

DIN EN ISO 13849-1



ICS 13.110

Entwurf

Einsprüche bis 2020-09-17
Vorgesehen als Ersatz für
DIN EN ISO 13849-1:2016-06

**Sicherheit von Maschinen –
Sicherheitsbezogene Teile von Steuerungen –
Teil 1: Allgemeine Gestaltungsleitsätze (ISO/DIS 13849-1:2020);
Deutsche und Englische Fassung prEN ISO 13849-1:2020**

Safety of machinery –
Safety-related parts of control systems –
Part 1: General principles for design (ISO/DIS 13849-1:2020);
German and English version prEN ISO 13849-1:2020

Sécurité des machines –
Parties des systèmes de commande relatives à la sécurité –
Partie 1: Principes généraux de conception (ISO/DIS 13849-1:2020);
Version allemande et anglaise prEN ISO 13849-1:2020

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2020-07-17 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nasg@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Sicherheitstechnische Grundsätze (NASG), 10772 Berlin oder Saatwinkler Damm 42/43, 13627 Berlin.

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

Gesamtumfang 304 Seiten

DIN-Normenausschuss Sicherheitstechnische Grundsätze (NASG)

Nationales Vorwort

Dieses Dokument (prEN ISO 13849-1:2020) wurde vom Technischen Komitee CEN/TC 114 „Sicherheit von Maschinen und Geräten“ erarbeitet, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige deutsche/nationale Normungsgremium ist der Gemeinschaftsarbeitsausschuss NA 095-01-03 GA „Gemeinschaftsarbeitsausschuss NASG/NAM/DKE: Steuerungen“ im DIN-Normenausschuss Sicherheitstechnische Grundsätze (NASG).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

IEC 60204-1:2016	siehe	DIN EN 60204-1 (VDE 0113-1):2019-06
IEC 60447	siehe	DIN EN 60447 (VDE 0196)
IEC 60529	siehe	DIN EN 60529 (VDE 0470-1)
IEC 60812	siehe	DIN EN 60812
IEC 60947 (all parts)	siehe	DIN EN 60947 (alle Teile)
IEC 61000-6-7:2014	siehe	DIN EN 61000-6-7 (VDE 0839-6-7):2015-12
IEC 61078:2016	siehe	DIN EN 61078:2018-03
IEC 61131-3	siehe	DIN EN 61131-3
IEC 61300 (all parts)	siehe	DIN EN 61300-1 (VDE 0885-300) (alle Teile)
IEC 61310 (all parts)	siehe	DIN EN 61310 (VDE 0113) (alle Teile)
IEC 61326-3-1:2017	siehe	DIN EN 61326-3-1 (VDE 0843-20-3-1):2018-04
IEC 61496-1	siehe	DIN EN 61496-1 (VDE 0113-201)
IEC 61508-1:2010	siehe	DIN EN 61508-1 (VDE 0803-1):2011-02
IEC 61508-2:2010	siehe	DIN EN 61508-2 (VDE 0803-2):2011-02
IEC 61508-3:2010	siehe	DIN EN 61508-3 (VDE 0803-3):2011-02
IEC 61508-4:2010	siehe	DIN EN 61508-4 (VDE 0803-4):2011-02
IEC 61508-6:2000	siehe	DIN EN 61508-6 (VDE 0803-6):2003-06
IEC 61800-3	siehe	DIN EN 61800-3 (VDE 0160-103)

IEC 61800-5-2:2016	siehe	DIN EN 61800-5-2 (VDE 0160-105-2):2017-11
IEC 61810 (all parts)	siehe	DIN EN IEC 61810-10 (VDE 0435) (alle Teile)
IEC 62046:2018	siehe	DIN EN IEC 62046 (VDE 0113-211):2019-03
IEC 62061:2015	siehe	DIN EN 62061 (VDE 0113-50):2016-05
ISO 4413	siehe	DIN EN ISO 4413
ISO 4414	siehe	DIN EN ISO 4414
ISO 7731	siehe	DIN EN ISO 7731
ISO 9001	siehe	DIN EN ISO 9001
ISO 10218-1	siehe	DIN EN ISO 10218-1
ISO 10218-2	siehe	DIN EN ISO 10218-2
ISO 11161	siehe	DIN EN ISO 11161
ISO 12100:2010	siehe	DIN EN ISO 12100:2011-03
ISO 13849-2:2012	siehe	DIN EN ISO 13849-2:2013-02
ISO 13850	siehe	DIN EN ISO 13850
ISO 13851	siehe	DIN EN ISO 13851
ISO 13855:2010	siehe	DIN EN ISO 13855:2010-10
ISO 13856-1	siehe	DIN EN ISO 13856-1
ISO 13856-2	siehe	DIN EN ISO 13856-2
ISO 14118	siehe	DIN EN ISO 14118
ISO 14119	siehe	DIN EN ISO 14119
ISO/TR 14121-2:2012	siehe	DIN ISO/TR 14121-2:2013-02
ISO/TR 22100-2:2013	siehe	DIN ISO/TR 22100-2:2014-09
ISO/TR 23849	siehe	DIN ISO/TR 23849

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Änderungen

Gegenüber DIN EN ISO 13849-1:2016-06 wurden folgende Änderungen vorgenommen:

- a) Verweisungen überarbeitet und aktualisiert;
- b) normative Verweisungen und Begriffe und Definitionen überarbeitet;
- c) Integration eines Abschnitts zur Risikobeurteilung (Abschnitt 4);
- d) Beschreibung der Anforderungen an das Design und die verschiedenen Performance Levels (Abschnitt 6);
- e) detaillierte Anforderungen an die Spezifikation der Sicherheitsfunktion
- f) Integration eines neuen Abschnittes (7) zu Softwaresicherheit;
- g) Integration eines neuen Abschnittes (9) zu Ergonomieaspekten;
- h) detaillierte Beschreibung von Validierungsprozessen (Abschnitt 10);
- i) Integration von Anhang L zu Immunitätsanforderungen für elektromagnetische Kompatibilität;
- j) Integration von Anhang M mit zusätzlichen Informationen für das SRS-System;
- k) Integration von Anhang N zur Vermeidung von systematischen Fehlern im Software-Design.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN 60204-1 (VDE 0113-1):2019-06, *Sicherheit von Maschinen — Elektrische Ausrüstung von Maschinen — Teil 1: Allgemeine Anforderungen (IEC 60204-1:2016, modifiziert); Deutsche Fassung EN 60204-1:2018*

DIN EN 60447 (VDE 0196), *Grund- und Sicherheitsregeln für die Mensch-Maschine-Schnittstelle, Kennzeichnung — Bedienungsgrundsätze*

DIN EN 60529 (VDE 0470-1), *Schutzarten durch Gehäuse (IP-Code)*

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

DIN EN 60947 (alle Teile), *Niederspannungsschaltgeräte*

DIN EN 61000-6-7 (VDE 0839-6-7):2015-12, *Elektromagnetische Verträglichkeit (EMV) — Teil 6-7: Fachgrundnormen — Störfestigkeitsanforderungen an Geräte und Einrichtungen, die zur Durchführung von Funktionen in sicherheitsbezogenen Systemen (funktionale Sicherheit) an industriellen Standorten vorgesehen sind (IEC 61000-6-7:2014); Deutsche Fassung EN 61000-6-7:2015*

DIN EN 61078:2018-03, *Zuverlässigkeitsblockdiagramme (IEC 61078:2016); Deutsche Fassung EN 61078:2016*

DIN EN 61131-3, *Speicherprogrammierbare Steuerungen*

DIN EN 61300-1 (VDE 0885-300) (alle Teile), *Lichtwellenleiter*

DIN EN 61310 (VDE 0113) (alle Teile), *Sicherheit von Maschinen — Anzeigen, Kennzeichen und Bedienen*

DIN EN 61326-3-1 (VDE 0843-20-3-1):2018-04, *Elektrische Mess-, Steuer-, Regel- und Laborgeräte — EMV-Anforderungen — Teil 3-1: Störfestigkeitsanforderungen für sicherheitsbezogene Systeme und für Geräte, die für sicherheitsbezogene Funktionen vorgesehen sind (Funktionale Sicherheit) — Allgemeine industrielle Anwendungen (IEC 61326-3-1:2017); Deutsche Fassung EN 61326-3-1:2017*

DIN EN 61496-1 (VDE 0113-201), *Sicherheit von Maschinen — Berührungslos wirkende Schutzeinrichtungen — Teil 1: Allgemeine Anforderungen und Prüfungen*

DIN EN 61508-1 (VDE 0803-1):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 1: Allgemeine Anforderungen (IEC 61508-1:2010); Deutsche Fassung EN 61508-1:2010*

DIN EN 61508-2 (VDE 0803-2):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (IEC 61508-2:2010); Deutsche Fassung EN 61508-2:2010*

DIN EN 61508-3 (VDE 0803-3):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 3: Anforderungen an Software (IEC 61508-3:2010); Deutsche Fassung EN 61508-3:2010*

DIN EN 61508-4 (VDE 0803-4):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 4: Begriffe und Abkürzungen* (IEC 61508-4:2010); Deutsche Fassung EN 61508-4:2010

DIN EN 61508-6 (VDE 0803-6):2003-06, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3* (IEC 61508-6:2000); Deutsche Fassung EN 61508-6:2001

DIN EN 61800-3 (VDE 0160-103), *Drehzahlveränderbare elektrische Antriebe — Teil 3: EMV-Anforderungen einschließlich spezieller Prüfverfahren*

DIN EN 61800-5-2 (VDE 0160-105-2):2017-11, *Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl — Teil 5-2: Anforderungen an die Sicherheit — Funktionale Sicherheit* (IEC 61800-5-2:2016); Deutsche Fassung EN 61800-5-2:2017

DIN EN 62061 (VDE 0113-50):2016-05, *Sicherheit von Maschinen — Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme* (IEC 62061:2005 + A1:2012 + A2:2015); Deutsche Fassung EN 62061:2005 + Cor.:2010 + A1:2013 + A2:2015

DIN EN IEC 62046 (VDE 0113-211):2019-03, *Sicherheit von Maschinen — Anwendung von Schutzeinrichtungen zur Anwesenheitserkennung von Personen* (IEC 62046:2018); Deutsche Fassung EN IEC 62046:2018

DIN EN IEC 61810-10 (VDE 0435) (alle Teile), *Elektromechanische Elementarrelais*

DIN EN ISO 4413, *Fluidtechnik — Allgemeine Regeln und sicherheitstechnische Anforderungen an Hydraulikanlagen und deren Bauteile*

DIN EN ISO 4414, *Fluidtechnik — Allgemeine Regeln und sicherheitstechnische Anforderungen an Pneumatikanlagen und deren Bauteile*

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

DIN EN ISO 9001, *Qualitätsmanagementsysteme — Anforderungen*

DIN EN ISO 10218-1, *Industrieroboter — Sicherheitsanforderungen — Teil 1: Roboter*

DIN EN ISO 10218-2, *Industrieroboter — Sicherheitsanforderungen — Teil 2: Robotersysteme und Integration*

DIN EN ISO 11161, *Sicherheit von Maschinen — Integrierte Fertigungssysteme — Grundlegende Anforderungen*

DIN EN ISO 12100:2011-03, *Sicherheit von Maschinen — Allgemeine Gestaltungsleitsätze — Risikobeurteilung und Risikominderung* (ISO 12100:2010); Deutsche Fassung EN ISO 12100:2010

DIN EN ISO 13849-2:2013-02, *Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen — Teil 2: Validierung* (ISO 13849-2:2012); Deutsche Fassung EN ISO 13849-2:2012

DIN EN ISO 13850, *Sicherheit von Maschinen — Not-Halt-Funktion — Gestaltungsleitsätze*

DIN EN ISO 13851, *Sicherheit von Maschinen — Zweihandschaltungen — Funktionelle Aspekte und Gestaltungsleitsätze*

DIN EN ISO 13855:2010-10, *Sicherheit von Maschinen — Anordnung von Schutzeinrichtungen im Hinblick auf Annäherungsgeschwindigkeiten von Körperteilen* (ISO 13855:2010); Deutsche Fassung EN ISO 13855:2010

DIN EN ISO 13856-1, *Sicherheit von Maschinen — Druckempfindliche Schutzeinrichtungen — Teil 1: Allgemeine Leitsätze für die Gestaltung und Prüfung von Schalmatten und Schaltplatten*

DIN EN ISO 13856-2, *Sicherheit von Maschinen — Druckempfindliche Schutzeinrichtungen — Teil 2: Allgemeine Leitsätze für die Gestaltung und Prüfung von Schaltleisten und Schaltstangen*

DIN EN ISO 14118, *Sicherheit von Maschinen — Vermeidung von unerwartetem Anlauf*

DIN EN ISO 14119, *Sicherheit von Maschinen — Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen — Leitsätze für Gestaltung und Auswahl*

DIN ISO/TR 14121-2:2013-02, *Sicherheit von Maschinen — Risikobeurteilung — Teil 2: Praktischer Leitfaden und Verfahrensbeispiele (ISO/TR 14121-2:2012)*

DIN ISO/TR 22100-2:2014-09, *Sicherheit von Maschinen — Beziehung zu ISO 12100 — Teil 2: Wie ISO 12100 und ISO 13849-1 zusammenhängen (ISO/TR 22100-2:2013)*

DIN ISO/TR 23849, *Leitfaden zur Anwendung von ISO 13849-1 und IEC 62061 bei der Gestaltung von sicherheitsbezogenen Steuerungen für Maschinen*

— Leerseite —

<i>Titel de:</i>	Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen — Teil 1: Allgemeine Gestaltungsleitsätze (ISO/DIS 13849-1:2020)
<i>Titel en:</i>	Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design (ISO/DIS 13849-1:2020)
<i>Titel fr:</i>	Sécurité des machines — Parties des systèmes de commande relatives à la sécurité — Partie 1: Principes généraux de conception (ISO/DIS 13849-1:2020)

Inhalt

	Seite
Europäisches Vorwort	6
Vorwort	7
Einleitung	8
1 Anwendungsbereich	12
2 Normative Verweisungen	12
3 Begriffe	13
3.1 Begriffe	13
3.2 Symbole und Abkürzungen	22
4 Überblick	24
4.1 Anforderungen an die Risikobeurteilung und Risikominderung	24
4.2 Beitrag der Sicherheitsfunktion zur Risikominderung	26
4.3 Risikominderung mithilfe eines SRP/CS	27
4.4 Verfahren	29
4.5 Erforderliche Informationen	30
4.6 Ausführung von Sicherheitsfunktionen mithilfe von Teilsystemen	30
5 Spezifikation der Sicherheitsfunktionen	31
5.1 Allgemeines	31
5.2 Spezifikation der Sicherheitsanforderungen (SRS, en: safety requirements specification)	31
5.2.1 Allgemeine Anforderungen	31
5.2.2 Zerlegung eines SRP/CS in Teilsysteme	34
5.2.3 Anforderungen an spezifische Sicherheitsfunktionen	36
5.3 Bestimmung des erforderlichen Performance Levels (PL _r) für jede Sicherheitsfunktion	41
5.4 Überprüfung der Spezifikation der Sicherheitsanforderungen	41
6 Gestaltungsaspekte	41
6.1 Bewertung des erreichten Performance Levels PL	41
6.1.1 Allgemeine Übersicht der Performance Level PL	41
6.1.2 Zusammenhang zwischen PL und SIL	43
6.1.3 Architektur – Kategorien und deren Beziehung zur MTTF _D jedes Kanals, zum DC _{avg} und zum CCF	44
6.1.4 Mittlere Zeit bis zum gefahrbringenden Ausfall (MTTF _D)	52
6.1.5 Diagnosedeckungsgrad (DC)	53
6.1.6 Ausfälle infolge gemeinsamer Ursache (CCF)	54
6.1.7 Systematische Ausfälle	54
6.1.8 Vereinfachtes Verfahren zur Abschätzung des PL	54
6.1.9 Alternatives Verfahren für die Bestimmung von PL und PFH _D ohne MTTF _D	56
6.1.10 Fehlerbetrachtung und Fehlerausschluss	58
6.1.11 Bewährtes Bauteil	59
6.2 Kombination von Teilsystemen zum Erreichen eines Gesamt-PL für die Sicherheitsfunktion	60
6.2.1 Allgemeines	60
6.2.2 Bekannte PFH _D -Werte	60
6.2.3 Unbekannte PFH _D -Werte	61
7 Software-Sicherheitsanforderungen	61
7.1 Allgemeines	61

