

DIN EN ISO 13849-1



ICS 13.110

Ersatz für
DIN EN ISO 13849-1:2016-06

**Sicherheit von Maschinen –
Sicherheitsbezogene Teile von Steuerungen –
Teil 1: Allgemeine Gestaltungsleitsätze (ISO 13849-1:2023);
Deutsche Fassung EN ISO 13849-1:2023**

Safety of machinery –
Safety-related parts of control systems –
Part 1: General principles for design (ISO 13849-1:2023);
German version EN ISO 13849-1:2023

Sécurité des machines –
Parties des systèmes de commande relatives à la sécurité –
Partie 1: Principes généraux de conception (ISO 13849-1:2023);
Version allemande EN ISO 13849-1:2023

Gesamtumfang 190 Seiten

DIN-Normenausschuss Sicherheitstechnische Grundsätze (NASG)

Nationales Vorwort

Dieses Dokument (EN ISO 13849-1:2023) 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).

Information zur Verwendung englischer Fachbegriffe

Der englische Begriff „tool“ wurde im Abschnitt 7 durchgängig auch im deutschen Text verwendet. Der Abschnitt 7 beschreibt Softwaresicherheitsanforderungen. Im Kontext mit Software ist die Verwendung der deutschen Übersetzung „Werkzeug“ nicht üblich. Ergänzend wurde im Anhang N, welcher Beispiele für die Umsetzung der Anforderungen aus Abschnitt 7 beschreibt, ebenfalls der englische Begriff beibehalten.

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

IEC 60204-1:2016+AMD1:2021	siehe	DIN EN 60204-1 (VDE 0113-1):2019-06
IEC 60447	siehe	DIN EN 60447 (VDE 0196)
IEC 60529	siehe	DIN EN 60529 (VDE 0470-1)
IEC 60812	siehe	DIN EN 60812
IEC 60947 (all parts)	siehe	DIN EN (IEC) 60947 (VDE 0660) (alle Teile)
IEC 61000-1-2	siehe	DIN EN 61000-1-2
IEC 61000-6-2	siehe	DIN EN IEC 61000-6-2
IEC 61000-6-7:2014	siehe	DIN EN 61000-6-7 (VDE 0839-6-7):2015-12
IEC 61025	siehe	DIN EN 61025
IEC 61078	siehe	DIN EN 61078
IEC 61131-3:2013	siehe	DIN EN 61131-3:2014-06
IEC 61300 (all parts)	siehe	DIN EN (IEC) 61300 (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	siehe	DIN EN 61326-3-1 (VDE 0843-20-3-1)
IEC 61496-1:2020	siehe	DIN EN IEC 61496-1 (VDE 0113-201):2021-06
IEC 61496-2	siehe	DIN EN IEC 61496-2 (VDE 0113-202)
IEC 61496-3	siehe	DIN EN IEC 61496-3 (VDE 0113-203)
IEC 61508-1	siehe	DIN EN 61508-1 (VDE 0803-1)
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	siehe	DIN EN 61508-5 (VDE 0803-5)

