

DIN EN ISO 13849-1

ICS 13.110

Entwurf

Einsprüche bis 2021-09-09
 Vorgesehen als Ersatz für
 DIN EN ISO 13849-1:2016-06;
 Ersatz für
 E DIN EN ISO 13849-1:2020-08

**Sicherheit von Maschinen –
 Sicherheitsbezogene Teile von Steuerungen –
 Teil 1: Allgemeine Gestaltungsleitsätze (ISO/DIS 13849-1.2:2021);
 Deutsche und Englische Fassung prEN ISO 13849-1:2021**

Safety of machinery –
 Safety-related parts of control systems –
 Part 1: General principles for design (ISO/DIS 13849-1.2:2021);
 German and English version prEN ISO 13849-1:2021

Sécurité des machines –
 Parties des systèmes de commande relatives à la sécurité –
 Partie 1: Principes généraux de conception (ISO/DIS 13849-1.2:2021);
 Version allemande et anglaise prEN ISO 13849-1:2021

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2021-07-09 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 332 Seiten

DIN-Normenausschuss Sicherheitstechnische Grundsätze (NASG)

Nationales Vorwort

Dieses Dokument (prEN ISO 13849-1:2021) wurde vom Technischen Komitee ISO/TC 199 „Safety of machinery“ in Zusammenarbeit mit dem 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 60529:1989+AMD2:2013	siehe	DIN EN 60529 (VDE 0470-1):2014-09
IEC 60812	siehe	DIN EN 60812
IEC 60947 (all parts)	siehe	DIN EN 60947 (VDE 0660) (alle Teile)
IEC 61000-1-2:2016	siehe	DIN EN 61000-1-2:2017-07
IEC 61000-6-2:2016	siehe	DIN EN IEC 61000-6-2:2019-11
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 61131-3:2013	siehe	DIN EN 61131-3:2014-06
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 61310-1:2007	siehe	DIN EN 61310-1 (VDE 0113-101):2008-09
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 61508-5:2010	siehe	DIN EN 61508-5 (VDE 0803-5):2011-02
IEC 61508-6:2010	siehe	DIN EN 61508-6 (VDE 0803-6):2011-02
IEC 61508-7:2010	siehe	DIN EN 61508-7 (VDE 0803-7):2011-02
IEC 61800-3:2017	siehe	DIN EN IEC 61800-3 (VDE 0160-103):2019-04

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 (VDE 0435) (alle Teile)
IEC 62046:2018	siehe	DIN EN IEC 62046 (VDE 0113-211):2019-03
IEC 62061:2005+AMD1:2012	siehe	DIN EN 62061 (VDE 0113-50):2016-05
ISO 4413:2010	siehe	DIN EN ISO 4413:2011-04
ISO 4414:2010	siehe	DIN EN ISO 4414:2011-04
ISO 7731	siehe	DIN EN ISO 7731
ISO 9001	siehe	DIN EN ISO 9001
ISO 9355-1:1999	siehe	DIN EN 894-1:1997-04*
ISO 9355-2:1999	siehe	DIN EN 894-2:1997-04**
ISO 9355-3:2006	siehe	DIN EN 894-3:2000-06***
ISO 10218-1:2011	siehe	DIN EN ISO 10218-1:2012-01
ISO 10218-2:2011	siehe	DIN EN ISO 10218-2:2012-06
ISO 11161:2007	siehe	DIN EN ISO 11161:2010-10
ISO 12100:2010	siehe	DIN EN ISO 12100:2011-03
ISO 13849-2:2012	siehe	DIN EN ISO 13849-2:2013-02
ISO 13850:2015	siehe	DIN EN ISO 13850:2016-05
ISO 13851:2019	siehe	DIN EN ISO 13851:2019-11
ISO 13855:2010	siehe	DIN EN ISO 13855:2010-10
ISO 13856-1:2013	siehe	DIN EN ISO 13856-1:2013-08
ISO 13856-2:2013	siehe	DIN EN ISO 13856-2:2013-08
ISO 14118:2017	siehe	DIN EN ISO 14118:2018-07
ISO 14119:2013	siehe	DIN EN ISO 14119:2014-03
ISO 16090 1:2017	siehe	DIN EN ISO 16090-1:2019-12
ISO 20607:2019	siehe	DIN EN ISO 20607:2019-10
ISO 23125:2015	siehe	DIN EN ISO 23125:2015-04
ISO/TR 14121-2:2012	siehe	DIN ISO/TR 14121-2 (DIN SPEC 33885):2013-02
ISO/TR 22100-2:2013	siehe	DIN ISO/TR 22100-2 (DIN SPEC 33887):2014-09
ISO/TR 22100-4	siehe	DIN CEN ISO/TR 22100-4
IEC/TR 63074	siehe	DIN IEC/TR 63074 (VDE 0113 74)

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

* Diese Ausgabe ist mit Ersatz zurückgezogen. Das aktuell gültige Ausgabedatum ist: 2009-01.

** Diese Ausgabe ist mit Ersatz zurückgezogen. Das aktuell gültige Ausgabedatum ist: 2009-02.

*** Diese Ausgabe ist mit Ersatz zurückgezogen. Das aktuell gültige Ausgabedatum ist: 2010-01.

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) Anforderungen an die Spezifikation der Sicherheitsfunktion überarbeitet (Abschnitt 5);
- e) Beschreibung der Anforderungen an das Design und die verschiedenen Performance Levels (Abschnitt 6);
- 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;
- l) Integration von Anhang O mit Beschreibung der sicherheitsbezogene Werte von Komponenten oder Teilen der Steuerungen.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN CEN ISO/TR 22100-4, *Sicherheit von Maschinen — Zusammenhang mit ISO 12100 — Teil 4: Leitlinien für Maschinenhersteller zur Berücksichtigung der damit verbundenen IT-Sicherheits- (Cybersicherheits-) Aspekte*

DIN EN 894-1:1997-04, *Sicherheit von Maschinen — Ergonomische Anforderungen an die Gestaltung von Anzeigen und Stellteilen — Teil 1: Allgemeine Leitsätze für Benutzer-Interaktion mit Anzeigen und Stellteilen; Deutsche Fassung EN 894-1:1997*

DIN EN 894-2:1997-04, *Sicherheit von Maschinen — Ergonomische Anforderungen an die Gestaltung von Anzeigen und Stellteilen — Teil 2: Anzeigen; Deutsche Fassung EN 894-2:1997*

DIN EN 894-3:2000-06, *Sicherheit von Maschinen — Ergonomische Anforderungen an die Gestaltung von Anzeigen und Stellteilen — Teil 3: Stellteile — Deutsche Fassung EN 894-3:2000*

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): 2014-09, *Schutzarten durch Gehäuse (IP-Code) (IEC 60529:1989 + A1:1999 + A2:2013); Deutsche Fassung EN 60529:1991 + A1:2000 + A2:2013*

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

DIN EN 60947 (alle Teile), *Niederspannungsschaltgeräte*

DIN EN 61000-1-2:2017-07, *Elektromagnetische Verträglichkeit (EMV) — Teil 1-2: Allgemeines — Verfahren zum Erreichen der funktionalen Sicherheit von elektrischen und elektronischen Systemen einschließlich Geräten und Einrichtungen im Hinblick auf elektromagnetische Phänomene (IEC 61000-1-2:2016); Deutsche Fassung EN 61000-1-2:2016*

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: 2014-06, *Speicherprogrammierbare Steuerungen — Teil 3: Programmiersprachen (IEC 61131-3:2013); Deutsche Fassung EN 61131-3:2013*

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 61310-1 (VDE 0113-101):2008-09, *Sicherheit von Maschinen — Anzeigen, Kennzeichen und Bedienen — Teil 1: Anforderungen an sichtbare, hörbare und tastbare Signale (IEC 61310-1:2007); Deutsche Fassung EN 61310-1:2008*

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 61508-5 (VDE 0803-5):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level) (IEC 61508-5:2010); Deutsche Fassung EN 61508-5:2010*

DIN EN 61508-6 (VDE 0803-6):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3 (IEC 61508-6:2010); Deutsche Fassung EN 61508-6:2010*

DIN EN 61508-7 (VDE 0803-7):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 7: Überblick über Verfahren und Maßnahmen (IEC 61508-7:2010); Deutsche Fassung EN 61508-7:2010*

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 61000-6-2:2019-11, *Elektromagnetische Verträglichkeit (EMV) — Teil 6-2: Fachgrundnormen — Störfestigkeit für Industriebereiche (IEC 61000-6-2:2016); Deutsche Fassung EN IEC 61000-6-2:2019*

DIN EN IEC 61800-3 (VDE 0160-103):2019-04, *Drehzahlveränderbare elektrische Antriebssysteme — Teil 3: EMV-Anforderungen einschließlich spezieller Prüfverfahren (IEC 61800-3:2017); Deutsche Fassung EN IEC 61800-3:2018*

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

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 ISO 4413:2011-04, *Fluidtechnik — Allgemeine Regeln und sicherheitstechnische Anforderungen an Hydraulikanlagen und deren Bauteile (ISO 4413:2010); Deutsche Fassung EN ISO 4413:2010*

DIN EN ISO 4414:2011-04, *Fluidtechnik — Allgemeine Regeln und sicherheitstechnische Anforderungen an Pneumatikanlagen und deren Bauteile (ISO 4414:2010); Deutsche Fassung EN ISO 4414:2010*

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

DIN EN ISO 9001, *Qualitätsmanagementsysteme — Anforderungen*

DIN EN ISO 10218-1:2012-01, *Industrieroboter — Sicherheitsanforderungen — Teil 1: Roboter (ISO 10218-1:2011); Deutsche Fassung EN ISO 10218-1:2011*

DIN EN ISO 10218-2:2012-06, *Industrieroboter — Sicherheitsanforderungen — Teil 2: Robotersysteme und Integration (ISO 10218-2:2011); Deutsche Fassung EN ISO 10218-2:2011*

DIN EN ISO 11161:2010-10, *Sicherheit von Maschinen — Integrierte Fertigungssysteme — Grundlegende Anforderungen (ISO 11161:2007 + Amd 1:2010); Deutsche Fassung EN ISO 11161:2007 + A1:2010*

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 13850:2016-05, *Sicherheit von Maschinen — Not-Halt-Funktion — Gestaltungsleitsätze (ISO 13850:2015); Deutsche Fassung EN ISO 13850:2015*

DIN EN ISO 13851:2019-11, *Sicherheit von Maschinen — Zweihandschaltungen — Funktionelle Aspekte und Gestaltungsleitsätze (ISO 13851:2019); Deutsche Fassung EN ISO 13851:2019*

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 13856-1:2013-08, *Sicherheit von Maschinen — Druckempfindliche Schutzeinrichtungen — Teil 1: Allgemeine Leitsätze für die Gestaltung und Prüfung von Schalmatten und Schaltplatten (ISO 13856-1:2013); Deutsche Fassung EN ISO 13856-1:2013*

DIN EN ISO 13856-2:2013-08, *Sicherheit von Maschinen — Druckempfindliche Schutzeinrichtungen — Teil 2: Allgemeine Leitsätze für die Gestaltung und Prüfung von Schaltleisten und Schaltstangen (ISO 13856-2:2013); Deutsche Fassung EN ISO 13856-2:2013*

DIN EN ISO 14118:2018-07, *Sicherheit von Maschinen — Vermeidung von unerwartetem Anlauf (ISO 14118:2017); Deutsche Fassung EN ISO 14118:2018*

DIN EN ISO 14119:2014-03, *Sicherheit von Maschinen — Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen — Leitsätze für Gestaltung und Auswahl (ISO 14119:2013); Deutsche Fassung EN ISO 14119:2013*