7.2	Sicherheitsbezogene Embedded-Software (SRESW)	62
7.3	Sicherheitsbezogene Anwendungssoftware (SRASW)	64
7.4	Programmiersprache mit eingeschränktem Sprachumfang (LVL)	67
7.4.1	Allgemeines	67
7.4.2	Programmiersprache mit nicht eingeschränktem Sprachumfang (FVL)	67
7.4.3	Entscheidung zwischen LVL oder FVL	68
7.5	Softwarebasierte Parametrisierung	69
7.5.1	Allgemeines	69
7.5.2	Einflüsse auf sicherheitsbezogene Parameter	70
7.5.3	Anforderungen an die softwarebasierte manuelle Parametrisierung	70
7.5.4	Verifizierung des Parametrisierungswerkzeugs	72
7.5.5	Ausführung der softwarebasierten manuellen Parametrisierung	72
8	Verifizierung, ob der erreichte PL dem PL _r entspricht	72
9	Ergonomische Aspekte der Gestaltung	73
10	Validierung	73
10.1	Grundsätze der Validierung	73
10.1.1	Allgemeines	73
10.1.2	Validierungsplan	75
10.1.3	Allgemeine Fehlerlisten	76
10.1.4	Spezielle Fehlerlisten	76
10.1.5	Angaben zur Validierung	76
10.2	Validierung durch Analyse	78
10.2.1	Allgemeines	78
10.2.2	Analysetechniken	78
10.3	Validierung durch Prüfung	79
10.3.1	Allgemeines	79
10.3.2	Messgenauigkeit	79
10.3.3	Zusätzliche Prüfanforderungen	80
10.3.4	Anzahl der Prüflinge	80
10.3.5	Prüfverfahren	80
10.4	Validierung der Spezifikation der Sicherheitsanforderungen (SRS)	81
10.5	Validierung der Sicherheitsfunktion	81
10.6	Validierung der Sicherheitsintegrität des SRP/CS	82
10.6.1	Validierung von Teilsystem(en)	82
10.6.2	Validierung der Maßnahmen zur Vermeidung systematischer Ausfälle	84
10.6.3	Validierung der sicherheitsbezogenen Software	85
10.6.4	Validierung der Kombination von Teilsystemen	86
10.6.5	Überprüfung/Verifizierung der Sicherheitsintegrität	86
11	Instandhaltung	86
12	Technische Dokumentation	87
13	Benutzerinformation	87
13.1	Allgemeines	87
13.2	Informationen für den SRP/CS-Integrator	87
13.3	Informationen für den Benutzer	88
Anhang A (informativ)	Bestimmung des erforderlichen Performance Levels (PL _r)	90
A.1	Auswahl des PL _r	90
A.2	Anleitung für die Auswahl der Parameter S, F und P zur Einschätzung des Risikos	91
A.2.1	Schwere der Verletzung S1 und S2	91
A.2.2	Häufigkeit und/oder Dauer der Gefährdungsexposition F1 und F2	91
A.2.3	Möglichkeit zur Vermeidung des Schadens	92
A.3	Überlagerte Gefährdungen	94

Anhang B (informativ) Blockmethode und sicherheitsbezogenes Blockdiagramm.....	95
B.1 Blockmethode	95
B.2 Sicherheitsbezogenes Blockdiagramm.....	95
Anhang C (informativ) Berechnung oder Abschätzung von MTTF _D -Werten für einzelne Bauteile	97
C.1 Allgemeines	97
C.2 Verfahren guter ingenieurmäßiger Praxis	97
C.3 Hydraulische Bauteile.....	97
C.4 MTTF _D von pneumatischen, mechanischen und elektromechanischen Bauteilen	99
C.4.1 Allgemeines	99
C.4.2 Berechnung der MTTF _D für Bauteile aus B_{10D}	100
C.4.3 Erläuterung der Gleichungen	101
C.4.4 Beispiel	101
C.5 MTTF _D -Daten für elektrische Bauteile.....	102
C.5.1 Allgemeines	102
C.5.2 Halbleiter.....	102
C.5.3 Passive Bauteile	103
Anhang D (informativ) Vereinfachtes Verfahren zur Abschätzung der MTTF _D für jeden Kanal.....	105
D.1 Parts-Count-Verfahren	105
D.2 MTTF _D für unterschiedliche Kanäle, Symmetrisierung der MTTF _D für jeden Kanal	106
Anhang E (informativ) Abschätzungen des Diagnosedeckungsgrades (DC) für Funktionen und Module	108
E.1 Beispiele für den Diagnosedeckungsgrad (DC)	108
E.2 Abschätzung des durchschnittlichen DC (DC _{avg})	111
Anhang F (informativ) Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF).....	112
F.1 Allgemeines	112
F.2 Abschätzung der Auswirkung eines CCF	112
F.3 Beschreibung der Maßnahmen gegen CCF nach Tabelle F.1	113
F.4 Maßnahmen gegen CCF und weitere einschlägige Normen	115
Anhang G (informativ) Systematischer Ausfall	116
G.1 Allgemeines	116
G.2 Maßnahmen zur Beherrschung systematischer Ausfälle	116
G.3 Maßnahmen zur Vermeidung systematischer Ausfälle.....	117
G.4 Maßnahmen zur Vermeidung systematischer Ausfälle während der Integration des SRP/CS	118
Anhang H (informativ) Beispiel für eine Kombination von mehreren Teilsystemen.....	119
Anhang I (informativ) Beispiele.....	122
I.1 Allgemeines	122
I.2 Sicherheitsfunktion und erforderlicher Performance Level (PL _r).....	122
I.3 Beispiel A, einkanaliges System	123
I.3.1 Identifikation der sicherheitsbezogenen Teile	123
I.3.2 Quantifizierung von MTTF _D , DC _{avg} , Maßnahmen gegen den Ausfall infolge gemeinsamer Ursache (CCF), Kategorie, PL	124
I.4 Beispiel B, redundantes System	125
I.4.1 Identifikation der sicherheitsbezogenen Teile	125
I.4.2 Quantifizierung der MTTF _D für jeden Kanal, DC _{avg} , Maßnahmen gegen den Ausfall infolge gemeinsamer Ursache (CCF), Kategorie und PL	127
Anhang J (informativ) Software	131
J.1 Beschreibung des Beispiels	131
J.2 Anwendung des V-Modells des Software-Sicherheitslebenszyklus	132
J.3 Verifizierung der Softwarespezifikation	132
J.4 Beispiel von Programmierregeln	133

Anhang K (informativ) Numerische Darstellung von Bild 12	135
Anhang L (informativ) Anforderungen an die elektromagnetische Störfestigkeit.....	139
Anhang M (informativ) Zusätzliche Informationen zur Spezifikation der Sicherheitsanforderungen	142
Anhang N (informativ) Vermeiden eines systematischen Ausfalls durch den Softwareentwurf	144
N.1 Auswahl von Maßnahmen zur Fehlervermeidung für den Softwareentwurf	144
Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der abzudeckenden EU-Richtlinie 2006/42/EG	156
Literaturhinweise.....	157

Europäisches Vorwort

Dieses Dokument (prEN ISO 13849-1:2020) wurde vom Technischen Komitee CEN/TC 114 „Sicherheit von Maschinen und Geräten“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur parallelen Umfrage vorgelegt.

Dieses Dokument wird EN ISO 13849-1:2015 ersetzen.

Dieses Dokument wurde im Rahmen eines Normungsauftrages erarbeitet, den die Europäische Kommission und die Europäische Freihandelsassoziation CEN erteilt haben, und unterstützt grundlegende Anforderungen der EU-Richtlinien.

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

Anerkennungsnotiz

Der Text von ISO/DIS 13849-1:2020 wurde von CEN als prEN ISO 13849-1:2020 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) ist eine weltweite Vereinigung nationaler Normungsinstitute (ISO-Mitgliedsorganisationen). Die Erstellung von Internationalen Normen wird üblicherweise von Technischen Komitees von ISO 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 staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO stehen, nehmen ebenfalls an der Arbeit teil. ISO arbeitet bei allen elektrotechnischen Normungsthemen eng mit der Internationalen Elektrotechnischen Kommission (IEC) 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. Es sollten insbesondere die unterschiedlichen Annahmekriterien für die verschiedenen ISO-Dokumentenarten 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 erhaltenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom Technischen Komitee ISO/TC 199, *Safety of machinery* erarbeitet.

Die erste Ausgabe von ISO 13849-1 wurde im Jahr 1999 veröffentlicht und basierte auf EN 954-1:1996.

Die zweite Ausgabe von ISO 13849-1 wurde im Jahr 2006 als überarbeitete Fassung veröffentlicht.

Die dritte Ausgabe wurde im Jahr 2015 als geänderte Fassung veröffentlicht.

Diese vierte Ausgabe ersetzt die dritte Ausgabe (ISO 13849-1:2015), die technisch überarbeitet wurde.

Eine Auflistung aller Teile der Normenreihe ISO 13849 ist auf der ISO-Internetseite abrufbar.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html zu finden.

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 angewendet werden können.
- b) Typ-B-Normen (Sicherheitsfachgrundnormen) behandeln einen oder mehrere Sicherheitsaspekte oder eine oder mehrere Arten 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 Gruppe von Maschinen.

Dieser Teil von ISO 13849 ist eine Typ-B1-Norm, wie in ISO 12100 angegeben.

Dieses Dokument ist insbesondere für die folgenden Interessengruppen von Relevanz, die die Marktakteure im Hinblick auf die Sicherheit von Maschinen repräsentieren:

- Maschinenhersteller (kleine, mittlere und große Unternehmen);
- Organisationen des Arbeits- und Gesundheitsschutzes (Gesetzgeber, Unfallversicherungen, Marktaufsicht usw.).

Das Niveau der Maschinensicherheit, das mithilfe dieses Dokuments von den oben genannten Interessengruppen erreicht wird, kann weitere interessierte Kreise betreffen. Es handelt sich dabei um:

- Maschinenanwender/Arbeitgeber (kleine, mittlere und große Unternehmen);
- Maschinenanwender/Arbeitnehmer (z. B. Gewerkschaften, Organisationen für Personen mit besonderen Bedürfnissen);
- Dienstleister (kleine, mittlere und große Unternehmen), z. B. für die Instandhaltung;
- Verbraucher (falls die behandelten Maschinen für die Nutzung durch Verbraucher bestimmt sind).

Den oben genannten Interessengruppen wurde die Möglichkeit eingeräumt, am Erarbeitungsprozess dieser Norm mitzuwirken.

Des Weiteren ist dieses Dokument an Normungsgremien gerichtet, die Typ-C-Normen erarbeiten.

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

Für Maschinen, die nach den Festlegungen der Typ-C-Norm konzipiert und gebaut worden sind, gilt: Wenn die Festlegungen in einer Typ-C-Norm von den Festlegungen in Typ-A- oder Typ-B-Normen abweichen, haben die Festlegungen der Typ-C-Norm Vorrang gegenüber den Festlegungen der anderen Normen.

ANMERKUNG 1 Die Grundlage für die Beispiele und für den Großteil des Inhalts bilden stationäre Maschinen in industriellen Anwendungen. Dies schließt jedoch andere Maschinen nicht aus. Dieses Dokument wurde mit der Absicht erarbeitet, in zahlreichen verschiedenen Maschinenindustrien angewendet zu werden sowie die Grundlage für Normungsgremien, die Typ-C-Normen erarbeiten, zu bilden.

Ziel dieses Teils von ISO 13849 ist es, denjenigen Interessengruppen einen Leitfaden bereitzustellen, die an der Gestaltung und Beurteilung von Steuerungen beteiligt sind, sowie den Technischen Komitees, die Typ-B2- oder Typ-C-Normen erarbeiten.

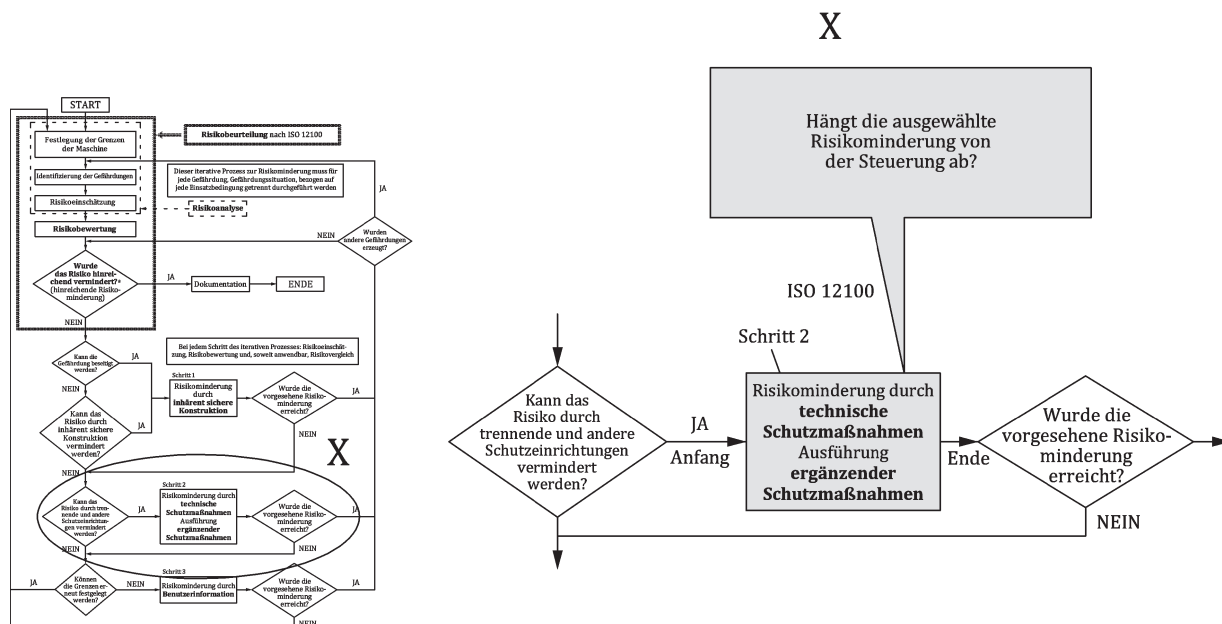
Risikominderung nach ISO 12100:2010, Abschnitt 6, wird erzielt, indem in der folgenden Reihenfolge Maßnahmen für eine inhärent sichere Konstruktion, Schutzmaßnahmen und/oder ergänzende risikomindernde Maßnahmen und Benutzerinformationen angewendet werden. Ein Konstrukteur kann Risiken durch risikomindernde Maßnahmen reduzieren, die Sicherheitsfunktionen besitzen können. Teile der Maschinensteuerung, die mit Sicherheitsfunktionen versehen sind, werden als sicherheitsbezogene Teile von Steuerungen (SRP/CS, en: safety-related parts of control systems) bezeichnet. Hierbei kann es sich um Hardware und/oder Software handeln, die entweder von der Maschinensteuerung getrennt verfügbar oder ein fester Bestandteil der Maschinensteuerung sein kann. Neben der Ausführung von Sicherheitsfunktionen können SRP/CS auch Betriebsfunktion ausführen.