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 61511-1:2016	siehe	DIN EN 61511-1 (VDE 0810-1):2019-02
IEC 61558-2-16	siehe	DIN EN 61558-2-16 (VDE 0570-2-16)
IEC 61709	siehe	DIN EN 61709
IEC 61784 (all parts)	siehe	DIN EN IEC 61784 (alle Teile)
IEC 61800-3	siehe	DIN EN IEC 61800-3 (VDE 0160-103)
IEC 61800-5-2:2016	siehe	DIN EN 61800-5-2 (VDE 0160-105-2):2017-11
IEC 61810-2-1	siehe	DIN EN 61810-2-1 (VDE 0435-120-1)
IEC 61810-3	siehe	DIN EN 61810-3 (VDE 0435-2022)
IEC 62021 (all parts)	siehe	DIN EN 62021 (alle Teile)
IEC 62024 (all parts)	siehe	DIN EN IEC 62024 (alle Teile)
IEC 62046:2018	siehe	DIN EN IEC 62046 (VDE 0113-211):2019-03
IEC 62061:2021	siehe	DIN EN IEC 62061 (VDE 0113-50):2023-02
IEC 62368-1	siehe	DIN EN IEC 62368-1 (VDE 0868-1)
IEC 62502	siehe	DIN EN 62502 (VDE 0050-3)
IEC/IEEE 82079-1:2019	siehe	DIN EN IEC/IEEE 82079-1 (VDE 0039-1):2021-09
IEC/TR 63074	siehe	DIN IEC/TR 63074 (VDE 0113-74)
ISO 4413:2010	siehe	DIN EN ISO 4413:2011-04
ISO 4414:2010	siehe	DIN EN ISO 4414:2011-04
ISO 7731:2003	siehe	DIN EN ISO 7731:2008-12
ISO 9000:2015	siehe	DIN EN ISO 9000:2015-11
ISO 9001:2015	siehe	DIN EN ISO 9001:2015-11
ISO 9241-210	siehe	DIN EN ISO 9241-210
ISO 10218-1:2011	siehe	DIN EN ISO 10218-1:2012-01
ISO 10218-2	siehe	DIN EN ISO 10218-2
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	siehe	DIN EN ISO 13851
ISO 13855:2010	siehe	DIN EN ISO 13855:2010-10
ISO 13856-1	siehe	DIN EN ISO 13856-1
ISO 13856-2	siehe	DIN EN ISO 13856-2
ISO 14118:2017	siehe	DIN EN ISO 14118:2018-07
ISO 14119:2013	siehe	DIN EN ISO 14119:2014-03
ISO 16090-1	siehe	DIN EN ISO 16090-1
ISO 20607:2019	siehe	DIN EN ISO 20607:2019-10
ISO 23125	siehe	DIN EN ISO 23125

ISO/TR 14121-2	siehe	DIN ISO/TR 14121-2 (DIN SPEC 33885)
ISO/TR 22100-2:2013	siehe	DIN ISO/TR 22100-2 (DIN SPEC 33887):2014-09
ISO/TR 22100-3	siehe	DIN ISO/TR 22100-3 (DIN SPEC 33888)
ISO/TR 22100-4	siehe	DIN CEN ISO/TR 22100-4
ISO/TS 15066:2016	siehe	DIN ISO/TS 15066 (DIN SPEC 5306):2017-04

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

Änderungen

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

- a) das gesamte Dokument wurde neu strukturiert, um den Entwurfs- und Entwicklungsprozess für Steuerungen besser nachvollziehen zu können;
- b) ein neuer Abschnitt 4 mit Empfehlungen für die Risikobeurteilung;
- c) Spezifikation der Sicherheitsfunktionen (aktualisierter Abschnitt 5);
- d) Kombination von verschiedenen Teilsystemen (aktualisiert in Abschnitt 6);
- e) ein neuer Abschnitt 7 mit Software-Sicherheitsanforderungen;
- f) ein neuer Abschnitt 9 zu ergonomischen Entwurfsaspekten;
- g) Validierung (Abschnitt 8 aktualisiert und nach Abschnitt 10 verschoben);
- h) ein neuer Abschnitt G.5 zum Management der funktionalen Sicherheit;
- i) ein neuer Anhang L zur elektromagnetischen Störfestigkeit (EMI, en: electromagnetic interference);
- j) ein neuer Anhang M mit zusätzlichen Informationen zur Spezifikation der Sicherheitsanforderungen;
- k) ein neuer Anhang N zu den Maßnahmen zur Fehlervermeidung für das sicherheitsrelevante Softwaredesign;
- l) ein neuer Anhang O mit sicherheitsbezogenen Werten von Bauteilen oder Komponenten der Steuerungen.