DIN EN ISO 16090-1:2019-12, *Werkzeugmaschinen-Sicherheit — Bearbeitungszentren, Fräsmaschinen, Transfermaschinen — Teil 1: Sicherheitsanforderungen (ISO 16090-1:2017); Deutsche Fassung EN ISO 16090-1:2018*

DIN EN ISO 20607:2019-10, *Sicherheit von Maschinen — Betriebsanleitung — Allgemeine Gestaltungsgrundsätze (ISO 20607:2019); Deutsche Fassung EN ISO 20607:2019*

DIN EN ISO 23125:2015-04, *Werkzeugmaschinen — Sicherheit — Drehmaschinen (ISO 23125:2015); Deutsche Fassung EN ISO 23125:2015*

DIN ISO/TR 14121-2 (DIN SPEC 33885):2013-02, *Sicherheit von Maschinen — Risikobeurteilung — Teil 2: Praktischer Leitfaden und Verfahrensbeispiele (ISO/TR 14121-2:2012)*

DIN ISO/TR 22100-2 (DIN SPEC 33887):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*

DIN IEC/TR 63074 (VDE 0113 74), *Maschinensicherheit — Aspekte zur Cybersicherheit in Verbindung mit der funktionalen Sicherheit von sicherheitsrelevanten Steuerungssystemen*

<i>Titel de:</i>	Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen — Teil 1: Allgemeine Gestaltungsleitsätze (ISO/DIS 13849-1.2:2021)
<i>Titel en:</i>	Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design (ISO/DIS 13849-1.2:2021)
<i>Titel fr:</i>	Sécurité des machines — Parties des systèmes de commande relatives à la sécurité — Partie 1: Principes généraux de conception (ISO/DIS 13849-1.2:2021)

Inhalt

	Seite
Europäisches Vorwort	5
Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der abzudeckenden Richtlinie 2006/42/EG	6
Vorwort	8
Einleitung	9
1 Anwendungsbereich.....	12
2 Normative Verweisungen	12
3 Begriffe, Symbole und Abkürzungen	13
3.1 Begriffe	13
3.2 Symbole und Abkürzungen	23
4 Überblick	25
4.1 Prozess zur Risikobeurteilung und Risikominderung an der Maschine.....	25
4.2 Beitrag zur Risikominderung.....	27
4.3 Entwurfsprozess eines SRP/CS	27
4.4 Verfahren.....	28
4.5 Erforderliche Informationen.....	29
4.6 Ausführung von Sicherheitsfunktionen mithilfe von Teilsystemen	30
5 Spezifikation der Sicherheitsfunktionen.....	30
5.1 Identifizierung und allgemeine Beschreibung der Sicherheitsfunktion.....	30
5.2 Spezifikation der Sicherheitsanforderungen	31
5.2.1 Allgemeine Anforderungen.....	31
5.2.2 Anforderungen an spezifische Sicherheitsfunktionen	34
5.3 Bestimmung des erforderlichen Performance Levels für jede Sicherheitsfunktion.....	40
5.4 Überprüfung der Spezifikation der Sicherheitsanforderungen	40
5.5 Zerlegung eines SRP/CS in Teilsysteme	40
6 Entwurfsaspekte	42
6.1 Bewertung des erreichten Performance Levels	42
6.1.1 Allgemeine Übersicht der Performance Levels	42
6.1.2 Zusammenhang zwischen dem Performance Level und dem Sicherheits-Integritätslevel	44
6.1.3 Architektur — Kategorien und deren Beziehung zur MTTF _D jedes Kanals, zum durchschnittlichen Diagnosedeckungsgrad und zum Ausfall infolge gemeinsamer Ursache	45
6.1.4 Mittlere Dauer bis zum gefahrbringenden Ausfall.....	53
6.1.5 Diagnosedeckungsgrad	54
6.1.6 Ausfälle infolge gemeinsamer Ursache	55
6.1.7 Systematische Ausfälle	55
6.1.8 Vereinfachtes Verfahren für die Abschätzung des Performance Levels für Teilsysteme	56
6.1.9 Alternatives Verfahren für die Bestimmung des Performance Levels und der PFH _D ohne MTTF _D	58
6.1.10 Fehlerbetrachtung und Fehlerausschluss	59
6.1.11 Bewährtes Bauteil	61
6.2 Kombination von Teilsystemen zum Erreichen eines gesamten Performance Levels für die Sicherheitsfunktion	61

6.2.1	Allgemeines	61
6.2.2	Bekannte PFH _D -Werte	61
6.2.3	Unbekannte PFH _D -Werte	62
7	Software-Sicherheitsanforderungen	63
7.1	Allgemeines	63
7.2	Programmiersprache mit eingeschränktem Sprachumfang und Programmiersprache mit nicht eingeschränktem Sprachumfang	64
7.2.1	Programmiersprache mit eingeschränktem Sprachumfang	64
7.2.2	Programmiersprache mit nicht eingeschränktem Sprachumfang	64
7.2.3	Entscheidung zwischen Programmiersprache mit eingeschränktem Sprachumfang und Programmiersprache mit nicht eingeschränktem Sprachumfang	64
7.3	Sicherheitsbezogene Embedded-Software	66
7.4	Sicherheitsbezogene Anwendungssoftware	67
7.5	Softwarebasierte manuelle Parametrisierung	70
7.5.1	Allgemeines	70
7.5.2	Einflüsse auf sicherheitsbezogene Parameter	71
7.5.3	Anforderungen an die softwarebasierte manuelle Parametrisierung	72
7.5.4	Verifizierung des Parametrisierungswerkzeugs	73
7.5.5	Dokumentation der softwarebasierten manuellen Parametrisierung	73
8	Verifizierung, ob der erreichte Performance Level dem erforderlichen Performance Level entspricht	74
9	Ergonomische Entwurfsaspekte	74
10	Validierung	74
10.1	Grundsätze der Validierung	74
10.1.1	Allgemeines	74
10.1.2	Validierungsplan	76
10.1.3	Allgemeine Fehlerlisten	77
10.1.4	Spezielle Fehlerlisten	77
10.1.5	Angaben zur Validierung	77
10.2	Validierung der Spezifikation der Sicherheitsanforderungen	79
10.3	Validierung durch Analyse	79
10.3.1	Allgemeines	79
10.3.2	Analysetechniken	80
10.4	Validierung durch Prüfung	80
10.4.1	Allgemeines	80
10.4.2	Messgenauigkeit	81
10.4.3	Zusätzliche Prüfanforderungen	81
10.4.4	Anzahl der Prüflinge	81
10.4.5	Prüfverfahren	82
10.5	Validierung der Sicherheitsfunktionen	82
10.6	Validierung der Sicherheitsintegrität des SRP/CS	83
10.6.1	Validierung von Teilsystem(en)	83
10.6.2	Validierung der Maßnahmen zur Vermeidung systematischer Ausfälle	85
10.6.3	Validierung der sicherheitsbezogenen Software	85
10.6.4	Validierung der Kombination von Teilsystemen	86
10.6.5	Gesamtvalidierung der Sicherheitsintegrität	87
10.7	Validierung der Umgebungsanforderungen	87
10.8	Aufzeichnung der Validierung	87
10.9	Validierung der Instandhaltungsanforderungen	88
11	Wartungsfreundlichkeit von SRP/CS	88
12	Technische Dokumentation	89

13	Benutzerinformation	89
13.1	Allgemeines	89
13.2	Informationen für die Integration des SRP/CS	89
13.3	Informationen für den Benutzer	90
Anhang A (informativ)	Leitlinien für die Bestimmung des erforderlichen Performance Levels.....	92
Anhang B (informativ)	Blockmethode und sicherheitsbezogenes Blockdiagramm.....	97
Anhang C (informativ)	Berechnung oder Abschätzung von MTTF_D-Werten für einzelne Bauteile	99
Anhang D (informativ)	Vereinfachtes Verfahren zur Abschätzung der MTTF_D für jeden Kanal.....	107
Anhang E (informativ)	Abschätzungen des Diagnosedeckungsgrades für Funktionen und Teilsysteme	109
Anhang F (informativ)	Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache.....	114
Anhang G (informativ)	Systematischer Ausfall	118
Anhang H (informativ)	Beispiel für eine Kombination von mehreren Teilsystemen.....	122
Anhang I (informativ)	Beispiele.....	125
Anhang J (informativ)	Beispiel für die Ausführung einer SRESW.....	134
Anhang K (informativ)	Numerische Darstellung von Bild 12	139
Anhang L (informativ)	Elektromagnetische Störfestigkeit.....	144
Anhang M (informativ)	Ergänzende Informationen zur Spezifikation der Sicherheitsanforderungen	148
Anhang N (informativ)	Vermeiden eines systematischen Ausfalls durch den Softwareentwurf.....	150
Anhang O (informativ)	Sicherheitsbezogene Werte von Bauteilen oder Komponenten der Steuerungen.....	164
Literaturhinweise.....		167

Europäisches Vorwort

Dieses Dokument (prEN ISO 13849-1:2021) wurde vom Technischen Komitee ISO/TC 199 „Safety of machinery“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 114 „Sicherheit von Maschinen und Geräten“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur zweiten parallelen Umfrage vorgelegt.

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

Dieses Dokument wurde im Rahmen eines Mandates erarbeitet, das die Europäische Kommission und die Europäische Freihandelsassoziation CEN erteilt haben, und unterstützt grundlegende Anforderungen der EU-Richtlinie(n).

Zum Zusammenhang mit EU-Richtlinie(n) siehe informativen Anhang ZA, der Bestandteil dieses Dokuments ist.

Anerkennungsnotiz

Der Text von ISO/DIS 13849-1.2:2021 wurde von CEN als prEN ISO 13849-1:2021 ohne irgendeine Abänderung genehmigt.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN abrufbar.

Anhang ZA (informativ)

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

Diese Europäische Norm wurde im Rahmen eines von der Europäischen Kommission erteilten Normungsauftrages „M/396 Mandat an CEN und CENELEC für Normungsarbeiten im Bereich Maschinen“ erarbeitet, um ein freiwilliges Mittel zur Erfüllung der grundlegenden Anforderungen der Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG (Neufassung) bereitzustellen.

Sobald diese Norm im Amtsblatt der Europäischen Union im Sinne dieser Richtlinie in Bezug genommen worden ist, berechtigt die Übereinstimmung mit den in Tabelle ZA.1 aufgeführten normativen Abschnitten dieser Norm innerhalb der Grenzen des Anwendungsbereiches dieser Norm zur Vermutung der Konformität mit den entsprechenden grundlegenden Anforderungen der Richtlinie und der zugehörigen EFTA-Vorschriften.

Tabelle ZA.1 — Zusammenhang zwischen dieser Europäischen Norm und der Richtlinie 2006/42/EG

Relevante grundlegende Anforderungen der Richtlinie 2006/42/EG	Abschnitt(e)/Unterabschnitt(e) dieser Europäischen Norm	Erläuterungen/Anmerkungen
1.1.6	9	
1.2.1	6, 7, 10	
1.2.3	5.2.2.3	Dieser Unterabschnitt befasst sich nur mit der Wiederanlauffunktion.
1.2.4.1	5.2.2.1	Dieser Unterabschnitt befasst sich nur mit derjenigen sicherheitsbezogenen Stopp-Funktion, mit der die Stopp-Kategorie 0 oder 1 erzielt wird.
1.2.4.2	5.2.2.1	Dieser Unterabschnitt befasst sich nur mit derjenigen sicherheitsbezogenen Stopp-Funktion, mit der die Stopp-Kategorie 2 erzielt wird.
1.2.4.3	5.2.1	Dieser Unterabschnitt befasst sich nur mit der Spezifikation der Sicherheitsanforderungen einer Not-Halt-Funktion.
1.2.5	5.2.2.8	
1.2.6	5.2.1.3 Listenpunkt i), 5.2.2.7	
1.6.1	11	
1.6.2	11	
1.6.4	11	
1.7.4.2 (e, g, i, r, s)	13	Dieser Unterabschnitt befasst sich nur mit der Anleitung für die Sicherheitsfunktionen.