ISO 12100 wird für die Risikobeurteilung der Maschine angewendet. Mithilfe von ISO 13849-1, Anhang A, kann der erforderliche Performance Level (PL_r) einer Sicherheitsfunktion, die vom SRP/CS ausgeführt wird, bestimmt werden, wenn kein PL_r in der einschlägigen Typ-C-Norm festgelegt ist.

ISO 13849-1 ist für die Sicherheitsfunktionen von SRP/CS von Bedeutung, die ausgeführt werden, um Risiken abzudecken, wenn eine nach ISO 12100 durchgeführte Risikobeurteilung Anlass für die Umsetzung einer risikomindernden Maßnahme (z. B. verriegelte trennende Schutzeinrichtung) gegeben hat, die auf einer sicherheitsbezogenen Steuerung basiert. In solchen Fällen muss die sicherheitsbezogene Steuerung eine Sicherheitsfunktion ausführen. ISO 13849-1 sollte bei der Gestaltung und Bewertung der sicherheitsbezogenen Teile der Steuerung angewendet werden. Nur derjenige Teil der Steuerung, der in Bezug zur Sicherheit steht (sicherheitsbezogen ist), wird vom Anwendungsbereich der ISO 13849-1 abgedeckt.

Bild 1 zeigt den Zusammenhang zwischen ISO 12100 und ISO 13849-1.

ANMERKUNG 2 Siehe auch ISO/TR 22100-2:2013 für weitere Informationen.



- a Beim erstmaligen Stellen der Frage wird diese mit dem Ergebnis der Ausgangsrisikobewertung beantwortet. Für weitere Informationen siehe Bild A.1.

Bild 1 — Integration von ISO 13849-1 in den Prozess zur Risikominderung nach ISO 12100

ANMERKUNG 3 Bild 1 zeigt auf, wo das SRP/CS zum Prozess der Risikominderung von ISO 12100, Schritt 2, beiträgt. Durch die Ausführung von Sicherheitsfunktionen unterstützt das SRP/CS die kombinierten risikomindernden Maßnahmen.

Die Fähigkeit sicherheitsbezogener Teile von Steuerungen, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen, wird einer von fünf Stufen zugeordnet, den so genannten Performance Level (PL). Der erforderliche Performance Level (PL_r) für eine bestimmte Sicherheitsfunktion wird durch Risikoeinschätzung ermittelt.

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.

Die funktionale Sicherheit umfasst eine Kategorisierung der Architektur nach spezifischer Gestaltung und festgelegtem Verhalten unter Fehlerbedingungen. Diese Architektur wird einer der fünf Kategorien B, 1, 2, 3 und 4 zugeordnet.

Die funktionale Sicherheit berücksichtigt das Ausfallverhalten der Elemente/Bauteile, die eine Sicherheitsfunktion ausführen. Für jede Sicherheitsfunktion wird dieses Ausfallverhalten als die Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde (PFH_D; en: probability of dangerous failure per hour) angegeben.

Die Risikoeinschätzung weist aufgrund der Subjektivität der Bewertungskriterien eine Varianz auf. Typ-C-Normen können spezifischere Methoden zur Risikoeinschätzung für spezifische Maschinenanwendungen enthalten, die eine geringere Subjektivität aufweisen können. Aus diesem Grund sollte die in diesem Dokument beschriebene Vorgehensweise eher als nützlicher Leitfaden für die Gestaltung von sicherheitsbezogenen Teilen der Steuerung angesehen werden und nicht als strenge

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

- Steuerungsbaugruppen (z. B. die Logik für Steuerungsfunktionen, Datenverarbeitung, Überwachung usw.), und
- berührungslos wirkende Schutzeinrichtungen (z. B. Lichtschranken), druckempfindliche Schutzeinrichtungen.

Es können die Performance Level berechnet und die Kategorien ermittelt werden für:

- SRP/CS, die Sicherheitsfunktionen für Maschinen ausführen;
- Teilsysteme von SRP/CS, die sicherheitsbezogene Teile (Komponenten) nutzen, wie beispielsweise:
- Schutzeinrichtungen (z. B. Zweihandschaltungen, Verriegelungseinrichtungen);
- leistungssteuernde Elemente (z. B. Relais, Ventile);
- Sensoren und HMI-Elemente (Wegmesseinrichtungen, Freigabeschalter).

Die von dieser Norm berücksichtigten Maschinen können von einfachen Maschinen (z. B. Küchenkleingeräte oder Automatiktüren und -tore) bis hin zu komplexen Maschinen (z. B. Verpackungsmaschinen, Druckereimaschinen, Pressen) reichen.

IEC 62061 und dieser Teil von ISO 13849 legen zusammen ein Verfahren fest und enthalten entsprechende Leitlinien für die Gestaltung und die Ausführung sicherheitsbezogener Steuerungen von Maschinen.

ANMERKUNG ISO/TR 23849 enthält einen Leitfaden zum Zusammenhang zwischen diesen beiden Normen und erläutert, wie sie sich gegenseitig ergänzen.

Die Anforderungen von ISO 13849-1, Abschnitt 10, ersetzen die Anforderungen von ISO 13849-2:2012 mit Ausnahme der informativen Anhänge. Es wird davon ausgegangen, dass ein SRP/CS, das den Anforderungen von Abschnitt 10 entspricht, die Anforderungen von ISO 13849-2:2012 ebenfalls erfüllt.

1 Anwendungsbereich

Dieser Teil von ISO 13849 legt ein Verfahren fest und enthält einen Leitfaden für die Gestaltung und Integration sicherheitsbezogener Teile von Steuerungen (SRP/CS), einschließlich der Entwicklung von Software. Dieses Dokument legt die Eigenschaften fest, die notwendig sind, um den erforderlichen Performance Level von Sicherheitsfunktionen zu ermitteln. Dieses Dokument gilt für SRP/CS in vielen Maschinenarten mit Betriebsart mit hoher Anforderungsrate und Betriebsart mit kontinuierlicher Anforderung einschließlich ihrer Teilsysteme, ungeachtet der Technologie und Energie (z. B. elektrisch, hydraulisch, pneumatisch, mechanisch). Die Norm gilt nicht für Betriebsarten mit niedriger Anforderungsrate.

Dieses Dokument legt nicht fest, welche Sicherheitsfunktionen oder erforderlichen Performance Level für spezielle Fälle zu verwenden sind.

Dieses Dokument stellt keine speziellen Anforderungen an den Entwurf von Produkten, die Teile von SRP/CS sind.

Dieses Dokument enthält keine spezifischen Maßnahmen für sicherheitsrelevante Aspekte (z. B. physische Sicherheitsaspekte, IT-Sicherheitsaspekte, Cybersicherheitsaspekte).

ANMERKUNG 1 Dieses Dokument legt ein Verfahren für die Gestaltung von SRP/CS fest, ohne dabei zu berücksichtigen, ob für bestimmte Maschinen (z. B. ortsveränderliche Maschinen) spezifische Anforderungen notwendig sind. Diese spezifischen Anforderungen können in einer Typ-C-Norm festgelegt sein.

ANMERKUNG 2 Siehe IEC 61508 für die Betriebsart mit niedriger Anforderungsrate.

ANMERKUNG 3 Siehe auch ISO/TR 22100-4 für IT-Sicherheitsaspekte und IEC/TR 63074 für allgemeine Sicherheitsaspekte.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. 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 13849-2:2013, *Safety of machinery — Safety-related parts of control systems — Part 2: Validation*

IEC 60204-1:2016, *Safety of machinery — Electrical equipment of machines — Part 1: General requirements*

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements*

IEC 62046:2018, *Safety of machinery — Application of protective equipment to detect the presence of persons*

ISO 62061:2015, *Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO 12100 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>
- ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>

3.1 Begriffe

3.1.1

sicherheitsbezogenes Teil einer Steuerung

SRP/CS, en: safety-related part of a control system

Teil einer Steuerung, der eine Sicherheitsfunktion ausführt, beginnend mit (einer) sicherheitsbezogenen Eingabe(n) bis hin zur Erzeugung von (einer) sicherheitsbezogenen Ausgabe(n)

Anmerkung 1 zum Begriff: Die sicherheitsbezogenen Teile einer Steuerung beginnen an dem Punkt, an dem sicherheitsbezogene Eingaben erzeugt werden (einschließlich z. B. Betätiger und Rolle eines Positionsschalters) und enden an den Ausgängen der leistungssteuernden Elemente (einschließlich z. B. Hauptkontakte eines Schützes).

3.1.2

Spezifikation der Sicherheitsanforderungen

SRS, en: safety requirement specification

Spezifikation der Anforderungen an die Sicherheitsfunktionen, die von der sicherheitsbezogenen Steuerung ausgeführt werden müssen; die Spezifikation erfolgt im Hinblick auf die Eigenschaften der Sicherheitsfunktionen (funktionale Eigenschaften) und die erforderlichen Performance Level

[QUELLE: IEC 61508-4:2010, 3.5.11 und 3.5.12, modifiziert, ANMERKUNG hinzugefügt]

3.1.3

Kategorie

Einstufung des Teilsystems bezüglich des Widerstands gegen Fehler und des nachfolgenden Verhaltens bei einem Fehler, das erreicht wird durch die Struktur der Anordnung der Teile, der Fehlererkennung und/oder ihrer Zuverlässigkeit

3.1.4

Fehler

Zustand eines Geräts, 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 Ergebnis eines Ausfalls der Einheit selbst, er kann aber auch ohne vorherigen Ausfall vorhanden sein.

Anmerkung 2 zum Begriff: In diesem Teil von ISO 13849-1 bedeutet der Begriff „Fehler“ entweder „zufälliger Fehler“ oder „durch systematischen Ausfall hervorgerufener Fehler“.

[QUELLE: IEC 60050-192:2015; modifiziert: Anmerkung 2 zum Begriff hinzugefügt]

3.1.5

Fehlerausschluss

Ausschluss von bestimmten Fehlern eines SRP/CS, wenn dies aufgrund ihrer Unwahrscheinlichkeit und ihres unbedeutenden Beitrags zur Zuverlässigkeit des SRP/CS gerechtfertigt ist

3.1.6

Ausfall

Beendigung der Fähigkeit eines Geräts, eine geforderte Funktion auszuführen

Anmerkung 1 zum Begriff: Nach einem Ausfall hat das Gerät einen Fehler.

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

Anmerkung 3 zum Begriff: Ausfälle, die nur die Verfügbarkeit des zu steuernden Prozesses betreffen, liegen nicht im Anwendungsbereich dieses Teils von ISO 13849.

[QUELLE: IEC 60050-192:2015; modifiziert: Anmerkung 4 zum Begriff hinzugefügt]

3.1.7

gefährbringender Ausfall

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

Anmerkung 1 zum Begriff: Ob dieses Potential bemerkt wird oder nicht, kann von der Leitungsarchitektur des Systems abhängen; in redundanten Systemen wird ein gefährbringender Hardwareausfall weniger wahrscheinlich zu einem gefährbringenden Ausfall oder zu einer gefährbringenden Fehlfunktion des Gesamtsystems führen.

[QUELLE: IEC 61508-4:2010, 3.6.7]

3.1.8

Ausfall infolge gemeinsamer Ursache

CCF, en: common cause failure

Ausfall, der das Ergebnis eines oder mehrerer Ereignisse ist, die gleichzeitige Ausfälle von zwei oder mehr getrennten Kanälen in einem mehrkanaligen Teilsystem verursachen und zum Ausfall einer Sicherheitsfunktion führen

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

[QUELLE: IEC 61508-4:2010]

3.1.9

systematischer Ausfall

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

Anmerkung 1 zum Begriff: Instandsetzung ohne Änderung wird üblicherweise nicht die Ausfallursache beseitigen.

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

Anmerkung 3 zum Begriff: Beispielursachen für systematische Ausfälle umfassen menschliches Versagen bei

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

[QUELLE: IEC 60050-192:2015]

3.1.10

Muting

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

3.1.11

manuelle Rückstellung

Sicherheitsfunktion des SRP/CS zum manuellen Wiederherstellen einer oder mehrerer Sicherheitsfunktionen vor dem Wiederanlaufen einer Maschine

3.1.12

Schaden

physische Verletzung oder Gesundheitsschädigung

[QUELLE: ISO 12100:2010, 3.5]

3.1.13

Gefährdung

potentielle Schadensquelle

Anmerkung 1 zum Begriff: Eine Gefährdung kann spezifiziert werden, um 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 und 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, Anmerkung 3 wurde gestrichen]

3.1.14

Gefährdungssituation

Sachlage, bei der eine Person mindestens einer Gefährdung ausgesetzt ist

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

[QUELLE: ISO 12100:2010, 3.10]

3.1.15

Risiko

Kombination der Wahrscheinlichkeit des Eintritts eines Schadens und seines Schadensausmaßes

[QUELLE: ISO 12100:2010, 3.12]

3.1.16

Restrisiko

verbleibendes Risiko, nachdem risikomindernde Maßnahmen (Schutzmaßnahmen) ergriffen wurden

Anmerkung 1 zum Begriff: Siehe Bild 2.

[QUELLE: ISO 12100:2010, 3.13, Anmerkung 1 zum Begriff geändert]

3.1.17

Risikobeurteilung

Gesamtheit des Verfahrens, das eine Risikoanalyse und Risikobewertung umfasst

[QUELLE: ISO 12100:2010, 3.17]

3.1.18

Risikoanalyse

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

[QUELLE: ISO 12100:2010, 3.15]

3.1.19

Risikobewertung

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

[QUELLE: ISO 12100:2010, 3.16]

3.1.20

bestimmungsgemäße Verwendung einer Maschine

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

[QUELLE: ISO 12100:2010, 3.23]

3.1.21

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]

3.1.22

Sicherheitsfunktion

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

Anmerkung 1 zum Begriff: Eine Sicherheitsfunktion ist eine Funktion, die von einem sicherheitsbezogenen Teil einer Steuerung auszuführen ist und die benötigt wird, um einen sicheren Zustand für die Maschine zu erreichen oder ihn im Falle eines spezifischen Gefährdungsereignisses aufrecht zu erhalten.

[QUELLE: ISO 12100:2010, 3.30]

3.1.23

Überwachung

Diagnosemaßnahme, mit der ein Zustand erkannt und mit einem erwarteten Wert verglichen wird

Anmerkung 1 zum Begriff: Überwachung erfolgt durch folgende Verfahren: Plausibilitätsprüfung (direkte oder indirekte Überwachung), zyklische Testimpulse oder Kreuzvergleiche.