Frühere Ausgaben

DIN EN 954-1: 1997-03
DIN EN 954-1 Beiblatt 1: 2000-01
DIN EN ISO 13849-1: 2007-02, 2007-07, 2008-12, 2016-06

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

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

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

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

DIN EN (IEC) 60947 (VDE 0660) (alle Teile), *Niederspannungsschaltgeräte*

DIN EN 61000-1-2, *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*

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 61025, *Fehlzustandsbaumanalyse*

DIN EN 61078, *Zuverlässigkeitsblockdiagramme*

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

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), *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*

DIN EN 61508-1 (VDE 0803-1), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 1: Allgemeine Anforderungen*

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

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 61511-1 (VDE 0810-1):2019-02, *Funktionale Sicherheit — PLT-Sicherheitseinrichtungen für die Prozessindustrie — Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Hardware und Anwendungsprogrammierung (IEC 61511-1:2016 + COR1:2016 + A1:2017); Deutsche Fassung EN 61511-1:2017 + A1:2017*

DIN EN 61709, *Elektrische Bauelemente — Zuverlässigkeit — Referenzbedingungen für Ausfallraten und Beanspruchungsmodelle zur Umrechnung*

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 61810-2-1 (VDE 0435-120-1), *Elektromechanische Elementarrelais — Teil 2-1: Funktionsfähigkeit (Zuverlässigkeit) — Verfahren zum Nachweis der B_{10} -Werte*

DIN EN 61810-3 (VDE 0435-2022), *Elektromechanische Elementarrelais — Teil 3: Relais mit (mechanisch) zwangsgeführten Kontakten*

DIN EN 62021 (alle Teile), *Isolierflüssigkeiten — Bestimmung des Säuregehaltes*

DIN EN 62502 (VDE 0050-3), *Verfahren zur Analyse der Zuverlässigkeit — Ereignisbaumanalyse*

DIN EN IEC 61000-6-2, *Elektromagnetische Verträglichkeit (EMV) — Teil 6-2: Fachgrundnormen — Störfestigkeit für Industriebereiche*

DIN EN (IEC) 61300 (VDE 0885-300) (alle Teile), *Lichtwellenleiter — Verbindungselemente und passive Bauteile — Grundlegende Prüf- und Messverfahren*

DIN EN IEC 61496-1 (VDE 0113-201):2021-06, *Sicherheit von Maschinen — Berührungslos wirkende Schutzeinrichtungen — Teil 1: Allgemeine Anforderungen und Prüfungen (IEC 61496-1:2020); Deutsche Fassung EN IEC 61496-1:2020*

DIN EN IEC 61496-2 (VDE 0113-202), *Sicherheit von Maschinen — Berührungslos wirkende Schutzeinrichtungen — Teil 2: Besondere Anforderungen an Einrichtungen, die aktive optoelektronische Schutzeinrichtungen (AOPD) verwenden*

DIN EN IEC 61496-3 (VDE 0113-203), *Sicherheit von Maschinen — Berührungslos wirkende Schutzeinrichtungen — Teil 3: Besondere Anforderungen an aktive optoelektronische diffuse Reflexion nutzende Schutzeinrichtungen (AOPDDR)*

DIN EN 61558-2-16 (VDE 0570-2-16), *Sicherheit von Transformatoren, Drosseln, Netzgeräten und entsprechenden Kombinationen — Teil 2-16: Besondere Anforderungen und Prüfungen für Schaltnetzteile und Transformatoren für Schaltnetzteile für allgemeine Anwendungen*

DIN EN IEC 61784 (alle Teile), *Industrielle Kommunikationsnetze — Profile*

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

DIN EN IEC 62024 (alle Teile), *Induktive Hochfrequenz-Bauelemente — Elektrische Eigenschaften und Messmethoden*

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

DIN EN IEC 62061 (VDE 0113-50):2023-02, *Sicherheit von Maschinen — Funktionale Sicherheit sicherheitsbezogener Steuerungssysteme (IEC 62061:2021); Deutsche Fassung EN IEC 62061:2021*