WARNHINWEIS 1 — Die Konformitätsvermutung bleibt nur bestehen, so lange die Fundstelle dieser Europäischen Norm in der im Amtsblatt der Europäischen Union veröffentlichten Liste erhalten bleibt. Anwender dieser Norm sollten regelmäßig die im Amtsblatt der Europäischen Union zuletzt veröffentlichte Liste einsehen.

WARNHINWEIS 2 — Für Produkte, die in den Anwendungsbereich dieser Norm fallen, können weitere Rechtsvorschriften der EU anwendbar sein.

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.

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

Die wesentlichen Änderungen im Vergleich zur Vorgängerausgabe sind folgende Neuerungen:

- Spezifikation der Sicherheitsfunktionen (Abschnitt 5);
- Software (Abschnitt 7);
- Validierung (Abschnitt 10);
- Kombination von mehreren Teilsystemen;
- Management der funktionalen Sicherheit (G.5);
- elektromagnetische Störfestigkeit (Anhang L);
- ergänzende Informationen für die Spezifikation der Sicherheitsanforderungen (Anhang M);
- Vermeiden von Fehlern/Maßnahmen zur Fehlervermeidung für den sicherheitsbezogenen Softwareentwurf (Anhang N);
- sicherheitsbezogene Werte von Bauteilen oder Komponenten der Steuerungen (Anhang O).

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

Dieses Dokument ist eine Typ-B1-Norm, wie in ISO 12100 angegeben.

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

Die zweite Ausgabe von ISO 13849-1 wurde 2006 überarbeitet.

Die dritte Ausgabe wurde 2015 geändert und veröffentlicht.

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

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

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

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);
- 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 dieses Dokuments 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 in den Anwendungsbereich einer Typ-C-Norm fallen und die nach deren Anforderungen konstruiert und gebaut worden sind, haben die Anforderungen dieser Typ-C-Normen Vorrang.

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 Dokuments ist es, denjenigen Interessengruppen einen Leitfaden bereitzustellen, die an der Gestaltung und Beurteilung von Steuerungen beteiligt sind, sowie denjenigen, die Typ-B2- oder Typ-C-Normen erarbeiten.

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

Bild 1, das aus ISO 12100 übernommen wurde, zeigt den Zusammenhang zwischen ISO 12100 und diesem Dokument. Für eine ausführliche Übersicht siehe Bild 2.

X



Die Fähigkeit sicherheitsbezogener Teile von Steuerungen, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen, wird einer von fünf Stufen zugeordnet, den so genannten Performance Levels (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 unter anderem von der Hardware- und Softwarestruktur, dem Umfang der Fehler-Detektionsmechanismen (Diagnosedeckungsgrad (DC)), der Zuverlässigkeit von Bauteilen (mittlere Zeit bis zum gefahrbringenden Ausfall ($MTTF_D$), dem Ausfall infolge gemeinsamer Ursache (CCF)), dem Gestaltungsprozess, der Belastung im Betrieb, den Umgebungsbedingungen und den betrieblichen Einsatzbedingungen.

Um den Entwurf von SRP/CS und die Beurteilung des erreichten PL zu erleichtern, wird in diesem Dokument ein Verfahren genutzt, das darauf basiert, Architekturen anhand spezifischer Entwurfskriterien ($MTTF_D$, DC_{avg} usw.) und dem spezifizierten Verhalten unter Fehlerbedingungen zu kategorisieren. Diese Architekturen werden einer von fünf Stufen zugeordnet, die als Kategorien B, 1, 2, 3 und 4 bezeichnet werden.

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. Aus diesem Grund sollte die in diesem Dokument beschriebene Vorgehensweise eher als nützlicher Leitfaden für die Gestaltung von sicherheitsbezogenen Teilen der Steuerung angesehen werden.

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

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

Die Performance Levels und die Kategorien können für Teilsysteme von SRP/CS definiert und bestimmt werden, die Sicherheitsteile (Komponenten) nutzen, wie beispielsweise:

- Schutzeinrichtungen (z. B. Zweihandschaltungen, Verriegelungseinrichtungen);
- leistungssteuernde Elemente (z. B. Relais, Ventile);
- Sensoren und HMI-Elemente (Wegmesseinrichtungen, Freigabeschalter).

Die von diesem Dokument berücksichtigten Maschinen können von einfachen Maschinen (z. B. Küchenkleingeräte oder Automatiktüren und -tore) bis hin zu komplexen Maschinen (z. B. Verpackungsmaschinen, Druckereimaschinen, Pressen und in ein System integrierte Maschinen) reichen.

Dieses Dokument und IEC 62061 legen zusammen ein Verfahren fest und enthalten entsprechende Leitlinien für die Gestaltung und die Ausführung sicherheitsbezogener Steuerungen von Maschinen.

Die Anforderungen von Abschnitt 10 dieses Dokuments 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

Dieses Dokument legt ein Verfahren fest und enthält zugehörige Empfehlungen und Anforderungen für die Gestaltung und Integration sicherheitsbezogener Teile von Steuerungen (SRP/CS), einschließlich der Entwicklung von Software. Dieses Dokument legt ein Verfahren fest und enthält einen Leitfaden für die Gestaltung und Integration sicherheitsbezogener Teile von Steuerungen (SRP/CS), die Sicherheitsfunktionen ausführen, einschließlich der Entwicklung von Software. Dieses Dokument gilt für SRP/CS für die Betriebsart mit hoher Anforderungsrate und die Betriebsart mit kontinuierlicher Anforderung einschließlich ihrer Teilsysteme, ungeachtet der Technologie und der Art der Energie (z. B. elektrisch, hydraulisch, pneumatisch und mechanisch). Dieses Dokument gilt nicht für Betriebsarten mit niedriger Anforderungsrate.

ANMERKUNG 1 Siehe 3.1.43 und IEC 61508 für die Betriebsart mit niedriger Anforderungsrate. Dieses Dokument legt nicht fest, welche Sicherheitsfunktionen oder welche erforderlichen Performance Levels für spezielle Fälle zu verwenden sind.

Dieses Dokument stellt keine speziellen Anforderungen an den Entwurf von Produkten/Bauteilen, die Teile von SRP/CS sind. Spezifische Anforderungen an den Entwurf von Bauteilen eines SRP/CS werden in den zutreffenden ISO- und IEC-Normen behandelt.

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

ANMERKUNG 2 Sicherheitsaspekte können einen Einfluss auf Sicherheitsfunktionen haben.-Siehe ISO/TR 22100-4 und IEC/TR 63074 für weitere Informationen.

ANMERKUNG 3 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 gelten. Diese spezifischen Anforderungen können in einer Typ-C-Norm festgelegt sein.

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

ISO 13855:2010, *Safety of machinery — Positioning of safeguards with respect to the approach speeds of parts of the human body*

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*

IEC 62061:2005+AMD1:2012, *Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems*

3 Begriffe, Symbole und Abkürzungen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO 12100:2010 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 <https://www.electropedia.org/>
- ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>

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

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).

3.1.3

Spezifikation der Sicherheitsanforderungen

SRS, en: safety requirement specification

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

[QUELLE: IEC 61508-4:2010, 3.5.11, modifiziert, Angaben aus 3.5.12 enthalten]

3.1.4

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

3.1.5

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.

3.1.6 erforderlicher Performance Level PL_r

Performance Level, der erforderlich ist, um die erforderliche Risikominderung für jede Sicherheitsfunktion zu erreichen

Anmerkung 1 zum Begriff: Siehe 5.3 und Bild A.1.

3.1.7 Sicherheits-Integritätslevel SIL

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

Anmerkung 1 zum Begriff: In diesem Dokument werden nur SIL 1 bis SIL 3 berücksichtigt.

[QUELLE: IEC 61508-4:2010, 3.5.8, modifiziert — ANMERKUNGEN wurden gestrichen und „die den sicherheitsbezogenen Systemen zugeordnet werden“ wurde ergänzt.]

3.1.8 Fehler Fehlzustand

Zustand eines Geräts, in dem es unfähig ist, eine geforderte Funktion zu erfüllen, wobei die durch Wartung oder andere geplante Handlungen verursachte Funktionsunfähigkeit ausgeschlossen ist

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 Dokument bedeutet der Begriff „Fehler“ entweder „zufälliger Fehler“ oder „durch systematischen Ausfall hervorgerufener Fehler“.

[QUELLE: IEC 60050-192:2015, modifiziert — Anmerkung 2 zum Begriff wurde ergänzt.]

3.1.9 Fehlerausschluss

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

3.1.10 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 Dokuments.

[QUELLE: IEC 60050-192:2015, modifiziert — Anmerkung 3 zum Begriff wurde ergänzt.]

3.1.11

permanenter Fehlzustand

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

[QUELLE: IEC 60050-192:2015]

3.1.12

gefährbringender Ausfall

Ausfall eines Elements und/oder Teilsystems und/oder Systems, das Anteil an der Ausführung der Sicherheitsfunktion hat, der:

- a) verhindert, dass eine Sicherheitsfunktion bei Anforderung ausgeführt wird (Anforderungsbetriebsart) oder den Ausfall einer Sicherheitsfunktion verursacht (Betriebsart mit kontinuierlicher Anforderung), so dass das SRP/CS in einen gefährlichen oder möglicherweise gefährlichen Zustand gebracht wird; oder
- b) die Wahrscheinlichkeit vermindert, die Sicherheitsfunktion bei Anforderung ordnungsgemäß auszuführen

[QUELLE: IEC 61508-4:2010, 3.6.7, modifiziert, „EUC“ wurde durch „SRP/CS“ ersetzt.]

3.1.13

Ausfall infolge gemeinsamer Ursache

CCF, en: common cause failure

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

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

[QUELLE: IEC 61508-4:2010, 3.6.10, Anmerkung 1 zum Begriff wurde ergänzt.]

3.1.14

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 der Software.

[QUELLE: IEC 60050-192:2015]

3.1.15

Überbrückungsfunktion

vorübergehende automatische Überbrückung einer Sicherheitsfunktion bzw. von Sicherheitsfunktionen durch das SRP/CS

[QUELLE: IEC 61496-1:2012, 3.16]

3.1.16

manuelle Rückstellung

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

3.1.17

Schaden

physische Verletzung oder Gesundheitsschädigung

[QUELLE: ISO 12100:2010, 3.5]

3.1.18

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 zum Begriff wurde gestrichen.]

3.1.19

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]

3.1.20

Risiko

Kombination der Wahrscheinlichkeit des Eintritts eines Schadens und seines Schadensausmaßes

[QUELLE: ISO 12100:2010, 3.12]

3.1.21

Restrisiko

Risiko, das verbleibt, nachdem risikomindernde Maßnahmen (Schutzmaßnahmen) umgesetzt wurden

Anmerkung 1 zum Begriff: Siehe Bild 3.

[QUELLE: ISO 12100:2010, 3.13, modifiziert — Anmerkung 1 zum Begriff wurde geändert.]