3.1.24

Kreuzvergleich

Diagnosemaßnahme zur Überprüfung der Plausibilität von redundanten Signalen in beiden Kanälen einer redundanten Logikeinheit

3.1.25

programmierbares elektronisches System **PE-System**

System zur Steuerung, zum Schutz oder zur Überwachung, basierend auf einem oder mehreren programmierbaren elektronischen Geräten, einschließlich aller Elemente des Systems wie z. B. Energieversorgung, Sensoren und anderer Eingabegeräte, Datenverbindungen und anderer Kommunikationswege sowie Aktoren und anderer Ausgabeeinrichtungen

[QUELLE: IEC 61508-4:2010, 3.3.1]

3.1.26

Performance Level **PL**

diskrete Stufe, welche die Fähigkeit von sicherheitsbezogenen Teilen einer Steuerung spezifiziert, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen

Anmerkung 1 zum Begriff: Siehe 6.1.

3.1.27

erforderlicher Performance Level **PL_r**

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

Anmerkung 1 zum Begriff: Siehe Bild 2 und Bild A.1.

3.1.28

mittlere Zeit bis zum gefahrbringenden Ausfall

MTTF_D, en: mean time to dangerous failure

erwarteter Wert der Zeit bis zum gefahrbringenden Ausfall

Anmerkung 1 zum Begriff: Im Fall von Einheiten mit exponentieller Verteilung der Betriebszeiten bis zum gefahrbringenden Ausfall (d. h. einer konstanten Ausfallrate) ist der numerische Wert von MTTF_D gleich dem Kehrwert der gefahrbringenden Ausfallrate.

[QUELLE: IEC 62061:2005, 3.2.34, Anmerkung 1 zum Begriff modifiziert]

3.1.29

mittlere Betriebsdauer zwischen Ausfällen

MTBF, en: mean time between failure

erwarteter Wert der Betriebsdauer zwischen aufeinanderfolgenden Ausfällen

3.1.30

Anteil gefahrbringender Ausfälle

RDF, en: ratio of dangerous failures

Anteil an der Gesamtausfallrate eines Elements, der zu einem gefahrbringenden Ausfall führen kann

3.1.31

Diagnosedeckungsgrad

DC, en: diagnostic coverage

Maß für die Wirksamkeit der Diagnosemaßnahmen, bestimmt als das Verhältnis der Rate der erkannten gefahrbringenden Ausfälle zur Gesamtrate der gefahrbringenden Ausfälle

Anmerkung 1 zum Begriff: Der Diagnosedeckungsgrad kann für das gesamte sicherheitsbezogene System oder für Teile eines sicherheitsbezogenen Systems gelten. Zum Beispiel könnte ein Diagnosedeckungsgrad für die Sensoren und/oder das Logiksystem und/oder für die leistungssteuernden Elemente vorhanden sein.

[QUELLE: IEC 61508-4:2010, 3.8.6]

3.1.32

risikomindernde Maßnahme

Schutzmaßnahme

Handlung oder Mittel zur Beseitigung von Gefährdungen oder zur Verminderung von Risiken

BEISPIEL Inhärent sichere Konstruktion; Schutzeinrichtungen; persönliche Schutzausrüstungen; Informationen zur Nutzung und Installation; Arbeitsorganisation; Schulungs- und Ausbildungsmaßnahmen; Anwendung von Ausrüstung; Überwachung.

[QUELLE: ISO Guide 51:2014, 3.13]

3.1.33

Gebrauchsdauer

T_M

Zeitraum, der die bestimmungsgemäße Verwendung eines SRP/CS abdeckt

Anmerkung 1 zum Begriff: Das SRP/CS wird üblicherweise nach Ablauf der Gebrauchsdauer ausgetauscht.

3.1.34

Testrate

r_t

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

3.1.35

Anforderungsrate

r_d

Häufigkeit von Anforderungen für eine von einem SRP/CS auszuführende Sicherheitsfunktion

3.1.36

Maschinensteuerung

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

Anmerkung 1 zum Begriff: Die Maschinensteuerung kann jede Technologie oder Kombination verschiedener Technologien verwenden (z. B. elektrische/elektronische, hydraulische, pneumatische und mechanische).

3.1.37

Sicherheits-Integritätslevel

SIL, en: safety integrity level

diskrete Stufe (eine von vier möglichen) zur Festlegung der Anforderungen an die Sicherheitsintegrität der Sicherheitsfunktionen, die den sicherheitsbezogenen elektrischen/elektronischen/programmierbar elektronischen Systemen zugeordnet werden, wobei Sicherheits-Integritätslevel 4 die höchste Stufe der Sicherheitsintegrität und Sicherheits-Integritätslevel 1 die niedrigste Stufe darstellt

[QUELLE: IEC 61508-4:2010, 3.5.8]

3.1.38

Programmiersprache mit eingeschränktem Sprachumfang

LVL, en: limited variability language

Sprachentypus, der es erlaubt, vordefinierte anwendungsspezifische Bibliotheksfunktionen und Grundlogik miteinander zu kombinieren, um so die Spezifikation der Sicherheitsanforderungen umzusetzen

Anmerkung 1 zum Begriff: Typische Beispiele von LVL (Kontaktplan, Funktionsbausteinsprache) sind in IEC 61131-3 angegeben.

[QUELLE: IEC 61511-1:2017, 3.2.75.2]

3.1.39

Programmiersprache mit nicht eingeschränktem Sprachumfang

FVL, en: full variability language

Sprachentypus, der die Fähigkeit hat, eine große Vielfalt von Funktionen und Anwendungen umzusetzen

Anmerkung 1 zum Begriff: Im Bereich der Maschinen findet sich FVL als C/C++-Compiler üblicherweise in Embedded-Software und wird selten in Anwendungssoftware verwendet.

[QUELLE: IEC 61511-1:2017, 3.2.75.3, modifiziert: Anmerkung 1 zum Begriff wurde gestrichen; Anmerkung 2 zum Begriff wurde geändert]

3.1.40

sicherheitsbezogene Anwendungssoftware

SRASW, en: safety related application software

anwendungsspezifische Software, die 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

3.1.41

sicherheitsbezogene Embedded-Software

SRESW, en: safety related embedded software

Firmware

Systemsoftware

Software, die als Bestandteil des Systems vom Hersteller mitgeliefert wird und durch den Endbenutzer der Maschine nicht verändert werden kann

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

[QUELLE: IEC 61511-1:2016, 3.2.76.2]

3.1.42

Betriebsart mit hoher Anforderungsrate oder Betriebsart mit kontinuierlicher Anforderung

Betriebsart, in der die Häufigkeit von Anforderungen an ein SRP/CS für die Ausführung seiner Sicherheitsfunktion mehr als einmal je Jahr beträgt oder die Sicherheitsfunktion die Maschine als Teil des Normalbetriebs in einem sicheren Zustand hält

[QUELLE: IEC 61508-4:2010, 3.5.16]

3.1.43

Betriebsart mit niedriger Anforderungsrate

Betriebsart, in der die Häufigkeit von Anforderungen an ein SRP/CS für die Ausführung seiner Sicherheitsfunktion nicht mehr als einmal je Jahr beträgt

Anmerkung 1 zum Begriff: Die Betriebsart mit niedriger Anforderungsrate wird in diesem Dokument nicht behandelt, siehe Abschnitt 1.

[QUELLE: IEC 61508-4:2010, 3.5.16, ANMERKUNG modifiziert]

3.1.44

Teilsystem

Einheit, die aus der Zerlegung eines SRP/CS auf erster Ebene resultiert und deren gefahrbringender Ausfall zu einem gefahrbringenden Ausfall einer Sicherheitsfunktion führt

Anmerkung 1 zum Begriff: Die Spezifikation des Teilsystems enthält dessen Rolle innerhalb der Sicherheitsfunktion und dessen Schnittstelle mit anderen Teilsystemen des SRP/CS.

Anmerkung 2 zum Begriff: Ein einziges Teilsystem kann Bestandteil von einem oder von mehreren SRP/CS sein, z. B. kann dieselbe Kombination von Schützen verwendet werden, um einen Motor abzuschalten, wenn eine Person in einem Gefahrenbereich erkannt wird, und auch wenn eine Schutzeinrichtung geöffnet wird.

3.1.45

Teilsystemelement

Bestandteil eines Teilsystems, der aus einem einzigen Bauteil oder einer Baugruppe besteht, und der nicht nur eine Sicherheitsfunktion ausführen kann

Anmerkung 1 zum Begriff: Ein Teilsystemelement kann Hardware und Software umfassen, z. B. Sensor, Schütz.

3.1.46

bewährte Sicherheitsprinzipien

Prinzipien, die sich in der Vergangenheit bei der Gestaltung oder Integration von sicherheitsbezogenen Steuerungen als wirkungsvoll erwiesen haben, und so kritische Fehler oder Ausfälle, welche die Leistung einer Sicherheitsfunktion beeinflussen können, vermeiden oder steuern

Anmerkung 1 zum Begriff: Neu entwickelte Sicherheitsprinzipien können nur dann als gleichwertig mit den „bewährten Sicherheitsprinzipien“ angesehen werden, wenn sie anhand von Grundsätzen überprüft werden, die ihre Eignung und Zuverlässigkeit für sicherheitsbezogene Anwendungen belegen.

Anmerkung 2 zum Begriff: Bewährte Sicherheitsprinzipien sind nicht nur gegen zufällige Hardwareausfälle wirksam, sondern auch gegen systematische Ausfälle, die sich irgendwann im Verlauf des Produktlebenszyklus in das Produkt einschleichen können, z. Fehler, die während des Entwurfs, der Integration, der Modifikation oder der Verschlechterung des Produkts auftreten.

Anmerkung 3 zum Begriff: Tabelle A.2, Tabelle B.2, Tabelle C.2 und Tabelle D.2 in den informativen Anhängen von ISO 13849-2 behandeln bewährte Sicherheitsprinzipien für verschiedene Technologien.

3.1.47

bewährtes Bauteil

Bauteil, dessen erfolgreicher Einsatz in vorherigen sicherheitsbezogenen Anwendungen nachgewiesen wurde

Anmerkung 1 zum Begriff: Siehe 6.1.11 für Anforderungen und ISO 13849-2 für eine Liste anerkannter bewährter Bauteile.

3.1.48

Betriebsart

Betriebsweise einer Maschine (d. h. Automatikbetrieb, manueller Betrieb, Instandhaltungsbetrieb), in der vordefinierte Maschinenfunktionen und Sicherheitsmaßnahmen in Verbindung mit diesen Funktionen ausgewählt sind

Anmerkung 1 zum Begriff: Für jede spezifische Betriebsart werden die maßgebenden Sicherheitsfunktionen und/oder Schutzmaßnahmen ausgeführt.

Anmerkung 2 zum Begriff: Die Betriebsart ist keine Maschinenfunktion an sich. Die unter dem Begriff einer Betriebsart zusammengefassten Funktionen (einschließlich der Sicherheitsfunktionen) können nur dann ausgeführt werden, wenn die jeweilige Betriebsart aktiviert worden ist.

3.1.49

dynamischer Test

Diagnosemaßnahme, welche regelmäßig einen Signalwechsel zu Testzwecken durchführt, der überwacht wird

Anmerkung 1 zum Begriff: Der Test ist nicht bestanden, wenn der Signalwechsel nicht wie erwartet bei der Überwachung erkannt wird.

Anmerkung 2 zum Begriff: Beim dynamischen Testen werden üblicherweise Testimpulse verwendet, um Kurzschlüsse oder Unterbrechungen in Signalpfaden zu erkennen oder um Fehlfunktionen aufzudecken. Zum Erkennen von Kurzschlüssen ist eine Zeitverzögerung zwischen den Testimpulsen notwendig, z. B. mit unterschiedlichen Frequenzen.

3.1.50

Plausibilitätsprüfung

Diagnosemaßnahme, die überwacht, ob der Status eines Eingangs (Ausgangs) zu dem Status des Systems oder anderer Eingänge (Ausgänge) passt

3.1.51

Sicherheits-Teilfunktion

Teil einer Sicherheitsfunktion, dessen Ausfall zu einem Ausfall der Sicherheitsfunktion führen kann

Anmerkung 1 zum Begriff: Eine Sicherheits-Teilfunktion ist eine Funktion, die von einem Teilsystem des SRP/CS auszuführen ist.

BEISPIEL Sicherheits-Teilfunktionen nach EN 61800-5-2 sind zum Beispiel sicher abgeschaltetes Drehmoment (STO, en: safe torque off) und sicherer Stopp 1 (SS1).

3.1.52

Kanal

Element oder Gruppe von Elementen, das bzw. die eine Sicherheitsfunktion oder einen Teil davon unabhängig ausführt

[QUELLE: IEC 61508-4:2010, 3.3.6]

3.1.53

Verifizierung

Bestätigung durch Bereitstellung eines objektiven Nachweises, dass festgelegte Anforderungen erfüllt worden sind

Anmerkung 1 zum Begriff: Der für eine Verifizierung erforderliche objektive Nachweis kann das Ergebnis einer Prüfung oder anderer Formen der Bestimmung sein, z. B. Durchführen alternativer Berechnungen oder Überprüfen von Dokumenten.

Anmerkung 2 zum Begriff: Die für die Verifizierung ausgeführten Tätigkeiten werden manchmal als Qualifizierungsprozess bezeichnet.

Anmerkung 3 zum Begriff: Die Benennung „verifiziert“ wird zur Bezeichnung des entsprechenden Status verwendet.

[QUELLE: ISO 9000:2015, 3.8.12, modifiziert, „vom SRP/CS“ wurde hinzugefügt]

3.1.54

Validierung

Bestätigung durch Bereitstellung eines objektiven Nachweises, dass die Anforderungen für einen spezifischen beabsichtigten Gebrauch oder eine spezifische beabsichtigte Anwendung vom SRP/CS erfüllt worden sind

Anmerkung 1 zum Begriff: Der für eine Validierung erforderliche objektive Nachweis ist das Ergebnis eines Tests oder einer anderen Form der Bestimmung, z. B. Durchführen alternativer Berechnungen oder Überprüfen von Dokumenten.

Anmerkung 2 zum Begriff: Die Benennung „validiert“ wird zur Bezeichnung des entsprechenden Status verwendet.

Anmerkung 3 zum Begriff: Die Anwendungsbedingungen für die Validierung können echt oder simuliert sein.

[QUELLE: ISO 9000:2015, 3.8.13, modifiziert, „vom SRP/CS“ wurde hinzugefügt]

3.1.55

permanenter Fehlzustand

Fehlzustand einer Einheit, der solange besteht, bis eine Instandsetzung ausgeführt worden ist

[QUELLE: IEC 60050-192:2015]

3.1.56

Fachkraft

Person, die aufgrund ihrer Weiterbildung, ihrer Ausbildung und ihrer Erfahrung befähigt ist, Risiken zu erkennen und Gefährdungen im Zusammenhang mit der jeweiligen Ausrüstung zu vermeiden

Anmerkung 1 zum Begriff: Bei der Beurteilung der Fachausbildung darf eine mehrjährige Praxis in dem jeweiligen Fachbereich berücksichtigt werden.

[QUELLE: ISO 14990-1:2016, 3.5.4, modifiziert, „Elektrizität“ wurde durch „der jeweiligen Ausrüstung“ ersetzt]

3.2 Symbole und Abkürzungen

Tabelle 1 enthält einen Überblick über die verwendeten Abkürzungen und Symbole.

