diagnosedeckungsgrad (DC)

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

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

Tabelle 6 — Diagnosedeckungsgrad (DC)

DC	
Bezeichnung	Bereich
kein	$DC < 60 \%$
niedrig	$60 \% \leq DC < 90 \%$
mittel	$90 \% \leq DC < 99 \%$
hoch	$99 \% \leq DC$

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 eines PL

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

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

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