3.1.22

Risikobeurteilung

Gesamtheit des Verfahrens, das eine Risikoanalyse und Risikobewertung umfasst

[QUELLE: ISO 12100:2010, 3.17]

3.1.23

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]

3.1.24

Risikoanalyse

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

[QUELLE: ISO 12100:2010, 3.15]

3.1.25

Risikobewertung

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

[QUELLE: ISO 12100:2010, 3.16]

3.1.26

bestimmungsgemäße Verwendung einer Maschine

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

[QUELLE: ISO 12100:2010, 3.23]

3.1.27

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]

3.1.28

Sicherheitsfunktion

Funktion der 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 im Falle eines spezifischen Gefährdungsereignisses einen sicheren Zustand für die Maschine zu erreichen oder diesen aufrecht zu erhalten.

[QUELLE: ISO 12100:2010, 3.30]

3.1.29

Teilfunktion

Teil einer Sicherheitsfunktion, dessen Ausfall zu einem Ausfall der Sicherheitsfunktion führt

Anmerkung 1 zum Begriff: Eine Teilfunktion ist eine Funktion, die von einem Teilsystem des SRP/CS auszuführen ist. Siehe auch IEC 61800-5-2:2016.

BEISPIEL Teilfunktionen nach IEC 61800-5-2 sind zum Beispiel sicher abgeschaltetes Drehmoment (STO, en: safe torque off) und sicherer Stopp 1 (SS1). Siehe Bild 6.

3.1.30

Überwachung

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

Anmerkung 1 zum Begriff: Überwachung erfolgt mithilfe der folgenden Verfahren: Plausibilitätsprüfung (direkt, indirekt oder Kreuzvergleich, siehe 3.1.24), zyklischer Testimpuls oder Kreuzvergleich.

3.1.31

Kreuzvergleich

Diagnosemaßnahme zur Überprüfung der Plausibilität von redundanten Signalen in beiden Kanälen eines redundanten Teilsystems

3.1.32

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]

3.1.33

mittlere Dauer bis zum gefahrbringenden Ausfall

MTTF_D, en: mean time to dangerous failure

Erwartungswert der Verteilung der Dauern bis zum gefahrbringenden Ausfall

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

[QUELLE: IEC 62061:2019, 3.2.34, modifiziert — Anmerkung 1 zum Begriff wurde geändert.]

3.1.34

mittlere Betriebsdauer zwischen Ausfällen

MTBF, en: mean time between failure

erwarteter Wert der Betriebsdauer zwischen aufeinanderfolgenden Ausfällen

3.1.35

gefährliche Ausfallrate

RDF, en: ratio of dangerous failures

Anteil der gesamten Ausfallrate eines Elements, der zu einem gefahrbringenden Ausfall führen kann

3.1.36

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.

3.1.37

Gebrauchsdauer

T_M

Zeitraum, der die bestimmungsgemäße Verwendung eines SRP/CS abdeckt

3.1.38

Testrate

r_t

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

3.1.39

Anforderungsrate

r_d

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

3.1.40

Programmiersprache mit eingeschränktem Sprachumfang

LVL, en: limited variability language

Art von Programmiersprache, die die Möglichkeit bietet, vorgegebene anwendungsspezifische Funktionen aus einer Bibliothek zu kombinieren, um die festgelegten Sicherheitsanforderungen zu implementieren

Anmerkung 1 zum Begriff: Eine LVL bietet eine enge funktionale Korrespondenz zu den zur Erreichung der Anwendung erforderlichen Funktionen.

Anmerkung 2 zum Begriff: Typische Beispiele für LVL sind in IEC 61131-3 angegeben. Hierzu zählen ein Leiterdiagramm, ein Funktionsblockdiagramm und eine sequentielle Funktionstabelle. Befehlslisten und strukturierter Text gelten nicht als LVL.

Anmerkung 3 zum Begriff: Typisches Beispiel für Systeme, die LVL verwenden: speicherprogrammierbare Steuerung (SPS), konfiguriert für die Maschinensteuerung.

[QUELLE: IEC 62061, FDIS 2020, 3.2.62]

3.1.41

Programmiersprache mit nicht eingeschränktem Sprachumfang

FVL, en: full variability language

Programmiersprache, die die Möglichkeit bietet, eine große Vielzahl unterschiedlicher Funktionen und Anwendungen zu implementieren

Anmerkung 1 zum Begriff: Allzweck-Computer sind ein gutes Beispiel für Systeme, die FVL verwenden.

Anmerkung 2 zum Begriff: FVL ist üblicherweise in Embedded-Software enthalten und wird nur selten für Anwendungssoftware verwendet.

Anmerkung 3 zum Begriff: FVL-Beispiele sind: Ada, C, Pascal, Instruction List, Assembler-Sprachen, C++, Java, SQL.

[QUELLE: IEC 62061, FDIS 2020, 3.2.61]

3.1.42

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

3.1.43

sicherheitsbezogene Embedded-Software

SRESW, en: safety related embedded software

Firmware

Software, die als Bestandteil des Systems vom Hersteller mitgeliefert wird

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

[QUELLE: IEC 61511-1:2016, 3.2.76.2, modifiziert — „und durch den Endbenutzer nicht verändert werden kann“ wurde gestrichen.]

3.1.44

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 normalen Betriebs in einem sicheren Zustand hält

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

3.1.45

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, modifiziert — Anmerkung 1 zum Begriff ergänzt.]

3.1.46

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.

3.1.47

Teilsystemelement

Teil eines Teilsystems, bestehend aus einem einzelnen Bauteil oder einer Baugruppe

Anmerkung 1 zum Begriff: Ein Teilsystemelement kann Hardware oder eine Kombination von Hardware und Software umfassen. Für die Anwendung dieses Dokuments werden Bauteile, die ausschließlich Software umfassen, nicht als Teilsystemelemente betrachtet.

3.1.48

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]

3.1.49

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 Verfahren 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. B. Fehler, die während des Entwurfs, der Integration, der Modifikation oder der Verschlechterung des Produkts auftreten.

Anmerkung 3 zum Begriff: In ISO 13849-2:2012, Tabelle A.2, Tabelle B.2, Tabelle C.2 und Tabelle D.2, werden bewährte Sicherheitsprinzipien für verschiedene Technologien behandelt.

3.1.50

bewährtes Bauteil

Bauteil, das erfolgreich in sicherheitsbezogenen Anwendungen eingesetzt wurde

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

3.1.51

Betriebsart

Betriebsweise einer Maschine (z. B. 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 risikomindernden Maßnahmen 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.

3.1.52

dynamisches Testen

überwachte Diagnosemaßnahme, die in geeigneten Abständen eine Signaländerung zu Testzwecken ausführt

Anmerkung 1 zum Begriff: Der Test ist nicht bestanden, wenn die Signaländerung 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.

3.1.53

Plausibilitätsprüfung

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

3.1.54

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]

3.1.55

Validierung

Bestätigen aufgrund einer Untersuchung und durch Bereitstellung eines objektiven Nachweises, dass die besonderen Anforderungen für eine spezielle beabsichtigte Verwendung 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: IEC 61508-4:2010, 3.8.2]

3.1.56

Fachkraft

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

Anmerkung 1 zum Begriff: Bei der Beurteilung der Fachausbildung kann 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.]

3.1.57

Black Box

Gerät, System oder Objekt, das hinsichtlich seiner Eingänge und Ausgänge überprüft werden kann

3.1.58

Grey Box

Gerät, System oder Objekt, von dem einige der internen Funktionen bekannt sind

Anmerkung 1 zum Begriff: Die dritte Art der Funktionsprüfung ist die „White Box“, von der alle internen Funktionen bekannt sind.

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 Levels	Tabelle K.1
AOPD	aktive optoelektronische Schutzeinrichtung (en: active optoelectronic protective device) (z. B. Lichtschranke)	Anhang H
B, 1, 2, 3, 4	Bezeichnung für die Kategorien	Tabelle 4
B_{10D}	Anzahl der Zyklen bis 10 % der Bauteile gefahrbringend ausgefallen sind (für Bauteile mit mechanischem Verschleiß)	Anhang C
Kat.	Kategorie	3.1.3
CC	Stromrichter (en: current converter)	Anhang I
CCF	Ausfall infolge gemeinsamer Ursache (en: common cause failure)	3.1.8
DC	Diagnosedeckungsgrad (en: diagnostic coverage)	3.1.31
DC_{avg}	durchschnittlicher Diagnosedeckungsgrad (en: average diagnostic coverage)	E.2
EMI	elektromagnetische Störung (en: electromagnetic interference)	6.2.2
ETA	Ereignisbaumanalyse (en: event tree analysis)	10.3.2
F, F1, F2	Häufigkeit und/oder Dauer der Gefährdungsexposition	A.2.2
FB	Funktionsblock (en: function block)	Anhang J
FVL	Programmiersprache mit nicht eingeschränktem Sprachumfang (en: full variability language)	3.1.40
FMEA	Fehlzustandsart- und -auswirkungsanalyse (en: failure modes and effects analysis)	6.1.5
FMECA	Ausfalleffekt- und Kritizitätsanalyse (en: failure modes, effects and critically analysis)	10.3.2
FTA	Fehlerbaumanalyse (en: fault tree analysis)	10.3.2
F(t)	kumulative Verteilungsfunktion	C.4.3
HFT	Hardware-Fehlertoleranz (en: hardware fault tolerance)	6.1
I, I1, I2	Eingabegerät, z. B. Sensor	6.1
i, j	Index für Zählung	Anhang D

Symbol oder Abkürzung	Beschreibung	Definition oder Fundort
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 (en: limited variability language)	3.1.38
λ_D	gefährbringende Ausfallrate eines Bauteils	Anhang C
M	Motor	Anhang I
MTTF	mittlere Dauer bis zum Ausfall	Anhang C
MTTF _D	mittlere Dauer bis zum gefährbringenden Ausfall	3.1.28
$n, N, \tilde{N}$	Anzahl von Einheiten	6.2, D.1
N_{niedrig}	Anzahl von Teilsystemen mit PL_{niedrig} in einer Kombination von Teilsystemen	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 (en: programmable electronic 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
SPS	speicherprogrammierbare Steuerung	Anhang I
PL_{niedrig}	niedrigster Performance Level eines Teilsystems in einer Kombination von Teilsystemen	6.2
PL_r	erforderlicher Performance Level	3.1.27
r_d	Anforderungsrate	3.1.35
r_t	Testrate	3.1.34
RDF	gefährliche Ausfallrate (en: ratio of dangerous failures)	C.4.2
RS	Drehgeber (en: rotation sensor)	Anhang I
S, S1, S2	Schwere der Verletzung	A.2.1
SB	Teilsystem	Bild 13, Bild H.1, Bild H.2
SOS	sicherer Betriebshalt	5.2.3.1
SS2	sicherer Stopp 2	5.2.3.1
SW1A, SW1B, SW2	Positionsschalter	Anhang I
SIL	Sicherheits-Integritätslevel	3.1.38, Abschnitt 6

Symbol oder Abkürzung	Beschreibung	Definition oder Fundort
SLS	sicher begrenzte Geschwindigkeit	Tabelle 3
SRASW	sicherheitsbezogene Anwendungssoftware	3.1.40
SRESW	sicherheitsbezogene Embedded-Software (en: safety-related embedded software)	3.1.41
SRP	sicherheitsbezogenes Teil (en: safety-related part)	Allgemeines
SRP/CS	sicherheitsbezogenes Teil einer Steuerung (en: safety-related part of a control system)	3.1.1
SRS	Spezifikation der Sicherheitsanforderungen (en: safety requirements specification)	3.1.2
STO	sicher abgeschaltetes Drehmoment (en: safe torque off)	Tabelle 3 und N.2
TE	Testeinrichtung (en: test equipment)	6.1
T_M	Gebrauchsdauer	3.1.33
T_{10D}	mittlere Zeit bis 10 % der Bauteile gefährlich ausfallen	Anhang C