Tabelle 1 — Symbole und Abkürzungen

Symbol oder Abkürzung	Beschreibung	Definition oder Fundort
a, b, c, d, e	Bezeichnung für die Performance Level	Tabelle K.1
AOPD	aktive optoelektronische Schutzeinrichtung (z. B. Lichtschranke)	Anhang H
B, 1, 2, 3, 4	Bezeichnung für die Kategorien	Tabelle 4
B_{10D}	Anzahl der Zyklen bis 10 % der Komponenten gefahrbringend ausgefallen sind (für Komponenten mit mechanischem Verschleiß)	Anhang C
Kat.	Kategorie	3.1.3
CC	Stromrichter	Anhang I
CCF	Ausfall infolge gemeinsamer Ursache	3.1.8
DC	Diagnosedeckungsgrad	3.1.31
DC_{avg}	durchschnittlicher Diagnosedeckungsgrad	E.2
EMI	elektromagnetische Störung	6.2.2
ETA	Ereignisbaumanalyse	10.3.2
F, F1, F2	Häufigkeit und/oder Dauer der Gefährdungsexposition	A.2.2

Symbol oder Abkürzung	Beschreibung	Definition oder Fundort
FB	Funktionsblock	Anhang J
FVL	Programmiersprache mit nicht eingeschränktem Sprachumfang	3.1.40
FMEA	Fehlzustandsart- und -auswirkungsanalyse	6.1.5
FMECA	Ausfalleffekt- und Kritizitätsanalyse	10.3.2
FTA	Fehlerbaumanalyse	10.3.2
F(t)	kumulative Verteilungsfunktion	C.4.3
HFT	Hardware-Fehlertoleranz	6.1
I, I1, I2	Eingabegerät, z. B. Sensor	6.1
i, j	Index für Zählung	Anhang D
I/O	Eingänge/Ausgänge	Tabelle E.1 und Tabelle E.2
i_m	Verbindungsmittel	Bild 7, Bild 8, Bild 9, Bild 10
K1A, K1B	Schütze	Anhang I
L, L1, L2	Logik	6.1
LVL	Programmiersprache mit eingeschränktem Sprachumfang	3.1.38
λ_D	gefährbringende Ausfälle eines Bauteils	Anhang C
M	Motor	Anhang I
MTTF	mittlere Zeit bis zum Ausfall	Anhang C
MTTF _D	mittlere Zeit bis zum gefährbringenden Ausfall	3.1.28
$n, N, \tilde{N}$	Anzahl von Einheiten	6.2, D.1
N_{niedrig}	Anzahl von SRP/CS mit PL _{niedrig} in einer Kombination von SRP/CS	6.2
n_{op}	mittlere Anzahl der jährlichen Betätigungen	Anhang C
O, O1, O2, OTE	Ausgabegerät, z. B. leistungssteuernde Elemente	6.1
P, P1, P2	Möglichkeit zum Vermeiden der Gefährdung	A.2.3
PES	programmierbares elektronisches System	3.1.26
PFH _D	durchschnittliche Wahrscheinlichkeit eines gefährbringenden Ausfalls je Stunde	Tabelle 2 und Tabelle K.1
PL	Performance Level	3.1.27
PLC	speicherprogrammierbare Steuerung	Anhang I
PL _{niedrig}	niedrigster Performance Level eines SRP/CS in einer Kombination von SRP/CS	6.2
PL _r	erforderlicher Performance Level	3.1.27
r_d	Anforderungsrate	3.1.35
r_t	Testrate	3.1.34

Symbol oder Abkürzung	Beschreibung	Definition oder Fundort
RDF	Anteil gefahrbringender Ausfälle	C.4.2
RS	Drehgeber	Anhang I
S, S1, S2	Schwere der Verletzung	A.2.1
SB	Teilsystem	Bild 13, Bild H.1, Bild H.2
SW1A, SW1B, SW2	Positionsschalter	Anhang I
SIL	Sicherheits-Integritätslevel	3.1.38, Abschnitt 5
SRASW	sicherheitsbezogene Anwendungssoftware	3.1.40
SRESW	sicherheitsbezogene Embedded-Software	3.1.41
SRP	sicherheitsbezogenes Teil	Allgemeines
SRP/CS	sicherheitsbezogenes Teil einer Steuerung	3.1.1
SRS	Spezifikation der Sicherheitsanforderungen	3.1.2
TE	Testeinrichtung	6.1
T_M	Gebrauchsdauer	3.1.33
T_{10D}	mittlere Zeit bis 10 % der Bauteile gefährlich ausfallen	Anhang C

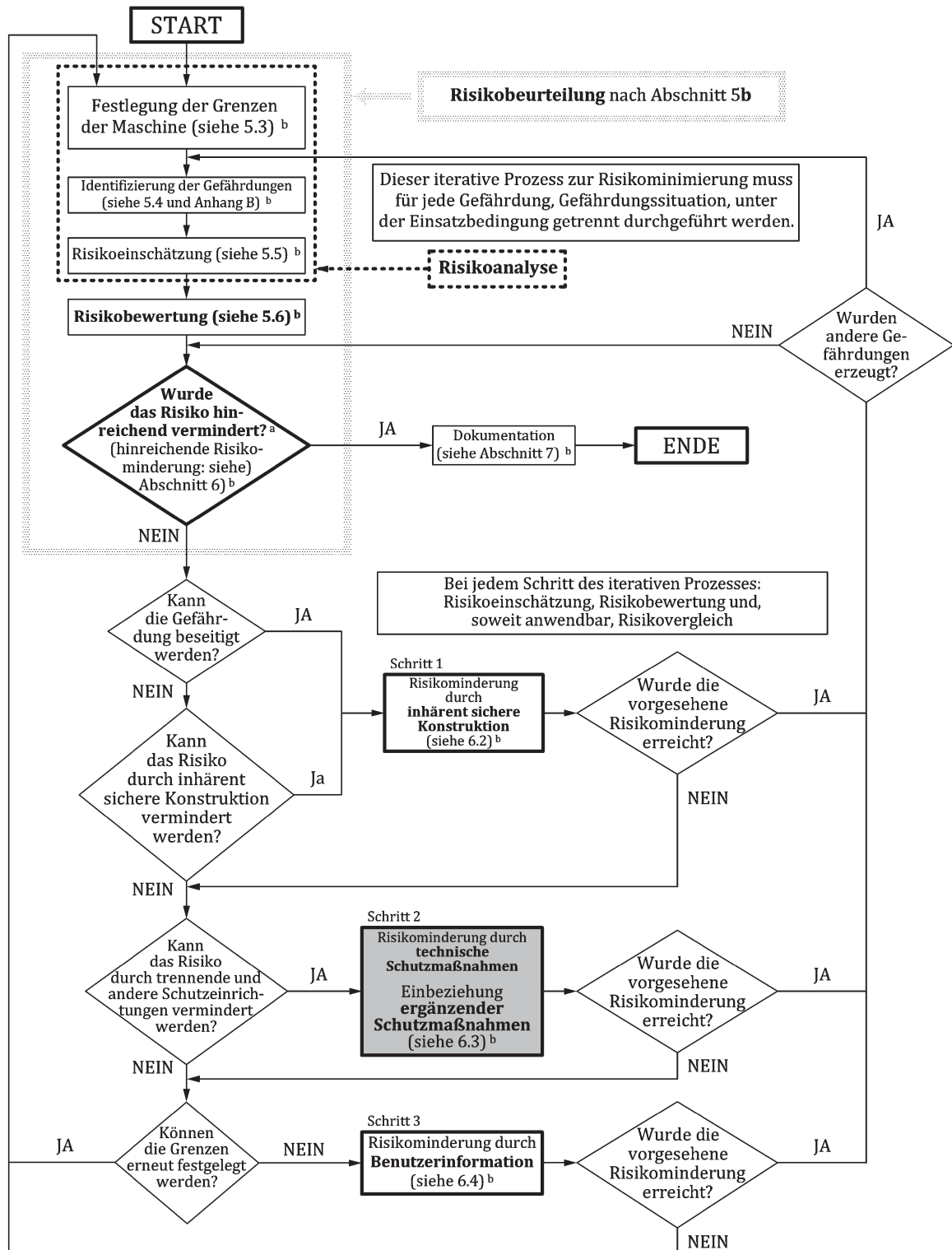
4 Überblick

4.1 Anforderungen an die Risikobeurteilung und Risikominderung

Der Prozess zur Risikobeurteilung wird in ISO 12100 definiert und ist in Bild 1 dargestellt. ISO 13849-1 hat einen festen Platz im Prozess zur Risikobeurteilung und Risikominderung, wenn eine Sicherheitsfunktion und deren zugehörigen Steuerung angewendet werden, um die Risikominderung durchzuführen.

Die Spezifikation der Sicherheitsanforderungen und die Gestaltung der SRP/CS müssen das Ergebnis der Risikobeurteilung berücksichtigen, einschließlich der bestimmungsgemäßen Verwendung und der vernünftigerweise vorhersehbaren Fehlanwendung der Maschine (siehe Bild 1 und Bild 3).

ANMERKUNG Dieses Dokument gilt nicht für Teile der Maschinensteuerung, die nicht sicherheitsbezogen sind (siehe Bild 5).



^a Beim erstmaligen Stellen der Frage, wird diese mit dem Ergebnis der Ausgangsrisikobewertung beantwortet.

^b bezieht sich auf ISO 12100:2010

■ Risikominderung durch technische Schutzmaßnahmen darf durch SRP/CS erfolgen, die Sicherheitsfunktionen ausführen. In diesem Fall gilt ISO 13849, siehe Bild 3.

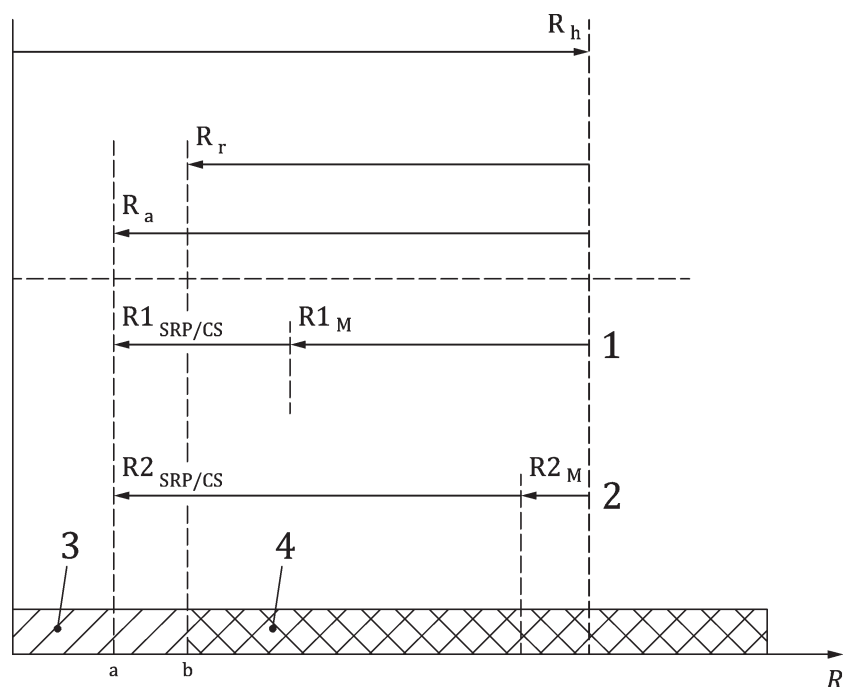
Bild 2 — Schematische Darstellung des Prozesses zur Risikominderung einschließlich des dreistufigen iterativen Prozesses nach ISO 12100:2010

ANMERKUNG In bestimmten Fällen gilt ISO 13849-1 auch für Schritt 3; für Beispiele für Anzeigen und Alarmer siehe Anhang M.

4.2 Beitrag der Sicherheitsfunktion zur Risikominderung

Nach der Risikobeurteilung muss der Konstrukteur entscheiden, welchen Beitrag zur Risikominderung von jeder relevanten Sicherheitsfunktion benötigt wird, die das SRP/CS ausführt. Der Beitrag bezieht sich auf das Risiko, das durch Anwendung jeder bestimmten Sicherheitsfunktion reduziert wird. Er bezieht sich nicht auf das Gesamtrisiko der gesteuerten Maschine.

ANMERKUNG Beispiele für solche Funktionen sind die Stopp-Funktion, die durch eine berührungslos wirkende Schutzvorrichtung an einer Presse ausgelöst wird, oder die Türverriegelungsfunktion an einer Waschmaschine.



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 durch andere Schutzmaßnahmen als durch ein SRP/CS (z. B. mechanische Maßnahmen), ein kleiner Beitrag zur Risikominderung erfolgt durch ein SRP/CS

2 Lösung 2 – Ein wesentlicher Teil der Risikominderung erfolgt durch ein SRP/CS (z. B. Lichtgitter), ein kleiner Beitrag zur Risikominderung erfolgt durch andere Schutzmaßnahmen als durch ein SRP/CS (z. B. mechanische Maßnahmen)

3 angemessene Risikominderung

4 unzureichende Risikominderung

R Risiko

a Restrisiko, das durch Lösung 1 und Lösung 2 verbleibt

b angemessene Risikominderung

$R1_{SRP/CS}$, $R2_{SRP/CS}$ 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 12100:2010.

Bild 3 — Überblick über den Prozess zur Risikominderung für jede Gefährdungssituation

4.3 Risikominderung mithilfe eines SRP/CS

Bild 4 zeigt den Gestaltungsprozess der Sicherheitsfunktionen, die von SRP/CS ausgeführt werden, sowie den Prozess zur Bestimmung, ob die Sicherheitsfunktionen die geplante Risikominderung erzielen.