4 Überblick

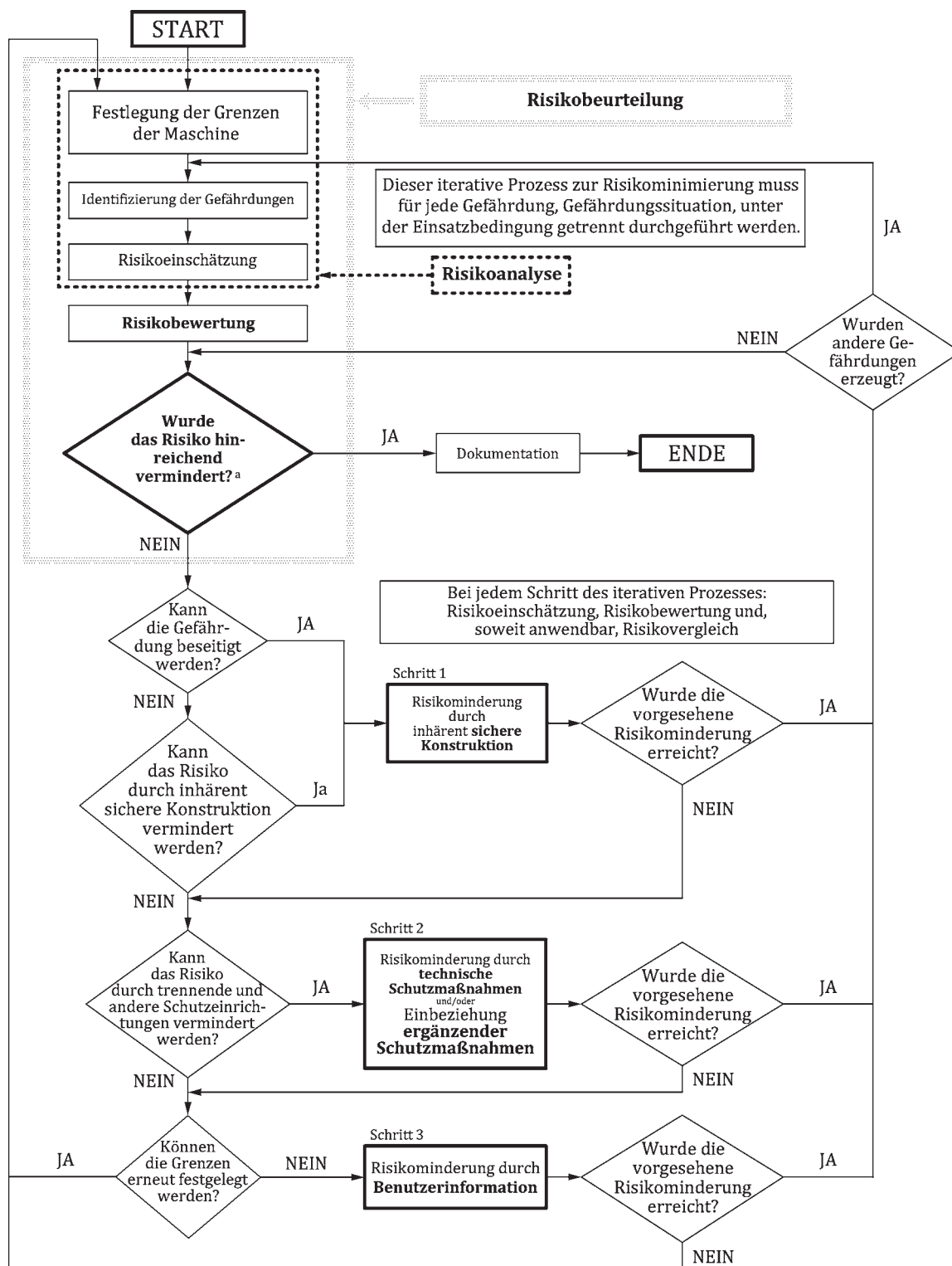
4.1 Prozess zur Risikobeurteilung und Risikominderung an der Maschine

Der Prozess zur Risikobeurteilung und Risikominderung wird in ISO 12100:2010 definiert und ist in Bild 2 dargestellt. ISO 13849-1 hat einen festen Platz im Prozess zur Risikominderung, wenn eine Sicherheitsfunktion und deren zugehöriges SRP/CS verwendet werden, um die Risikominderung durchzuführen.

ANMERKUNG Für weitere Informationen siehe ISO/TR 22100-2:2013.

Bei der Spezifikation der Sicherheitsanforderungen und dem Entwurf des SRP/CS muss das Ergebnis der Risikobeurteilung berücksichtigt werden, einschließlich der bestimmungsgemäßen Verwendung und der vernünftigerweise vorhersehbaren Fehlanwendung der Maschine (siehe Bild 1 und Bild 2).

ANMERKUNG Dieses Dokument gilt nicht für Teile der Maschinensteuerung, die nicht sicherheitsbezogen sind (siehe Bild 6).



Legende

- ^a Beim erstmaligen Stellen der Frage wird diese mit dem Ergebnis der Ausgangsrisikobeurteilung beantwortet.
- Risikominderung durch technische Schutzmaßnahmen darf durch die SRP/CS erfolgen, die Sicherheitsfunktionen ausführen. In diesem Fall, dieses Dokument.

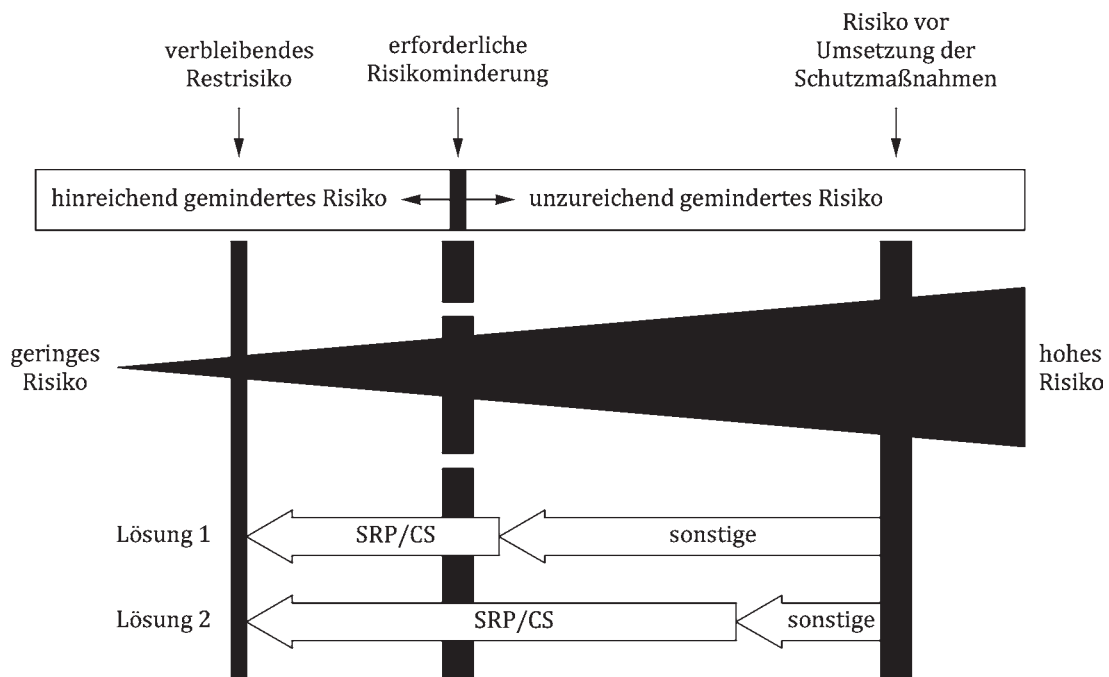
Bild 2 — Schematische Darstellung des Prozesses zur Risikominderung einschließlich des dreistufigen iterativen Prozesses nach ISO 12100:2010

ANMERKUNG In besonderen Fällen gilt dieses Dokument auch für Schritt 3 von Bild 2. Für Beispiele siehe Anhang M für Anzeigen und Alarme.

4.2 Beitrag zur Risikominderung

Nach der Risikobeurteilung muss der Konstrukteur entscheiden, welcher Beitrag zur Risikominderung von jeder relevanten Sicherheitsfunktion benötigt wird, die vom SRP/CS ausgeführt wird. Dieser Beitrag deckt das durch die Anwendung jeder einzelnen Sicherheitsfunktion reduzierte Risiko ab (siehe Bild 3), das durch andere Maßnahmen als SRP/CS erreicht werden kann. Er bezieht sich nicht auf das Gesamtrisiko der gesteuerten Maschine.

BEISPIEL Die Sicherheits-Stoppfunktion einer Presse, die mithilfe einer berührungslos wirkenden Schutzeinrichtung ausgelöst wird, oder die Sicherheitsfunktion zur Verriegelung der Tür einer Waschmaschine usw.



Legende

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 (z. B. Lichtschranke).

Lösung 2 Ein wesentlicher Teil der Risikominderung erfolgt durch ein SRP/CS, ein kleiner Beitrag zur Risikominderung erfolgt durch andere Schutzmaßnahmen als durch ein SRP/CS.

ANMERKUNG Für weitere Informationen zur Risikominderung siehe ISO 12100:2010.

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

4.3 Entwurfsprozess eines SRP/CS

Bild 4 zeigt den Entwurfsprozess eines SRP/CS sowie den Prozess zur Bestimmung, ob das SRP/CS die geplante Risikominderung erzielt.

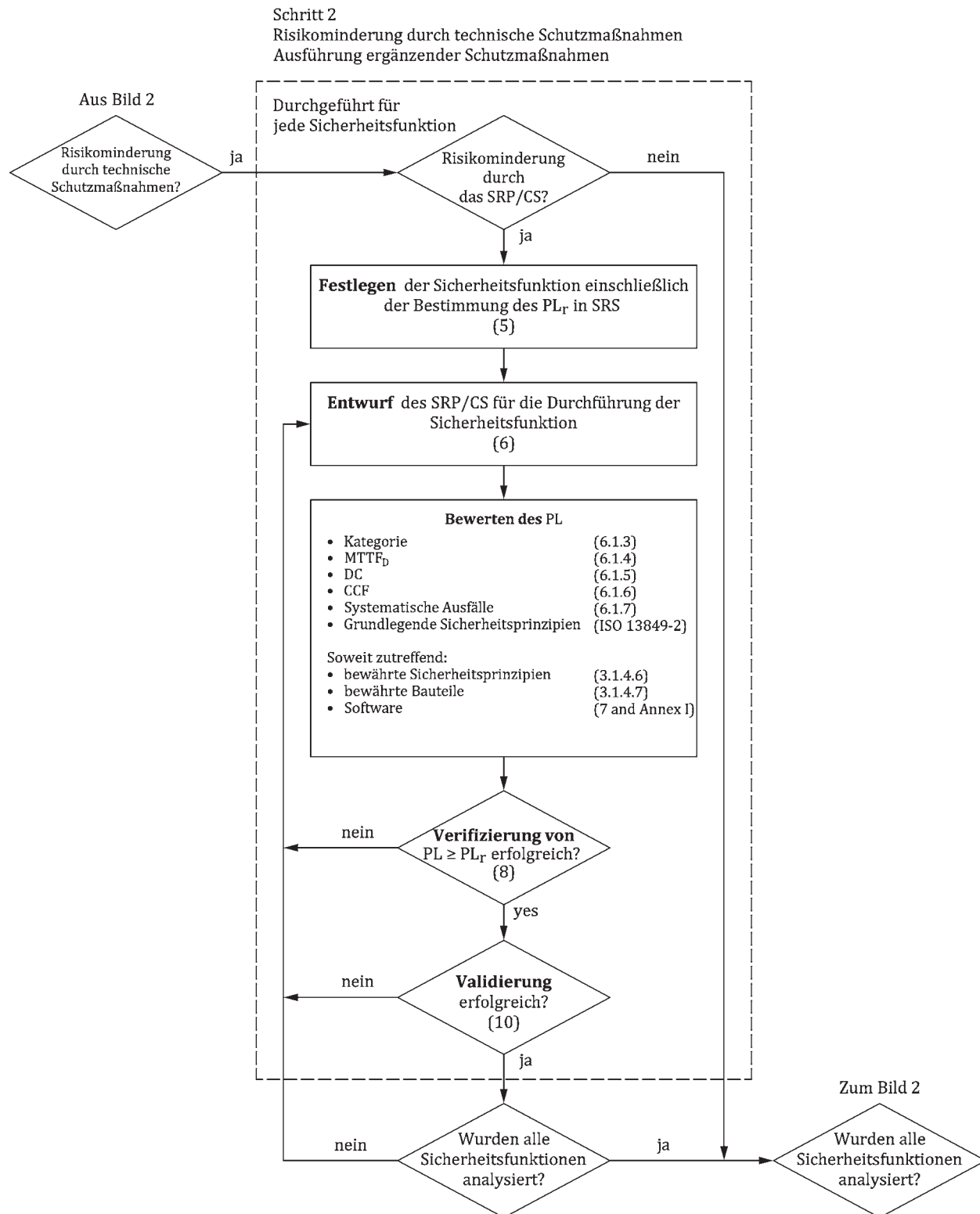


Bild 4 — Iterativer Prozess für den Entwurf von sicherheitsbezogenen Teilen von Steuerungen