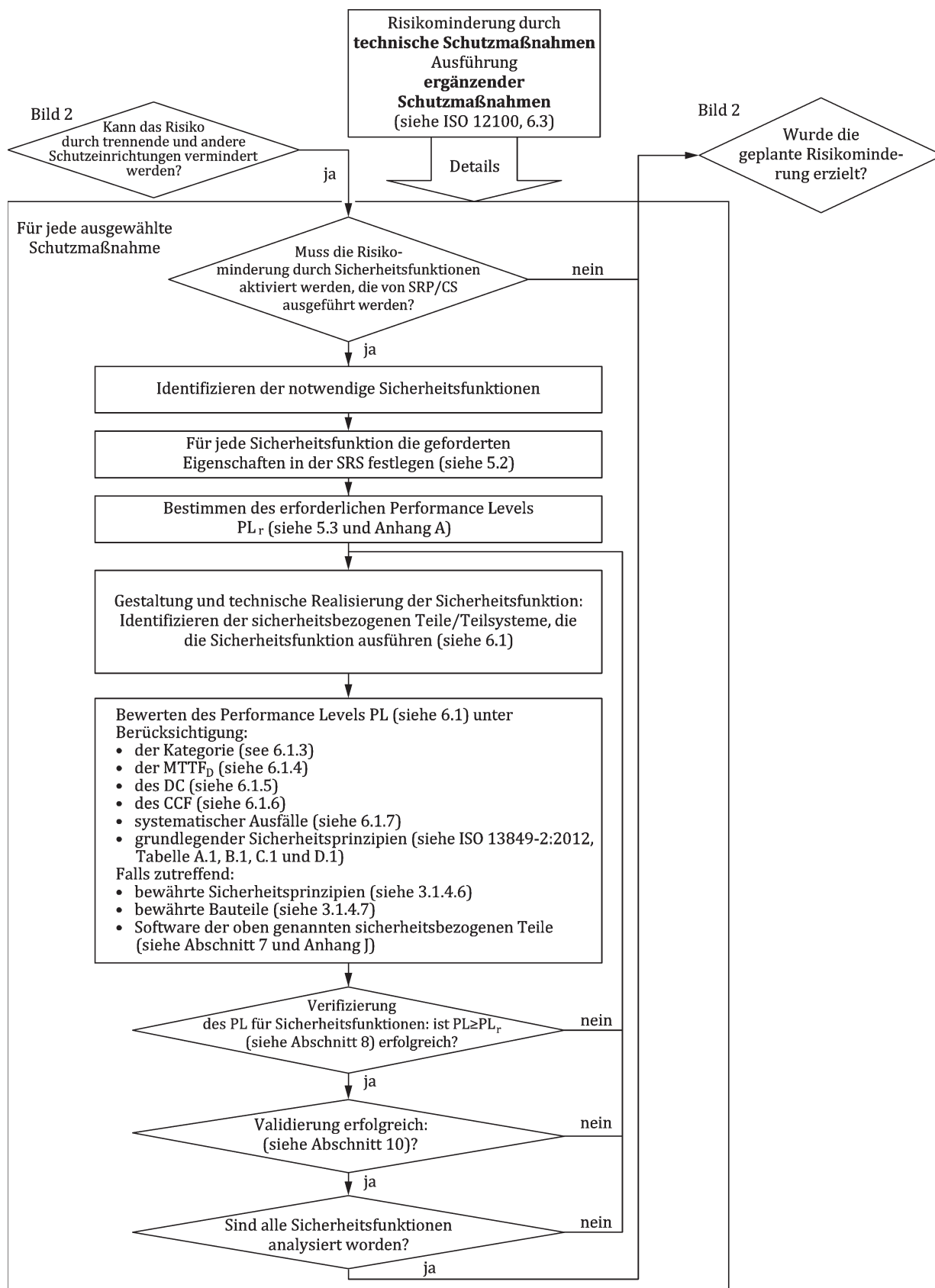


Bild 4 — Iterativer Prozess zur Gestaltung von sicherheitsbezogenen Teilen von Steuerungen (SRP/CS)

4.4 Verfahren

Dieses Dokument beschreibt das folgende Verfahren:

- 1) Festlegen der erforderlichen Eigenschaften für jede Sicherheitsfunktion (5.2);
- 2) Bestimmen eines erforderlichen Performance Levels (PL_r) für jede Sicherheitsfunktion (siehe 5.3);
- 3) Gestalten und technisches Umsetzen der Sicherheitsfunktionen einschließlich der Identifizierung der SRP/CS und deren Teilsysteme, die jede Sicherheitsfunktion ausführen;
 - a) Gestaltungsaspekte (Abschnitt 6),
 - b) Software-Sicherheitsanforderungen (Abschnitt 7);
- 4) Verifizieren, ob der erreichte PL dem PL_r entspricht (Abschnitt 8);
- 5) ergonomische Gestaltungsaspekte (Abschnitt 9);
- 6) Validierung (Abschnitt 10 oder ISO 13849-2);
- 7) Instandhaltung (Abschnitt 11);
- 8) technische Dokumentation (Abschnitt 12);
- 9) Benutzerinformation (Abschnitt 13).

Der erforderliche Performance Level bezieht sich auf die von der Sicherheitsfunktion zu erbringende Risikominderung. Je höher die Risikominderung ist, desto höher muss die erforderliche Sicherheitsleistung sein.

Die Performance Level werden im Hinblick auf die durchschnittliche Wahrscheinlichkeit eines gefahrbringenden Ausfalls der Sicherheitsfunktion je Stunde definiert. Es gibt fünf Performance Level, von der Bereitstellung des PL a mit der geringsten Risikominderung bis hin zum PL e mit der größten Risikominderung. Die definierten Bereiche der Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde sind in Tabelle 2 aufgeführt.

Tabelle 2 — Performance Level (PL)

PL	Durchschnittliche Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde (PFH_D) 1/h
a	$10^{-5} \leq PFH_D < 10^{-4}$
b	$3 \times 10^{-6} \leq PFH_D < 10^{-5}$
c	$10^{-6} \leq PFH_D < 3 \times 10^{-6}$
d	$10^{-7} \leq PFH_D < 10^{-6}$
e	$PFH_D < 10^{-7}$

Teilsysteme müssen nach Abschnitt 5 bis Abschnitt 13 mit demselben Prozess bewertet werden wie die SRP/CS-Systeme.

Für jede Sicherheitsfunktion muss der erreichte Performance Level den erforderlichen Performance Level (PL_r) entweder erreichen oder überschreiten.

4.5 Erforderliche Informationen

Um die Anforderungen dieses Dokuments zu erfüllen, müssen die folgenden Informationen angegeben werden:

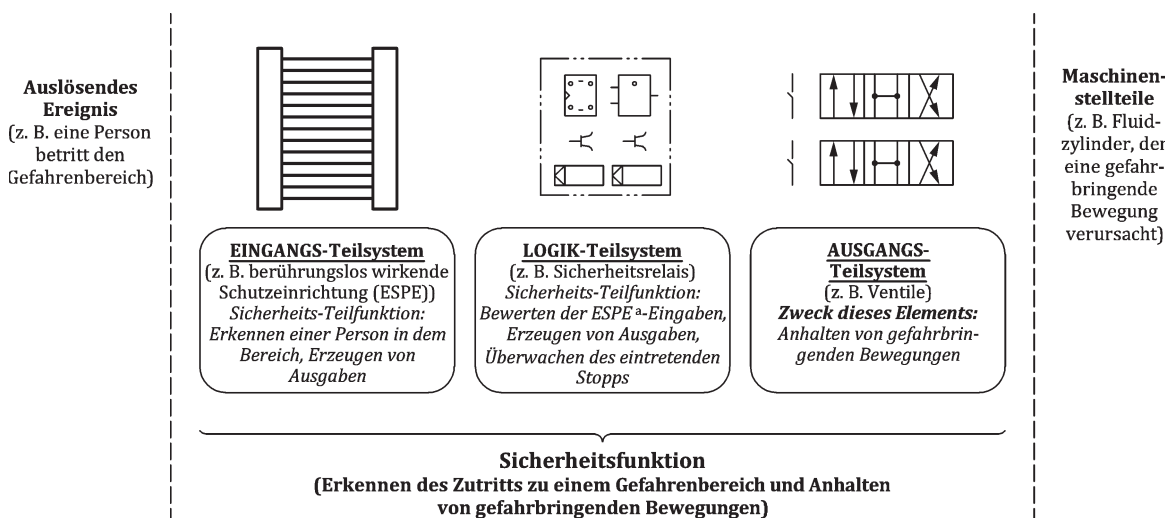
- Ergebnisse der Risikobeurteilung;
- Informationen über alle Sicherheitsfunktionen (siehe Abschnitt 5), die für den Prozess zur Risikominderung für jede Gefährdung als notwendig ermittelt wurde;
- ausführliche Beschreibung jeder Sicherheitsfunktion (siehe 5.2);
- Bestimmung des erforderlichen Performance Levels (PL_r) für jede Sicherheitsfunktion (siehe 5.3).

ANMERKUNG Diese Information kann bereits in den zutreffenden Typ-C-Normen enthalten sein.

4.6 Ausführung von Sicherheitsfunktionen mithilfe von Teilsystemen

Die Ausführung einer Sicherheitsfunktion, mit welcher der erforderliche PL erreicht wird, darf durch die Gestaltung des SRP/CS erfolgen:

- mithilfe von bereits zuvor validierten Teilsystemen nach diesem Dokument oder nach IEC 62061, IEC 61508 oder sonstigen maßgebenden sicherheitsbezogenen Produktnormen (z. B. IEC 61496-1 und IEC 61800-5-2); oder
- Gestaltung neuer Teilsysteme nach diesem Dokument; oder
- durch eine Kombination der beiden vorstehenden Optionen (siehe Beispiel in Bild 5).



Legende

- ^a berührungslos wirkende Schutzeinrichtung (ESPE, en: electrosensitive protective equipment)

Bild 5 — Beispiel für eine Kombination von Teilsystemen

5 Spezifikation der Sicherheitsfunktionen

5.1 Allgemeines

Das Ziel dieses Unterabschnitts ist es, einen Leitfaden darüber bereitzustellen, wie die Anforderungen an jede Sicherheitsfunktion, die von dem SRP/CS auszuführen ist, festgelegt werden sollen.

Ein Teil des Prozesses zur Risikominderung ist es, die Sicherheitsfunktionen der Maschine zu bestimmen, wie z. B. Verhindern des unerwarteten Anlaufs. Eine Sicherheitsfunktion darf durch ein oder mehrere Teilsysteme ausgeführt werden, die zu einem SRP/CS kombiniert sind, und mehrere Sicherheitsfunktionen dürfen ein oder mehrere Teilsysteme gemeinsam nutzen [z. B. eine Logikeinheit, (ein) leistungssteuernde(s) Element(e)].

Die Spezifikation der Sicherheitsfunktion kann nach ISO 12100 erfolgen und einen Teil der Konstruktionsspezifikation für das SRP/CS nach ISO 13849-1 darstellen.

Dieser Unterabschnitt behandelt die folgenden Schritte:

- 1) allgemeine Beschreibung der Sicherheitsfunktion (Verknüpfung der Gefährdungen mit den Sicherheitsfunktionen);
- 2) ausführliche Beschreibung der Sicherheitsanforderungen (siehe 5.2);
- 3) ANMERKUNG Für zusätzliche Anforderungen an bestimmte Sicherheitsfunktionen siehe 5.2.3.
- 4) Bestimmung des PLr für jede Sicherheitsfunktion (d. h. wie zuverlässig die Sicherheitsfunktion sein muss – siehe 5.3);
- 5) Überprüfung der Spezifikation der Sicherheitsanforderungen (siehe 5.4).

Eine Sicherheitsfunktion muss allgemein beschrieben sein, um den Beitrag des SRP/CS zur Risikominderung festzulegen. Die Beschreibung muss auf die Gefährdungen Bezug nehmen, die in der Risikobeurteilung definiert sind, und muss angeben, wie die Funktion bis zum Erreichen der erforderlichen Sicherheit arbeitet. Der Prozess zum Festlegen von Sicherheitsfunktionen erfordert ausführliche Angaben aus der Risikobeurteilung, die in Übereinstimmung mit ISO 12100 durchgeführt wurde.

5.2 Spezifikation der Sicherheitsanforderungen (SRS, en: safety requirements specification)

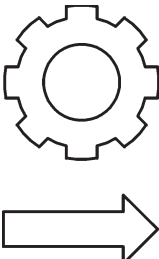
5.2.1 Allgemeine Anforderungen

5.2.1.1 Allgemeines

Die Spezifikation der Sicherheitsanforderungen muss die Details jeder durchzuführenden Sicherheitsfunktion dokumentieren.

ANMERKUNG 1 Die Spezifikation der Sicherheitsanforderungen ist sehr wichtig, um Fehler beim Übergang vom Risikobeurteilungs- und -minderungsprozess nach ISO 12100 zum SRP/CS-Entwurfs- und Bewertungsprozess nach ISO 13849 zu vermeiden, insbesondere wenn diese beiden Prozesse von unterschiedlichen Personen oder Organisationen durchgeführt werden (siehe Tabelle 3).

Tabelle 3 — Übergang vom Risikobeurteilungs- und -minderungsprozess nach ISO 12100 zum SRP/CS-Entwurfs- und Bewertungsprozess nach ISO 13849

Erforderliche Informationen für das Erstellen der SRS (siehe 5.2.1.2)		Festlegung aller Sicherheitsfunktionen in der SRS (siehe 5.2.1.3)
<ul style="list-style-type: none"> — Ergebnisse der Risikobeurteilung, einschließlich gefährlicher Teile — Betriebseigenschaften der Maschine, z. B. bestimmungsgemäße Verwendung — Handlungen im Notfall — Beschreibung der Wechselwirkung verschiedener Arbeitsprozesse und manueller Aktionen, z. B. Instandsetzung — ergonomische Aspekte — Anwendungsgrenzen in Zusammenhang mit den Umgebungsbedingungen 		<p>Erforderliche Sicherheitsfunktionen (Beispiele):</p> <p>1) Verriegelungsfunktion</p> <ul style="list-style-type: none"> — Betriebsart (alle) — Auslösung durch: Öffnen einer beweglichen trennenden Schutzeinrichtung — sicherheitsbezogene Reaktion: sicher abgeschaltetes Drehmoment (STO) aller Bewegungen — PL_r z. B. PL d — Ansprechzeit: z. B. 200 ms — ... <p>2) sicher begrenzte Geschwindigkeit (SLS: en: safely limited speed)</p> <ul style="list-style-type: none"> — Betriebsart (manuelle) — Auslösung durch: Geschwindigkeit, welche die festgelegte Geschwindigkeitsgrenze überschreitet — sicherheitsbezogene Reaktion: sicher abgeschaltetes Drehmoment (STO) aller Bewegungen — PL_r z. B. PL c — Ansprechzeit: z. B. 150 ms — ...

5.2.1.2 Erforderliche Informationen für das Erstellen der SRS

Die folgenden Informationen sollten vom Konstrukteur der sicherheitsbezogenen Steuerung verwendet werden, um die Spezifikation der Sicherheitsanforderungen zu erstellen:

- a) Ergebnisse der Risikobeurteilung für jede spezifische Gefährdung, wobei die dazugehörige(n) risikomindernde(n) Maßnahme(n) auf einer sicherheitsbezogenen Steuerung beruht/beruhen, um so eine Sicherheitsfunktion auszuführen;
- b) Betriebseigenschaften der Maschine, mit
 - 1) der bestimmungsgemäßen Verwendung der Maschine;
 - 6) der vernünftigerweise vorhersehbaren Fehlanwendung;
 - 7) den Betriebsarten (z. B. lokale Betriebsart, Automatikbetrieb, Betrieb mit Bezug zu einem Bereich oder Teil der Maschine);

- 8) der/den Betriebsart(en), während der/denen die Sicherheitsfunktion aktiviert ist sein muss;
- 9) der Zyklusdauer; und
- 10) der Ansprechzeit bis ein sicherer Zustand erreicht ist (siehe auch ISO 13855, 5.1);

ANMERKUNG 1 Die Ansprechzeit der Steuerung ist Teil der Gesamt-Ansprechzeit der Maschine. Die erforderliche Gesamt-Ansprechzeit der Maschine kann die Gestaltung der sicherheitsbezogenen Teile beeinflussen, z. B. die Notwendigkeit, eine Bremse bereitzustellen.

ANMERKUNG 2 Betriebsfunktionen (z. B. Anlaufen, normaler Stopp) können auch Sicherheitsfunktionen sein, aber dies kann erst nach einer vollständigen Risikobeurteilung an der Maschine ermittelt werden.

- c) Handlungen im Notfall (siehe ISO 12100, 3.39 und IEC 60204-1, Anhang E);
- d) Beschreibung der Wechselwirkung verschiedener Arbeitsprozesse und manueller Aktionen (z. B. Instandsetzen, Einrichten, Reinigung, Fehlersuche, Betriebsarten mit deaktivierten Schutzeinrichtungen);
- e) ergonomische Aspekte zum Verhindern einer fehlerhaften Bedienung oder Umgehung;
- f) Anwendungsgrenzen in Zusammenhang mit den Umgebungsbedingungen.

5.2.1.3 Festlegung aller Sicherheitsfunktionen in der SRS

Der Konstrukteur muss die folgenden Informationen einbeziehen, die notwendig sind, um die von der Steuerung auszuführenden Sicherheitsmaßnahmen für die spezielle Anwendung zu verwirklichen:

Kurzbeschreibung/Titel der Sicherheitsfunktion für eine klare Bezugnahme;

- a) das Ereignis, das die Sicherheitsfunktion auslöst;
- b) der erforderliche Performance Level PL_r für jede Sicherheitsfunktion (siehe 5.3);

ANMERKUNG 1 Sofern notwendig, wird die erforderliche Kategorie festgelegt (siehe 6.1.3).

- c) die sicherheitsbezogene Reaktion der Maschine, die durch die Ausgabe(n) der Sicherheitsfunktion herbeigeführt wird;

BEISPIEL 1 Sicherer Halt einer gefahrbringenden Bewegung.

- d) die Ansprechzeit der Maschine zum Erreichen eines sicheren Zustands, nachdem der Befehl im Zuge der Sicherheitsfunktion ausgelöst wurde, z. B. das Gesamt-Anhaltevermögen des Systems (Reaktionszeit plus Anhaltezeit) nach ISO 13855;
- e) die Betriebsart(en), während der/denen die Sicherheitsfunktion aktiviert ist sein muss;
- f) alle Verknüpfungen zwischen den Sicherheitsfunktionen sowie zwischen den Sicherheitsfunktionen und jeder anderen nicht sicherheitsbezogenen Funktion (entweder innerhalb oder außerhalb der Maschine);

BEISPIEL 2 Eine Sicherheitsfunktion darf deaktiviert werden, um den Transport von Materialien in einen Gefahrenbereich hinein oder aus einem Gefahrenbereich heraus zu ermöglichen.

- g) sofern notwendig, alternative Reaktionen, um die Maschine im Fall eines Fehlers in einem Funktionskanal in einen sicheren Zustand zu überführen, einschließlich der Beschreibung, wie der sichere Zustand beibehalten wird, bis der Fehler behoben ist;

BEISPIEL 3 Die Hydraulikpumpe darf ausgeschaltet werden, um die Bewegung eines Zylinders anzuhalten, falls ein Fehler in einem Ventil erkannt wurde.

- h) das Verhalten der Maschine bei Energieverlust (siehe auch 5.2.3.7);

ANMERKUNG 2 In einigen Fällen kann es notwendig sein, das Verhalten der Maschine bei Energieverlust zu berücksichtigen, wenn es beispielsweise notwendig ist, eine vertikale Achse beizubehalten, um ein Absinken durch Schwerkraft zu verhindern. Das kann zwei getrennte Sicherheitsfunktionen erfordern: mit Energie verfügbar und ohne Energie verfügbar. Ein Not-Halt muss jederzeit verfügbar sein und muss alle anderen Funktionen übersteuern.

- i) die Anforderungsrate oder Betriebshäufigkeit;
- j) die Priorität der Sicherheitsfunktionen, die gleichzeitig aktiv sein können und dadurch zu Konflikten führen können.

BEISPIEL 4 Ein Not-Halt hat Vorrang vor allen anderen Funktionen.

BEISPIEL 5 Die Sicherheitsfunktion „sicher begrenzte Geschwindigkeit“ (siehe IEC 61800-5-2, 4.2.3.4) kann eine Voraussetzung für eine Sicherheitsfunktion „selbsttätige Rückstellung“ sein.

Oben gemachte Angaben sind eine nicht vollständige Liste von Einzelheiten für Sicherheitsfunktionen, die durch das SRP/CS bereitgestellt werden können.

Wenn in Typ-C-Normen oder in anderen maßgebenden Normen Sicherheitsanforderungen an die Gestaltung eines SRP/CS oder eines Teilsystems festgelegt sind (z. B. ISO 23125, ISO 13851), sollten sie berücksichtigt werden.

Für Betriebsfunktionen, die sowohl betriebliche Funktionen als auch Sicherheitsfunktionen ausführen können, sollte der Konstrukteur bzw. sollten die Normungsgremien, die Typ-C-Normen erarbeiten, die ausgeführte Sicherheitsfunktion sowie den PL_r angeben, der der jeweiligen Sicherheitsfunktion zugeteilt ist.

Siehe auch Anhang M.

5.2.2 Zerlegung eines SRP/CS in Teilsysteme

Die Sicherheitsfunktionen müssen in Teilfunktionen zerlegt werden, die den jeweiligen Teilsystemen zugeordnet werden. Die Beschreibung jeder Teilfunktion muss Folgendes enthalten:

- die Sicherheitsanforderungen an jede Teilfunktion (Anforderungen an Funktion und Integrität); und
- Eingänge und Ausgänge jeder Teilfunktion.

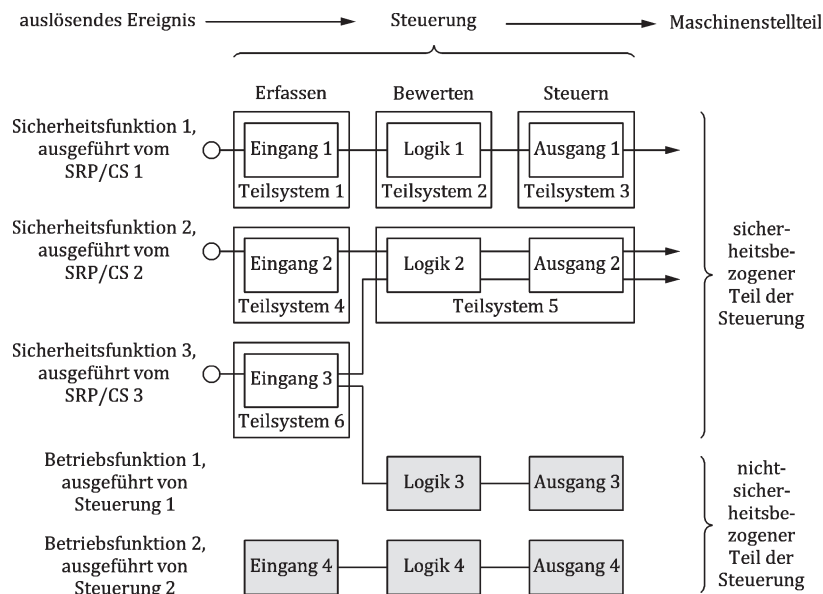
Ein SRP/CS kann Folgendes umfassen:

- ein oder mehrere zuvor validierte(s) Teilsystem(e);
- ein oder mehrere Teilsystem(e) basierend auf (einem) Teilsystemelement(en).

Ein gefahrbringender Ausfall (3.1.7) eines beliebigen Teilsystems (3.1.44) kann per Definition zum Verlust der gesamten Sicherheitsfunktion führen.

ANMERKUNG 1 Ein SRP/CS kann als ein einziges Teilsystem mit einem Sensor, Logikeinheiten und leistungssteuernden Elementen definiert werden. Ein Beispiel für die Ausführung eines SRP/CS aus einem einzigen Teilsystem ist eine „intelligente“ Sensoreinheit (z. B. Lichtvorhang, Laserscanner) mit integrierter Ausgangsschaltanordnung (z. B. Relais zum Ausschalten eines Laserstrahls).

BEISPIEL Bild 6 zeigt ein Beispiel für die Zerlegung; sie beginnt beim Erkennen und Bewerten eines ‚auslösenden Ereignisses‘ (z. B. manuelles Betätigen eines Drucktasters, Öffnen einer trennenden Schutzeinrichtung, Unterbrechen eines Strahls der AOPD) und endet mit einem Ausgang, der eine Reaktion eines Maschinenstellteils bewirkt (z. B. Motor, Zylinder).



Legende

- Sicherheitsfunktion 1 wird in Teilfunktion 1, Teilfunktion 2 und Teilfunktion 3 zerlegt. Teilfunktion 1 wird von Teilsystem 1 ausgeführt usw.
- Sicherheitsfunktion 2 wird in Teilfunktion 4 und Teilfunktion 5 zerlegt. Teilfunktion 4 wird von Teilsystem 4 ausgeführt usw.
- Sicherheitsfunktion 3 wird in Teilfunktion 6 und Teilfunktion 5 zerlegt. Teilfunktion 6 wird von Teilsystem 6 ausgeführt usw.

Bild 6 — Beispiel für die Zerlegung einer Sicherheitsfunktion und ihre Aufteilung in Teilsysteme

Bild 6 zeigt eine schematische Darstellung von Teilsystemen, die zu (einem) SRP/CS kombiniert sind, mit:

- Eingang (z. B. Endschalter, Sensor, AOPD) (Teilsysteme 1, 4 und 6);
- Logik/Verarbeitung (Teilsysteme 2 und 5);
- Ausgang/leistungssteuernde Elemente (z. B. Ventil, Schütz, Stromrichter) (Teilsysteme 3 und 5); und
- Verbindungen (z. B. elektrisch, optisch).

Die Zerlegung eines SRP/CS in Teilsysteme nach Bild 6 ist typisch, aber das gesamte SRP/CS darf auch durch ein einziges Teilsystem oder durch mehr als drei Teilsysteme verwirklicht werden.

ANMERKUNG 2 Es ist aber auch möglich, dass ein Teilsystem oder ein SRP/CS Sicherheitsfunktionen und normale Steuerungsfunktionen ausführt. 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 zur Auslösung eines Zyklus).

ANMERKUNG 3 Der Konstrukteur eines zuvor validierten Teilsystems kann ein Maschinenhersteller oder ein Bauteilhersteller sein.

ANMERKUNG 4 Bei Verwendung eines zuvor validierten Teilsystems stellt der Hersteller dieses Teilsystems die relevanten Informationen bereit, siehe 13.2.

5.2.3 Anforderungen an spezifische Sicherheitsfunktionen

5.2.3.1 Sicherheitsbezogene Stopp-Funktion

Eine sicherheitsbezogene Stopp-Funktion (z. B. eingeleitet durch eine Schutzeinrichtung) muss so schnell wie notwendig nach ihrer Auslösung die Maschine in den sicheren Zustand bringen. Solch eine sicherheitsbezogene Stopp-Funktion hat Vorrang vor allen Startfunktionen und nicht sicherheitsbezogenen Stopp-Funktionen.

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

Als Ergebnis der Risikobeurteilung können Stopp-Funktionen entsprechend den Stopp-Kategorien von IEC 60204-1, 9.2.2, und/oder entsprechend einem sicher abgeschalteten Drehmoment (STO), einem sicheren Stopp 1 (SS1), einem sicheren Stopp 2 (SS2), einem sicheren Betriebshalt (SOS, en: safe operating stop) (IEC 61800-5-2, 4.2.4) ausgeführt werden.

Nach der Einleitung eines Stopp-Befehls durch eine sicherheitsbezogene Funktion muss der Stopp-Zustand aufrechterhalten bleiben, bis ein sicherer Zustand für einen Wiederanlauf gegeben ist. Siehe auch Tabelle M.1 in Anhang M.

5.2.3.2 Manuelle Rückstellfunktion

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

Die manuelle Rückstellfunktion

- muss durch ein getrenntes, manuell zu bedienendes Gerät, das vom Start-Befehl getrennt ist, in dem SRP/CS bereitgestellt werden,
- darf nur dann erreicht werden, wenn alle davon beeinflussten Sicherheitsfunktionen und Schutzeinrichtungen funktionsfähig sind,
- darf selbst keine Gefährdungssituation einleiten,
- muss eine beabsichtigte Handlung sein,
- muss der Steuerung ermöglichen, einen separaten Start-Befehl anzunehmen,
- muss durch Signalwechsel angenommen werden.

Die Teile, welche die manuelle Rückstellfunktion bereitstellen, müssen so ausgewählt werden, dass sie die von der zugehörigen Sicherheitsfunktion erforderliche Sicherheit nicht mindern.

Wenn die Funktion „manuelle Rückstellung“ als Sicherheitsfunktion ausgeführt sein muss (z. B. Verhindern eines unerwarteten Anlaufs), ist der erforderliche Performance Level zu bestimmen.

ANMERKUNG 1 Es ist nicht immer notwendig, dass die manuelle Rückstellungsfunktion denselben PL_r wie die zugehörige Sicherheitsfunktion besitzt.

Das Stellteil zum Rücksetzen muss außerhalb des Gefahrenbereichs und an einer Stelle mit guter Einsicht angebracht werden, von der aus sichergestellt werden kann, dass sich keine Person im Gefahrenbereich befindet. Es darf nicht möglich sein, die Rückstellungsfunktion von einer Stelle innerhalb des Gefahrenbereichs zu aktivieren.

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

ANMERKUNG 2 Eine Lösung ist die Verwendung von nacheinander durchgeführtem Rücksetzen. Die Rückstellfunktion wird innerhalb des Gefahrenbereichs durch das erste Stellteil in Kombination mit einem zweiten Stellteil zum Rücksetzen außerhalb des Gefahrenbereichs (nahe der Schutzeinrichtung) eingeleitet. Dieses Rückstellverfahren muss innerhalb einer begrenzten Zeit erfolgen, bevor die Steuerung einen separaten Startbefehl akzeptiert.

Siehe auch Tabelle M.1 in Anhang M.

5.2.3.3 Wiederanlauffunktion

Ein Wiederanlauf darf nur dann automatisch erfolgen, wenn keine Gefährdungssituation bestehen kann. Insbesondere trifft ISO 12100:2010, 6.3.3.2.5, bei einer verriegelten trennenden Schutzeinrichtung mit Startfunktion zu.

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

BEISPIEL Während des Automatikbetriebs einer Maschine wird die Rückmeldung eines Sensorsignals an die Steuerung häufig zur Steuerung des Prozessablaufs verwendet. Wenn ein Werkstück seine Position verlässt, wird der Prozessablauf gestoppt. Wenn die Überwachung der verriegelten trennenden Schutzeinrichtung keinen Vorrang vor der automatischen Steuerung hat, könnte eine Gefahr bestehen, dass die Maschine unerwartet wieder anläuft, wenn die Bedienerperson der Maschine die Lage des Werkstücks korrigiert. Deshalb sollte der automatische Wiederanlauf nicht erlaubt werden, bis die trennende Schutzeinrichtung wieder geschlossen ist und der Bediener den Gefahrenbereich verlassen hat. Der Beitrag zur Verhinderung eines unerwarteten Anlaufs (siehe ISO 14118) durch die Steuerung hängt vom Ergebnis der Risikobeurteilung ab.

Siehe auch Tabelle M.1 in Anhang M.

5.2.3.4 Lokale Steuerungsfunktion

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

- die Mittel zur Anwahl der lokalen Steuerung müssen außerhalb des Gefahrenbereichs angebracht sein;
- das Erteilen eines Befehls durch eine lokale Steuerung darf nur in einem Bereich möglich sein, der durch die Risikobeurteilung definiert wurde, um Gefährdungssituationen zu vermeiden;
- die Umschaltung zwischen lokaler Steuerung und einer anderen Steuerung darf keine Gefährdungssituationen erzeugen;
- die Steuerung muss so ausgelegt sein, dass das Auslösen von Befehlen von anderen Steuerungen aus nicht zu einer Gefährdungssituation führt. Es kann notwendig sein, die Verwendung anderer Steuerungen zu verhindern, wenn die lokale Steuerung betätigt wird.

Siehe auch Tabelle M.1 in Anhang M.

5.2.3.5 Mutingfunktion

Muting ist ein vorübergehendes automatisches Deaktivieren einer Sicherheitsfunktion durch die sicherheitsbezogene Steuerung einer Maschine. Es kann angewendet werden, um den Zutritt von Personen oder die Beförderung von Materialien zu ermöglichen:

- während eines ungefährlichen Abschnitts des Maschinenzyklus; oder
- wenn die Sicherheit durch andere Maßnahmen aufrechterhalten wird.