4.4 Verfahren

Dieses Dokument beschreibt das folgende Verfahren:

- 1) Spezifikation der Sicherheitsfunktionen (Abschnitt 5);

- 2) Entwurf und technische Umsetzung der Sicherheitsfunktionen einschließlich der Identifizierung der SRP/CS und deren Teilsysteme, die alle Sicherheitsfunktionen ausführen;
 - a) Entwurfsaspekte (Abschnitt 6);
 - b) Software-Sicherheitsanforderungen (Abschnitt 7);
- 3) Verifizieren, ob der erreichte PL dem PL_r entspricht (Abschnitt 8);
- 4) ergonomische Entwurfsaspekte (Abschnitt 9);
- 5) Validierung (Abschnitt 10 oder ISO 13849-2);
- 6) Instandhaltung (Abschnitt 11);
- 7) technische Dokumentation (Abschnitt 12);
- 8) Benutzerinformation (Abschnitt 13).

Der erforderliche Performance Level bezieht sich auf die von der Sicherheitsfunktion zu erbringende Risikominderung. Je höher der Beitrag zur erforderlichen Risikominderung ist, desto höher muss die erforderliche Sicherheitsleistung sein. Die Performance Levels werden im Hinblick auf die durchschnittliche Wahrscheinlichkeit eines gefahrbringenden Ausfalls der Sicherheitsfunktion je Stunde definiert. Es gibt fünf Performance Level, angefangen von PL a für einen geringen Beitrag zur Risikominderung, bis hin zu PL e für einen hohen Beitrag zur Risikominderung. Die Bereiche der Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde sind in Tabelle 2 definiert.

Tabelle 2 — Performance Levels

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	$PFH_D < 10^{-7}$

ANMERKUNG 1 Es wird davon ausgegangen, dass der PFH_D -Wert mit dem PFH nach IEC 61508 identisch ist.

Teilsysteme (siehe 5.5) müssen mit dem gleichen Prozess wie für SRP/CS-Systeme nach Abschnitt 5 bis Abschnitt 13 bewertet werden. Für jede Sicherheitsfunktion muss der erreichte Performance Level dem erforderlichen Performance Level (PL_r) entsprechen oder ihn überschreiten.

4.5 Erforderliche Informationen

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

- die Ergebnisse der Risikobeurteilung der Maschine oder eines Teils davon;

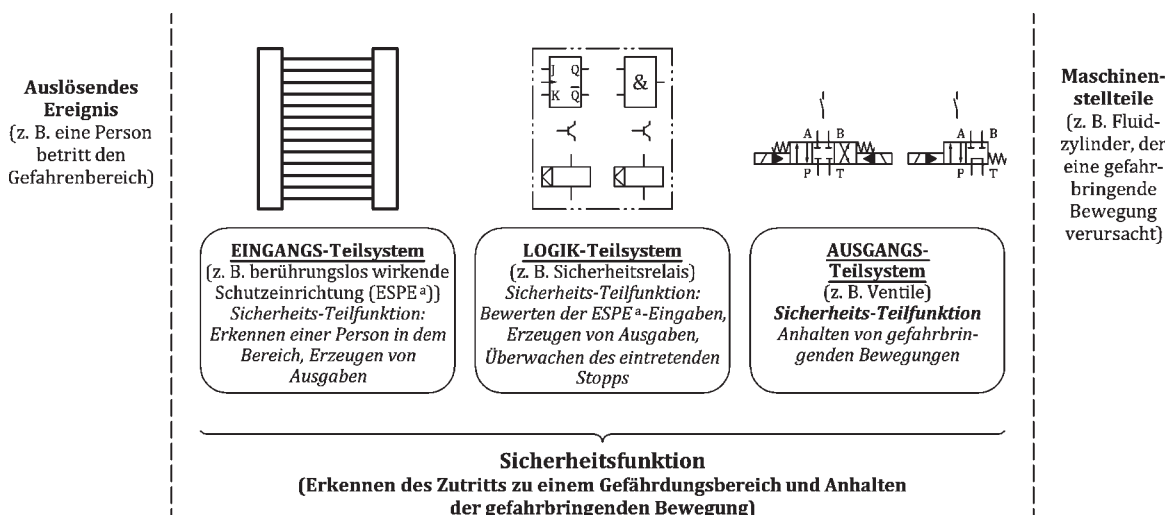
- Informationen über alle Sicherheitsfunktionen (siehe Abschnitt 5), die für den Prozess zur Risikominderung bei jeder Gefährdung als notwendig ermittelt wurden. Dazu gehört:
 - eine ausführliche Beschreibung jeder Sicherheitsfunktion (siehe 5.2);
 - die Bestimmung des erforderlichen Performance Levels (PL_r) für jede Sicherheitsfunktion (siehe 6.3).

ANMERKUNG Diese Informationen sind bereits in den zutreffenden Typ-C-Normen enthalten.

4.6 Ausführung von Sicherheitsfunktionen mithilfe von Teilsystemen

Die Ausführung einer Sicherheitsfunktion darf erfolgen:

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



^a berührungslos wirkende Schutzeinrichtung (BWS)

Bild 5 — Beispiel für eine Kombination von Teilsystemen

5 Spezifikation der Sicherheitsfunktionen

5.1 Identifizierung und allgemeine Beschreibung der Sicherheitsfunktion

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 ermitteln, 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, 6.2.11, erfolgen und einen Teil der Entwurfsspezifikation für das SRP/CS nach diesem Dokument darstellen.

Abschnitt 5 behandelt die folgenden Schritte:

- 1) allgemeine Beschreibung der Sicherheitsfunktion (Verknüpfung der Gefährdungen mit den Sicherheitsfunktionen);
- 2) ausführliche Beschreibung der Sicherheitsanforderungen (siehe 5.2);
- 3) Bestimmung des PL_r für jede Sicherheitsfunktion, d. h. wie zuverlässig die Sicherheitsfunktion sein muss, siehe 5.3;
- 4) 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 nach ISO 12100:2010 durchgeführt wurde.

5.2 Spezifikation der Sicherheitsanforderungen

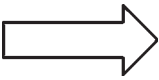
5.2.1 Allgemeine Anforderungen

5.2.1.1 Allgemeines

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

Die Spezifikation der Sicherheitsanforderungen ist dafür vorgesehen, Fehler beim Übergang vom Risiko-bewertungs- und -minderungsprozess nach ISO 12100:2010 zum SRP/CS-Entwurfs- und -Bewertungsprozess nach diesem Dokument zu verhindern, 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 13849-1

Erforderliche Informationen für das Erstellen der SRS (siehe 5.2.1.2)	Umwandlung	Beispiele für die Festlegung der Sicherheitsfunktionen in der SRS (siehe 5.2.1.3)
<ul style="list-style-type: none"> — Ergebnisse der Risikobeurteilung der Maschine oder eines Teils davon, 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> <ol style="list-style-type: none"> 1) Verriegelungsfunktion <ul style="list-style-type: none"> — Betriebsart (alle) — Auslösung durch: Öffnen einer beweglichen trennenden Schutzeinrichtung — sicherheitsbezogene Reaktion: sicher abgeschaltetes Drehmoment (STO) aller Bewegungen — PL_{Td} — Ansprechzeit — usw. 2) sicher begrenzte Geschwindigkeit (SLS: en: safely limited speed) <ul style="list-style-type: none"> — Betriebsart (manuell) — Auslösung durch: Geschwindigkeit, welche die festgelegte Geschwindigkeitsgrenze überschreitet — sicherheitsbezogene Reaktion: sicher abgeschaltetes Drehmoment (STO) aller Bewegungen — PL_{rc} — Ansprechzeit — usw.

5.2.1.2 Notwendige Informationen für die Erstellung der Spezifikation der Sicherheitsanforderungen

ANMERKUNG Die folgenden Informationen werden für die technische Dokumentation verwendet. Für die Informationen für den Benutzer siehe 13.3.

Die folgenden Informationen, soweit maßgebend, müssen dem Konstrukteur der sicherheitsbezogenen Steuerung zur Verfügung stehen, um die Spezifikation der Sicherheitsanforderungen zu erstellen:

- a) Ergebnisse der Risikobeurteilung der Maschine oder eines Teils davon 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, einschließlich:
 - 1) der bestimmungsgemäßen Verwendung der Maschine;
 - 2) der vernünftigerweise vorhersehbaren Fehlanwendung;
 - 3) des Einflusses von überlagerten Gefährdungen;

- 4) der Betriebsarten (z. B. lokale Betriebsart, Automatikbetrieb, Betrieb mit Bezug zu einem Bereich oder Teil der Maschine);
- 5) der/den Betriebsart(en), während der/denen die Sicherheitsfunktion aktiviert sein muss;
- 6) der Zyklusdauer; und
- 7) der Ansprechzeit bis ein sicherer Zustand erreicht ist (siehe auch ISO 13855:2010, 5.1);

ANMERKUNG 1 Die Ansprechzeit der Steuerung ist Teil der Gesamt-Ansprechzeit der Maschine. Die erforderliche Gesamt-Ansprechzeit der Maschine kann den Entwurf 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 (IEC 60204-1:2016, Anhang E);
- d) Beschreibung der Wechselwirkung verschiedener Arbeitsprozesse und manueller Aktionen (z. B. Instandsetzen, Einrichten, Reinigen, Fehlersuche, Betriebsarten mit deaktivierten Schutzeinrichtungen);
- e) ergonomische Aspekte zum Minimieren einer fehlerhaften Bedienung oder Umgehung;
- f) Anwendungsgrenzen in Zusammenhang mit den Umgebungsbedingungen;
- g) Einfluss von überlagerten Gefährdungen (siehe A.3).

5.2.1.3 Festlegung aller Sicherheitsfunktionen in der Spezifikation der Sicherheitsanforderungen

Die SRS muss im Verhältnis zur jeweiligen Anwendung die folgenden Informationen für jede Sicherheitsfunktion enthalten:

- a) die Kurzbeschreibung/Bezeichnung der Sicherheitsfunktion für eine klare Bezugnahme;
- b) das Ereignis, das die Sicherheitsfunktion auslöst;
- c) die Reaktion, die durch die Ausgabe(n) der Sicherheitsfunktion auszulösen ist, um den beabsichtigten sicheren Zustand zu erreichen;

BEISPIEL 1 Anhalten von gefahrbringenden Bewegungen.

- d) den erforderlichen Performance Level PL_r für jede Sicherheitsfunktion (siehe 5.3);
- e) 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 13855:2010;
- f) die Betriebsart(en), während der/denen die Sicherheitsfunktion aktiviert sein muss;
- g) Schnittstellen der Sicherheitsfunktionen;
- h) falls notwendig, im Falle einer Fehlererkennung in einem Funktionskanal, Verfahren, um die Maschine in einen sicheren Zustand zu bringen, einschließlich der Art und Weise, wie der sichere Zustand aufrechterhalten wird, bis der Fehler behoben ist;

BEISPIEL 2 Liegt ein Fehler in einem Funktionskanal vor und Stopp-Kategorie 1 ist nicht möglich, dann kann eine Reaktion auf einen Fehler ausgelöst werden, indem Stopp-Kategorie 0 verwendet wird. Für Stopp-Kategorien siehe IEC 60204-1.

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

ANMERKUNG Es kann notwendig sein, eine Vertikalachse aufrechtzuerhalten, um einen Sturz infolge Erdanziehungskräften zu verhindern. Wenn äußere Kräfte einen Einfluss auf die funktionale Sicherheit haben können, z. B. an solchen schwerkraftbelasteten Achsen, kann aufgrund systematischer Anforderungen eine Verstärkung (z. B. für Antriebselemente) notwendig sein. Geeignete Entwurfslösungen können der Einbau eines Rückschlagventils in Zylinder oder zusätzliche mechanische Bremsen sein. Das kann auch den Entwurf von zwei getrennten Sicherheitsfunktionen erfordern: eine, die mit Energie verfügbar ist und eine, die ohne Energie verfügbar ist.

- j) die Anforderungsrate der Sicherheitsfunktion und/oder die Betriebshäufigkeit des SRP/CS;
k) die Priorität der Sicherheitsfunktionen, die gleichzeitig aktiv sein können und dadurch zu Konflikten führen können;

BEISPIEL 3 Eine Not-Halt-Funktion hat Vorrang vor allen anderen Funktionen.

BEISPIEL 4 Die Funktion der sicher begrenzten Geschwindigkeit (SLS) kann eine Voraussetzung für die Sicherheitsfunktion „mit selbsttätiger Rückstellung“ sein.

- l) Sicherheitsanforderungen in Typ-C-Normen für den Entwurf eines SRP/CS oder eines Teilsystems (z. B. ISO 23125:2015, ISO 16090-1:2017).

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

Siehe auch Anhang M für typische Sicherheitsfunktionen und deren Eigenschaften und sicherheitsbezogenen Parameter.

5.2.2 Anforderungen an spezifische Sicherheitsfunktionen

5.2.2.1 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 muss Vorrang vor allen maßgebenden Startfunktionen und nicht sicherheitsbezogenen Stopp-Funktionen haben. Wenn eine Gruppe von Maschinen koordiniert zusammenarbeitet, müssen Vorkehrungen getroffen werden, um der übergeordneten Steuerung und/oder den anderen Maschinen eine solche Stopp-Bedingung zu signalisieren.

Als Ergebnis der Risikobeurteilung können sicherheitsbezogene Stopp-Funktionen entsprechend den Stopp-Kategorien von IEC 60204-1:2016, 9.2.2, ausgeführt werden.

ANMERKUNG IEC 61800-5-2:2016 enthält Informationen über sicherheitsbezogene Antriebssysteme einschließlich einer Beschreibung des sicher abgeschalteten Drehmoments (STO), des sicheren Stopps 1 (SS1), des sicheren Stopps 2 (SS2) und des sicheren Betriebshalts (SOS, en: safe operating stop).

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

5.2.2.2 Manuelle Rückstellfunktion

Die Wiederherstellung der Sicherheitsfunktion durch die Rückstellung der Schutzeinrichtung hebt den Stopp-Befehl auf. Wenn dies in der Risikobeurteilung angegeben ist, 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, bereitgestellt werden;
- darf nur dann ausgeführt werden, wenn alle davon beeinflussten Sicherheitsfunktionen und Schutzeinrichtungen funktionsfähig sind;
- darf selbst keine Gefährdungssituation einleiten;
- muss durch eine beabsichtigte Handlung ausgelöst werden;
- muss der Steuerung ermöglichen, einen separaten Start-Befehl anzunehmen; und
- muss von einer überwachten Signaländerung akzeptiert werden, um eine vorhersehbare Fehlanwendung zu vermeiden.

Wenn die Funktion „manuelle Rückstellung“ eine Sicherheitsfunktion ausführen muss (z. B. Verhindern eines unerwarteten Anlaufs), ist der erforderliche Performance Level zu bestimmen. Der PL der manuellen Rückstellfunktion kann sich vom PL_r der zugehörigen Sicherheitsfunktion unterscheiden.

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

Das Stellteil zum Rücksetzen muss außerhalb des Gefährdungsbereichs und an einer Stelle mit ausreichender Sicht angebracht werden, von der aus sichergestellt werden kann, dass sich keine Person im Gefährdungsbereich befindet. Es darf nicht möglich sein, die Rückstellfunktion von einer Stelle innerhalb des Gefährdungsbereichs zu aktivieren.

Wenn die Sicht auf den Gefährdungsbereich nicht ausreicht, muss ein spezifischer Ablauf für die Rückstellung vorhanden sein oder der nicht sichtbare Bereich muss überwacht werden.

BEISPIEL Eine Lösung ist die Durchführung der Rückstellung in einer bestimmten Reihenfolge. Die Rückstellfunktion wird innerhalb des Gefährdungsbereichs durch das erste Stellteil in Kombination mit einem zweiten Stellteil zum Rücksetzen außerhalb des Gefährdungsbereichs (nahe der Schutzeinrichtung) eingeleitet. Dieses Rückstellverfahren kann innerhalb einer begrenzten Zeit erfolgen, bevor die Steuerung einen separaten Start-Befehl akzeptiert. Die Überwachung des Bereichs kann beispielsweise durch Anwesenheitsmelder erfolgen, die Personen in Gefährdungsbereichen erkennen, die von der Stelle der Rückstellung aus nicht sichtbar sind.

Siehe auch Tabelle M.1.

5.2.2.3 Wiederanlauffunktion

Ein Wiederanlauf darf nur dann automatisch erfolgen, wenn der sichere Zustand sichergestellt ist. Insbesondere trifft ISO 12100:2010, 6.3.3.2.5, bei einer verriegelten trennenden Schutzeinrichtung mit Startfunktion zu.

Siehe auch Tabelle M.1.

Wird eine Maschine lokal gesteuert, z. B. durch einen tragbaren Steuerstand, der ein tragbares Gerät oder eine Hängebedienungs­tafel sein kann, müssen folgende Anforderungen erfüllt werden:

- Siehe auch Tabelle M.1.

Die Überbrückungsfunktion ist ein vorübergehendes automatisches Deaktivieren einer Sicherheitsfunktion durch die sicherheitsbezogene Steuerung einer Maschine. Sie kann ausgeführt 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 Überbrückungsfunktion 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 Überbrückungssensoren oder -signale dürfen keinen Überbrückungszustand bewirken.

Der Teil bzw. die Teile der Steuerung, der/die die Überbrückungsfunktion ausführt/ausführen, muss/müssen eine angemessene sicherheitsbezogene Leistung aufweisen (SIL nach IEC 62061 oder PL nach diesem Dokument) und darf/dürfen die sicherheitsbezogene Leistung der Schutzfunktion nicht unter die für die jeweilige Anwendung geforderte verringern.

Nach dem Überbrücken müssen alle davon beeinflussten Sicherheitsfunktionen wiederhergestellt werden und aktiv sein.

Die Ausführung der Überbrückungsfunktion muss den Anforderungen von IEC 62046:2018 entsprechen. Siehe auch Tabelle M.1.

5.2.2.6 Sicherheitsbezogene Parameter

Wenn sicherheitsbezogene Parameter, z. B. Position, Geschwindigkeit, Temperatur, Zeit, Drehmoment oder Druck, von geltenden Grenzwerten abweichen, muss die sicherheitsbezogene Steuerung geeignete Maßnahmen einleiten.

Wenn Abweichungen in manuell eingegebenen sicherheitsbezogenen Daten für programmierbare oder konfigurierbare elektronische Systeme zu Gefährdungssituationen führen können, sollte in der sicherheitsbezogenen Steuerung ein Datenkontrollsystem vorhanden sein, z. B. für die Kontrolle von Grenzwerten, Format und/oder Logik der Eingangswerte. Für ergänzende Anforderungen siehe 7.5 und siehe auch Tabelle M.2.

Anhang O enthält Informationen zu sicherheitsbezogenen Werten von Bauteilen oder Komponenten der Steuerungen.

5.2.2.7 Schwankungen, Verlust und Wiederkehr der Spannungsversorgung

Wenn Schwankungen im Energieniveau auftreten, die außerhalb des Betriebsbereichs liegen, einschließlich des Verlusts der Energieversorgung, muss das SRP/CS weiterhin Ausgangssignale bereitstellen oder einleiten, die den anderen Teilen der Maschine ermöglichen, den sicheren Zustand aufrechtzuerhalten. Siehe auch Tabelle M.2.

5.2.2.8 Anforderungen an die Betriebsartenwahl

Die Wahl der Betriebsart ist eine Sicherheitsfunktion, durch die (eine) Sicherheitsfunktion(en) freigegeben oder abgeschaltet wird/werden. 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;

ANMERKUNG Es reicht aus, wenn eine Betriebsart in der gesamten Sicherheitsfunktion identifiziert oder angezeigt werden kann.

- 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 die beabsichtigte Risikominderung zu verlieren.

Die Funktion der Betriebsartenwahl muss als Sicherheitsfunktion ausgeführt werden, wenn sie durch die Risikobeurteilung unter Berücksichtigung der systematischen Anforderungen a) bis c) erforderlich ist. Die Vorrichtungen für die Wahl der Betriebsart dürfen den PL der Sicherheitsfunktionen, die in dieser Betriebsart aktiv sind, nicht herabsetzen.

5.2.2.9 Sicherheitsfunktion(en) für Instandhaltungsaufgaben

Beim Entwurf der Maschine müssen die Instandhaltungsaufgaben berücksichtigt werden, die an der Maschine durchgeführt werden, und es müssen Sicherheitsfunktionen für diese Aufgaben vorgesehen werden. Die Ergebnisse der Risikobeurteilung für jede maßgebende Sicherheitsfunktion müssen in der Spezifikation des SRP/CS berücksichtigt werden.

ANMERKUNG 1 Zu den Instandhaltungsaufgaben können unter anderem folgende gehören:

- Einrichten;
- Einlernen (Teachen)/Programmieren;
- Umrüsten;
- Reinigung und Sauberhaltung;
- Desinfizieren;
- geplante oder ungeplante vorbeugende Instandhaltung oder Instandsetzung;
- Fehlersuche/Fehlerbehandlung;
- Fehlerdiagnose.