Die Mutingfunktion muss automatisch ausgelöst und beendet werden. Dies muss durch die Anwendung von angemessen ausgewählten und angeordneten Sensoren oder durch Signale der Maschinensteuerung erfolgen. Fehlerhafte Signale, Reihenfolgen oder Zeitvorgaben der Mutingsensoren oder -signale dürfen keinen Mutingzustand bewirken.

Der Teil bzw. die Teile der Steuerung, der/die die Mutingfunktion ausführt/ausführen, muss/müssen eine angemessene sicherheitsbezogene Leistung aufweisen (SIL oder PL, siehe IEC 62061 oder ISO 13849-1) und darf/dürfen die sicherheitsbezogene Leistung der Schutzfunktion nicht unter die für die jeweilige Anwendung geforderte verringern.

Nach dem Muting müssen alle davon beeinflussten Sicherheitsfunktionen des SRP/CS wiederhergestellt werden.

Der Performance Level der sicherheitsbezogenen Teile, die die Mutingfunktion ausführen, muss so ausgewählt werden, dass die Aufnahme der Mutingfunktion die von der entsprechenden Sicherheitsfunktion geforderte Sicherheit nicht verringert.

Die Umsetzung der Mutingfunktion muss den Anforderungen von IEC 62046 entsprechen. Siehe auch Tabelle M.1 in Anhang M.

5.2.3.6 Sicherheitsbezogene Parameter

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

Wenn Abweichungen in manuell eingegebenen sicherheitsbezogenen Daten für programmierbare oder konfigurierbare elektronische Systeme zu Gefährdungssituationen führen können, sollte in der sicherheitsbezogenen Steuerung ein Datentest bereitgestellt werden, z. B. Test bezüglich Grenzwerten, Format und/oder Logik der Eingangswerte. Für ergänzende Anforderungen siehe 7.4.

In Produktnormen und Typ-C-Normen können Anforderungen an einen Datentest für einige oder alle manuellen Parameter enthalten sein. Siehe maßgebende Normen.

Siehe auch Tabelle M.2 in Anhang M.

5.2.3.7 Schwankungen, Verlust und Wiederkehr der Spannungsversorgung

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

Siehe auch Tabelle M.2 in Anhang M.

5.2.3.8 Anforderungen an die Betriebsartenwahl

Es gelten die folgenden Anforderungen:

- a) es darf nur eine Betriebsart nach der anderen aktiviert werden; jede gewählte Betriebsart muss deutlich erkennbar sein bzw. angezeigt werden;
- b) durch die Betriebsartenwahl selbst darf keine Maschinenbewegung ausgelöst werden. Hierzu muss eine separate Betätigung der Anlaufsteuerung erforderlich sein;
- c) beim Wechsel zwischen Betriebsarten müssen Sicherheitsfunktionen und/oder risikomindernde Maßnahmen, die für die gewählte Betriebsart notwendig sind, aktiviert werden, ohne dabei während des Wechsels den Schutz zu verlieren.

ANMERKUNG Andere Sicherheitsfunktionen und/oder risikomindernde Maßnahmen, die entsprechend der Risikobeurteilung für die gewählte Betriebsart nicht notwendig sind, können deaktiviert werden.

Die Sicherheitsfunktion(en) muss/müssen den erforderlichen PL entsprechend der Risikobeurteilung für die Betriebsartenwahl aufweisen.

BEISPIEL Zum Arbeiten bei geöffneten Schutzeinrichtungen im Einrichtbetrieb wird die Sicherheitsfunktion der Verriegelung deaktiviert und gleichzeitig werden die Sicherheitsfunktionen der Zustimmungsfunktion und die sicher begrenzte Geschwindigkeit (SLS) aktiviert. Es kann ein Risiko entstehen, wenn nicht alle relevanten Sicherheitsfunktionen aktiviert sind.

5.2.3.9 Instandhaltungsaspekte von Sicherheitsfunktionen

Bei der Gestaltung der Maschine müssen die Instandhaltungsaufgaben berücksichtigt werden, die an der Maschine durchgeführt werden, und es müssen Sicherheitsfunktionen vorgesehen werden, um diese Instandhaltungsaufgaben mit einem annehmbaren Risiko auszuführen.

ANMERKUNG 1 Zu den Instandhaltungsaufgaben können unter anderem folgende gehören:

- Einrichten;
- Einlernen (Teachen)/Programmieren;
- Umrüsten;
- Reinigung und Sauberhaltung;
- geplante oder ungeplante vorbeugende oder Fehler behebende Instandhaltung;
- Fehlersuche/Fehlerfindung;
- Fehlerdiagnose.

Einige Instandhaltungsaufgaben erfordern eine vollständige Trennung der Maschine von allen Energiequellen und stützen sich daher nicht auf das SRP/CS. Für andere Instandhaltungsaufgaben (z. B. Einlernen oder Fehlersuche) könnte es sein, dass Maschinenbewegungen ermöglicht werden müssen, während sich das Instandhaltungspersonal im Gefahrenbereich aufhält. Insbesondere bei der Gestaltung des SRP/CS müssen die Instandhaltungsaufgaben berücksichtigt werden, da bestimmte Sicherheitsfunktionen ein manuelles Deaktivieren oder Übersteuern erfordern. Soweit notwendig, muss die Gestaltung des SRP/CS das manuelle Deaktivieren oder Übersteuern mit einem annehmbaren Risiko erlauben, indem eine alternative Sicherheitsfunktion (z. B. Zustimmungsfunktionen und Geschwindigkeitsbegrenzungsfunktion) zur Verfügung gestellt wird.

Weitere Sicherheitsfunktionen in Zusammenhang mit der Instandhaltung können beispielsweise folgende sein:

- Einrichtung mit selbsttätiger Rückstellung;
- Zustimmungsfunktion;
- Überwachung oder Begrenzung der Geschwindigkeit, des Drehmoments, der Leistung, der Position;
- Verhindern des unerwarteten Anlaufs;
- Energietrennungs- und -ableitungsfunktion.

ANMERKUNG 1 Siehe Anhang M für ergänzende Informationen.

ANMERKUNG 2 Aktuelle Sicherheitsstudien belegen, dass viele Verletzungen darauf zurückzuführen sind, dass das SRP/CS übergangen oder umgangen wurde. Deshalb sollten die Instandhaltungsaspekte bei der Gestaltung des SRP/CS genau berücksichtigt werden.

Der Anreiz zum Übergehen bzw. Umgehen von risikomindernden Maßnahmen, die vom SRP/CS während der Instandhaltung der Maschine ausgeführt werden, muss bei der Gestaltung und Auswahl des SRP/CS betrachtet werden.

ANMERKUNG 3 Der Anreiz oder die Notwendigkeit, das SRP/CS zu übergehen bzw. zu umgehen, hängt sowohl von den vorherrschenden Umständen ab als auch von den Gestaltungsdetails der risikomindernden Maßnahme(n). Anreize zum Übergehen oder Umgehen einer risikomindernden Maßnahme können unter anderem die folgenden Faktoren umfassen:

- a) die risikomindernde Maßnahme verhindert, dass die Aufgabe durchgeführt wird;
- b) es besteht die Notwendigkeit, eine Aufgabe durchzuführen, deren Gefährdungen und Risiken nicht ermittelt und beurteilt worden sind;
- c) die risikomindernde Maßnahme verlangsamt die Produktion oder stört andere Aktivitäten oder Präferenzen des Benutzers;
- d) die risikomindernde Maßnahme ist schwierig anzuwenden;
- e) andere Personen als der/die vorgesehene(n) Bediener führen die Aufgabe aus, z. B.:
 - a) der Bediener führt Rückstell- und Wiederanlauffunktionen aus, während sich das Instandhaltungspersonal im Gefahrenbereich aufhält;
 - b) risikomindernde Maßnahmen, durch die eine Person geschützt werden soll, werden unangemessen für mehrere Personen eingesetzt;
 - f) die risikomindernde Maßnahme und/oder deren zugehörige Gefährdung wird/werden vom Personal nicht als solche erkannt;
 - g) die risikomindernde Maßnahme wird nicht als geeignet, notwendig oder angemessen für ihre Funktion angesehen.

ANMERKUNG 4 Die Verwendung von speicherprogrammierbaren Systemen bietet eine weitere Möglichkeit, um Bestimmungen für den Zugriff auf speicherprogrammierbare Systeme zu übergehen oder zu umgehen, wenn diese nicht ordnungsgemäß angewendet oder überwacht werden. Dies ist insbesondere dann von Bedeutung, wenn ein Fernzugang zu diagnostischen Zwecken oder Zwecken der Prozesskorrektur erforderlich ist.

Wenn eine Maschine zu diagnostischen Zwecken oder zur Prozesskorrektur für den Fernzugriff ausgelegt ist, muss das SRP/CS so gestaltet sein, dass es betriebsfähig bleibt, sofern keine anderen risikomindernden Maßnahmen angewendet werden, um das Risiko auf einem annehmbaren Niveau zu halten.

Die Gestaltung des SRP/CS muss einen ferngesteuerten Wiederanlauf der Maschine verhindern, wenn keine angemessene Benachrichtigung oder Anzeige für Personen an der Maschine oder in deren Nähe vorhanden ist.

ANMERKUNG 5 Ein ferngesteuerter Wiederanlauf, der von den an der Maschine arbeitenden Personen nicht vorhergesehen wird, kann zu Verletzungen führen.

5.3 Bestimmung des erforderlichen Performance Levels (PL_r) für jede Sicherheitsfunktion

Für jede gewählte Sicherheitsfunktion, die von einem SRP/CS auszuführen ist, muss ein erforderlicher Performance Level (PL_r) festgelegt und dokumentiert werden. Die Bestimmung des erforderlichen Performance Levels muss auf dem Ergebnis der Risikobeurteilung basieren und muss im Verhältnis zur Risikominderung stehen, die vom SRP/CS ausgeführt wird (siehe Bild 3). Der erforderliche Performance Level für jede Sicherheitsfunktion muss durch Risikoeinschätzung bestimmt werden. Der informative Anhang A enthält einen Leitfaden für die Bestimmung des PL_r für die Sicherheitsfunktion.

Da das Verfahren zur Bestimmung des erforderlichen Performance Levels eine subjektive Einschätzung umfasst, ist eine gewisse Variabilität bei der praktischen Anwendung bestimmter Fälle zulässig.

ANMERKUNG Der PL_r für eine Sicherheitsfunktion bestimmt die Zuverlässigkeit, mit der die Steuerung diese Sicherheitsfunktion ausführt und die vorgesehene Risikominderung erreicht wird. Der PL_r wird mithilfe verschiedener Risikofaktoren bestimmt. Siehe auch Anhang A.

5.4 Überprüfung der Spezifikation der Sicherheitsanforderungen

Die Spezifikation der Sicherheitsanforderungen muss überprüft werden, bevor mit der Gestaltung begonnen wird, da jedes weitere Vorgehen auf diesen Anforderungen basiert. Durch die Überprüfung muss sichergestellt werden, dass alle Sicherheitsfunktionen festgelegt sind, um die vorgesehene Risikominderung an der Maschine zu erreichen.

ANMERKUNG Je nach spezifischen Sicherheitsfunktionen kann es hilfreich sein, die SRS von zwei voneinander unabhängigen Personen anzufertigen und überprüfen zu lassen.

6 Gestaltungsaspekte

6.1 Bewertung des erreichten Performance Levels PL

6.1.1 Allgemeine Übersicht der Performance Level PL

Die Fähigkeit von sicherheitsbezogenen Teilen, eine Sicherheitsfunktion auszuführen, wird durch die Bewertung des Performance Levels bestimmt.

Ein Performance Level muss für jedes Teilsystem und/oder jede Kombination von Teilsystemen, die eine Sicherheitsfunktion ausführen, bestimmt werden. Der PL des Teilsystems muss durch die Abschätzung der folgenden Aspekte bestimmt werden:

- 1) der Architektur (siehe 6.1.3);
 - a) Zuweisen einer Kategorie zum Teilsystem und Bewerten des Ergebnisses;
 - b) Bewerten, sofern die geltenden qualitativen (nicht quantifizierbaren) Anforderungen der Kategorie erfüllt sind, einschließlich:
 - grundlegende Sicherheitsprinzipien (siehe ISO 13849-2:2013, Tabelle A.1, Tabelle B.1, Tabelle C.1 und Tabelle D.1);
 - bewährte Sicherheitsprinzipien (siehe ISO 13849-2:2013, Tabelle A.2, B.2, C.2 und D.2);
 - bewährte Bauteile (siehe ISO 13849-2:2013, Tabelle A.3 und Tabelle D.3, Anhang B und Anhang C);

- c) Bewerten, ob das erforderliche Verhalten bei (einem) Fehler(n) eingehalten wird;
- 2) des $MTTF_D$ -Werts einzelner Bauteile (siehe 6.1.4, Anhang C und Anhang D);
- 3) des DC (siehe 6.1.5 und Anhang F);
- 4) des CCF (siehe 6.1.6 und Anhang F);
- 5) des Einflusses der Gestaltung der sicherheitsbezogenen Software auf den Bediener der Hardware (siehe Abschnitt 7 und Anhang J);
- 6) des Einflusses der Maßnahmen gegen systematische Ausfälle (siehe 6.1.7 und Anhang G).

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, Architektur);
- b) nicht quantifizierbare, qualitative Aspekte, die das Verhalten des Teilsystems beeinflussen (Verhalten der Sicherheitsfunktion unter Fehlerbedingungen, sicherheitsbezogene Software, systematischer Ausfall, die Anwendung von grundlegenden und bewährten Sicherheitsprinzipien, die Anwendung von bewährten Bauteilen, Umgebungsbedingungen und Fehlerausschluss).

ANMERKUNG 2 Der Beitrag der Zuverlässigkeit (z. B. $MTTF_D$, Architektur) kann in Abhängigkeit von den verwendeten sicherheitsbezogenen Teilen variieren. Zum Beispiel ist es möglich (innerhalb bestimmter Grenzen), dass ein einzelner Kanal sicherheitsbezogener Teile mit hoher Verfügbarkeit den gleichen oder einen höheren PL bereitstellt als eine fehlertolerante Architektur mit niedrigerer Verfügbarkeit.

ANMERKUNG 3 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 Petri-Netze (GSPN), Zuverlässigkeitsblockdiagramme [siehe z. B. IEC 61508, IEC 61078].

Um die Beurteilung des PL zu erleichtern, liefert dieser Teil der ISO 13849 ein vereinfachtes Verfahren, das auf der Definition von fünf vorgesehenen Architekturen basiert, die spezielle Konstruktionsmerkmale und Verhalten bei einem Fehler erfüllen (siehe 6.1.3).

Die Anforderungen für die Bewertung des PL eines Teilsystems sind in 6.1 angegeben. Ein vereinfachter Ansatz für die Bewertung des PL eines Teilsystems ist in 6.1.8 (Bild 12), 6.1.9 angegeben, zusammen mit dem Verfahren von Anhang B bis Anhang H, Anhang J, Anhang K und Anhang L.

Für die Bewertung des PL von Teilsystem-Kombinationen siehe 6.2.

Das Erreichen qualitativer Aspekte des PL und das Vermeiden systematischer Ausfälle können durch die Anwendung der in diesem Dokument und Anhang G angegebenen Maßnahmen nachgewiesen werden.