Einige Instandhaltungsaufgaben erfordern eine vollständige Trennung der Maschine von allen Energiequellen und sind daher nicht vom SRP/CS abhängig. Bei Instandhaltungsaufgaben, die Antriebs- und/oder Maschinenbewegungen erfordern, während sich das Instandhaltungspersonal im Gefährdungsbereich aufhält, und bei denen eine manuelle Aussetzung oder Überbrückung bestimmter Sicherheitsfunktionen erforderlich ist, darf dies nur durch Bereitstellung alternativer und geeigneter Sicherheitsfunktionen (z. B. Sicherheitsfunktion durch Zustimmungseinrichtung mit Sicherheitsfunktion durch Geschwindigkeitsbegrenzung) zulässig sein.

BEISPIEL Einlernen (Teachen)/Programmieren, Fehlersuche, Feinabstimmung des Prozesses sind Aufgaben, bei denen eine Antriebs- und Maschinenbewegung erforderlich ist.

Die folgenden Sicherheitsfunktionen sind Beispiele dafür, was häufig für Instandhaltungsaufgaben vorgesehen ist:

- a) Steuerung mit selbsttätiger Rückstellung;
- b) Steuerung mit Zustimmungseinrichtung;
- c) Überwachung oder Begrenzung der Geschwindigkeit, des Drehmoments, der Leistung, der Position, der Temperatur, der Stufe usw.;
- d) Verhindern des unerwarteten Anlaufs;
- e) Isolations- und Energieableitungsfunktion;
- f) mechanische Rückhaltung oder Einhausung.

ANMERKUNG 2 Siehe Anhang M für ergänzende Informationen.

Der Anreiz zum Übergehen bzw. Umgehen von risikomindernden Maßnahmen, die vom SRP/CS während der Instandhaltung der Maschine ausgeführt werden, muss bei der Spezifikation, beim Entwurf und bei der Auswahl des SRP/CS berücksichtigt werden (siehe 5.2.2.10).

Beim SRP/CS muss in Betracht gezogen werden, dass neben der/den vorgesehenen Bedienperson(en) weitere Personen eine Aufgabe durchführen, wie z. B.:

- ein Bediener führt Rückstell- und Wiederanlauffunktionen aus, während sich das Instandhaltungspersonal im Gefährdungsbereich aufhält;
- risikomindernde Maßnahmen, durch die eine Person geschützt werden soll, werden unangemessen für mehrere Personen eingesetzt.

In der Betriebsart für die Instandhaltung muss ein ferngesteuerter Zugriff (siehe 5.2.2.11) auf die Maschinensteuerung durch den Entwurf des SRP/CS verhindert werden, wenn keine angemessene Benachrichtigung oder Anzeige für Personen an der Maschine oder in deren Nähe vorhanden ist.

5.2.2.10 Anreiz zum Übergehen von Sicherheitsfunktionen

Der Anreiz zum Übergehen oder Umgehen einer Sicherheitsfunktion hängt vom Prozess, von der bestimmungsgemäßen Verwendung der Maschine (oder eines Teils der Maschine) und den Entwurfsdetails der risikomindernden Maßnahmen ab. Der Anreiz zum Übergehen einer Sicherheitsfunktion muss im Entwurf des SRP/CS auf ein Mindestmaß begrenzt werden.

ANMERKUNG 1 Mithilfe von Maßnahmen zur einfachen Durchführung von Aufgaben und dem gleichzeitigen Schutz der Bediener kann der Anreiz zum Übergehen oder Umgehen von Sicherheitsfunktionen und/oder Schutzeinrichtungen gemindert werden.

ANMERKUNG 2 ISO 14119 beschreibt ein Verfahren und enthält Beispiele, wie die Möglichkeiten zum Übergehen einer Verriegelungseinrichtung auf ein Mindestmaß verringert werden.

ANMERKUNG 3 Forschungsarbeiten zum Thema Sicherheit haben gezeigt, dass viele Verletzungen auf das Übergehen von Sicherheitsfunktionen und/oder Schutzeinrichtungen zurückzuführen sind. Siehe Literaturhinweise für ergänzende Informationen.

BEISPIEL Anreize zum Übergehen bzw. Umgehen einer risikomindernden Maßnahme (einschließlich Sicherheitsfunktion(en)) können sein:

- dass die risikomindernde Maßnahme verhindert, dass die Aufgabe ausgeführt wird; es besteht die Notwendigkeit, eine Aufgabe auszuführen, die hinsichtlich Gefährdungen und Risiken nicht identifiziert und bewertet wurde;
- die risikomindernde Maßnahme verlangsamt die Produktion oder stört andere Aktivitäten oder Präferenzen des Benutzers;
- die risikomindernde Maßnahme ist schwierig anzuwenden;
- die risikomindernde Maßnahme und/oder deren zugehörige Gefährdung wird/werden vom Personal nicht als solche erkannt;
- die risikomindernde Maßnahme wird nicht als geeignet, notwendig oder angemessen für ihre Funktion angesehen.

Die Verwendung von und der Zugriff auf speicherprogrammierbare Systeme bietet eine weitere Möglichkeit, um Sicherheitsfunktionen zu übergehen oder zu umgehen, wenn diese nicht ordnungsgemäß angewendet oder überwacht werden.

5.2.2.11 Fernzugriff

Ist eine Maschine für den Fernzugriff ausgelegt, muss das SRP/CS aktiviert bleiben. Alternative risikomindernde Maßnahmen können angewendet werden, wenn dies in den Benutzerinformationen angegeben ist.

Der Entwurf des SRP/CS darf den Fernzugriff auf eine Maschine nicht ohne besondere Maßnahmen zum Vermeiden von gefährlichen Situationen erlauben, die durch die Anwesenheit von Personen im Inneren oder in der Nähe der Maschine entstehen können.

ANMERKUNG Ein ferngesteuertes Anlaufen, das von den an der Maschine arbeitenden Personen nicht vorhergesehen wird, kann zu Verletzungen führen.

5.3 Bestimmung des erforderlichen Performance Levels für jede Sicherheitsfunktion

Für jede gewählte Sicherheitsfunktion muss ein erforderlicher Performance Level (PL_r) festgelegt und dokumentiert werden. Die Festlegung des PL_r muss auf dem Ergebnis der Risikobeurteilung der Maschine oder eines Teils davon basieren und muss in Zusammenhang mit der erforderlichen Risikominderung stehen (siehe Bild 3). Anhang A enthält einen Leitfaden für die Bestimmung des PL_r für die Sicherheitsfunktion. Überlagerte Gefährdungen, sofern maßgebend, müssen ebenfalls bei der Festlegung der Sicherheitsfunktionen berücksichtigt werden. Siehe A.3 für weitere Anleitungen.

ANMERKUNG 1 Andere Verfahren, wie beispielsweise das in IEC 62061 angegebene, können stattdessen angewendet werden.

ANMERKUNG 2 Typ-C-Normen enthalten üblicherweise Informationen zum PL_r.

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

ANMERKUNG 3 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 mit der Risikobeurteilung abgeglichen werden, bevor mit dem Entwurf 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. Siehe auch 10.4 für die Validierung der SRS.

ANMERKUNG Je nach spezifischen Sicherheitsfunktionen kann es hilfreich sein, die SRS von einer anderen Person überprüfen zu lassen als von der, die die SRS angefertigt hat.

5.5 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:

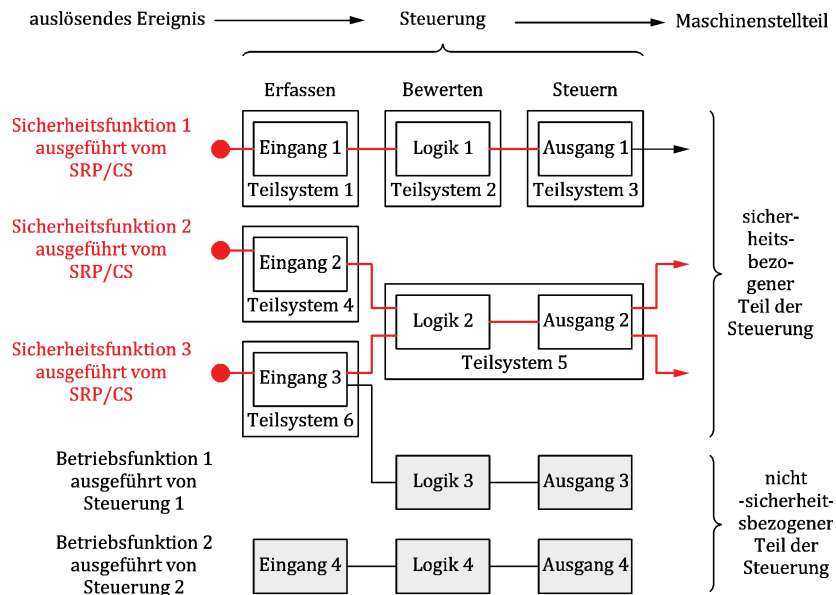
- die Sicherheitsanforderungen an jede Teilfunktion (Anforderungen an Funktion und Integrität); und
- Eingänge und Ausgänge jeder Teilfunktion.

Ein SRP/CS kann Folgendes umfassen:

- ein oder mehrere zuvor validierte(s) Teilsystem(e);
- ein oder mehrere Teilsystem(e) basierend auf (einem) Teilsystemelement(en);
- eine Kombination der beiden vorstehenden Optionen.

Ein gefahrbringender Ausfall eines beliebigen Teilsystems führt per Definition zum Verlust der gesamten Sicherheitsfunktion.

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 Schutteinrichtung, Unterbrechen eines Strahls der AOPD) und endet mit einem Ausgang, der eine sichere Reaktion eines ‚Maschinenstellteils‘ (z. B. Motor, Zylinder) bewirkt.



ANMERKUNG 1 Sicherheitsfunktion 1 wird in Teilfunktion 1, Teilfunktion 2 und Teilfunktion 3 zerlegt. Teilfunktion 1 wird von Teilsystem 1 ausgeführt.

ANMERKUNG 2 Sicherheitsfunktion 2 wird in Teilfunktion 4 und Teilfunktion 5 zerlegt. Teilfunktion 4 wird von Teilsystem 4 ausgeführt.

ANMERKUNG 3 Sicherheitsfunktion 3 wird in Teilfunktion 6 und Teilfunktion 5 zerlegt. Teilfunktion 6 wird von Teilsystem 6 ausgeführt.

Bild 6 — Beispiel für die Zerlegung von Sicherheitsfunktionen und deren Zuordnung zu den Teilsystemen

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

- auslösendem Ereignis (z. B. Öffnen einer trennenden Schutteinrichtung, Unterbrechen eines Strahls einer AOPD);
- 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, Bremsen) (Teilsysteme 3 und 5);
- Maschinenstellteil (z. B. Motor, Zylinder);
- Verbindungen (z. B. elektrisch, optisch).

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

ANMERKUNG 3 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 4 Der Konstrukteur eines zuvor validierten Teilsystems kann ein Systemintegrator, ein Maschinenhersteller oder ein Bauteilhersteller sein.

Der Hersteller eines zuvor validierten Teilsystems muss die einschlägigen Informationen nach 13.2 bereitstellen.

6 Entwurfsaspekte

6.1 Bewertung des erreichten Performance Levels

6.1.1 Allgemeine Übersicht der Performance Levels

Die Fähigkeit, 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, ob die geltenden qualitativen (nicht quantifizierbaren) Anforderungen der Kategorie erfüllt sind, einschließlich:
 - grundlegende Sicherheitsprinzipien (siehe ISO 13849-2:2012, Tabelle A.1, Tabelle B.1, Tabelle C.1 und Tabelle D.1);
 - bewährte Sicherheitsprinzipien (siehe ISO 13849-2:2012, Tabelle A.2, B.2, C.2 und D.2);
 - bewährte Bauteile (siehe ISO 13849-2:2012, 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 E);
- 4) des CCF (siehe 6.1.6 und Anhang F);
- 5) des Einflusses des Entwurfs 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).