DIN EN IEC 62368-1 (VDE 0868-1), *Einrichtungen für Audio/Video-, Informations- und Kommunikationstechnik — Teil 1: Sicherheitsanforderungen*

DIN EN IEC/IEEE 82079-1 (VDE 0039-1):2021-09, *Erstellung von Nutzungsinformationen (Gebrauchsanleitungen) für Produkte — Teil 1: Grundsätze und allgemeine Anforderungen (IEC/IEEE 82079-1:2019); Deutsche Fassung EN IEC/IEEE 82079-1:2020*

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 7731:2008-12, *Ergonomie — Gefahrensignale für öffentliche Bereiche und Arbeitsstätten — Akustische Gefahrensignale (ISO 7731:2003); Deutsche Fassung EN ISO 7731:2008*

DIN EN ISO 9000:2015-11, *Qualitätsmanagementsysteme — Grundlagen und Begriffe (ISO 9000:2015); Deutsche und Englische Fassung EN ISO 9000:2015*

DIN EN ISO 9001:2015-11, *Qualitätsmanagementsysteme — Anforderungen (ISO 9001:2015); Deutsche und Englische Fassung EN ISO 9001:2015*

DIN EN ISO 9241-210, *Ergonomie der Mensch-System-Interaktion — Teil 210: Menschzentrierte Gestaltung interaktiver Systeme*

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, *Industrieroboter — Sicherheitsanforderungen — Teil 2: Robotersysteme und Integration*

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, *Sicherheit von Maschinen — Zweihandschaltungen — Funktionelle Aspekte und Gestaltungsleitsätze*

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

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

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

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, *Werkzeugmaschinen-Sicherheit — Bearbeitungszentren, Fräsmaschinen, Transfermaschinen — Teil 1: Sicherheitsanforderungen*

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, *Werkzeugmaschinen — Sicherheit — Drehmaschinen*

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

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 22100-3 (DIN SPEC 33888), *Sicherheit von Maschinen — Beziehung zu ISO 12100 — Teil 3: Implementierung ergonomischer Grundsätze in Sicherheitsnormen*

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

DIN ISO/TS 15066 (DIN SPEC 5306):2017-04, *Roboter und Robotikgeräte — Kollaborierende Roboter (ISO/TS 15066:2016)*

Deutsche Fassung

Sicherheit von Maschinen —
Sicherheitsbezogene Teile von Steuerungen —
Teil 1: Allgemeine Gestaltungsleitsätze (ISO 13849-1:2023)

Safety of machinery —
Safety-related parts of control systems —
Part 1: General principles for design
(ISO 13849-1:2023)

Sécurité des machines —
Parties des systèmes de commande
relatives à la sécurité —
Partie 1: Principes généraux de conception
(ISO 13849-1:2023)

Diese Europäische Norm wurde vom CEN am 3. März 2023 angenommen.

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

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

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



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

CEN-CENELEC Management-Zentrum: Rue de la Science 23, B-1040 Brüssel

Inhalt

	Seite
Europäisches Vorwort	7
Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der abzudeckenden Richtlinie 2006/42/EG	8
Vorwort	11
Einleitung	13
1 Anwendungsbereich	17
2 Normative Verweisungen	17
3 Begriffe, Symbole und Abkürzungen	18
3.1 Begriffe	18
3.2 Symbole und Abkürzungen	28
4 Überblick	30
4.1 Prozess zur Risikobeurteilung und Risikominderung an der Maschine	30
4.2 Beitrag zur Risikominderung	32
4.3 Entwurfsprozess eines SRP/CS	33
4.4 Verfahren	34
4.5 Erforderliche Informationen	35
4.6 Ausführung von Sicherheitsfunktionen mithilfe von Teilsystemen	35
5 Spezifikation der Sicherheitsfunktionen	36
5.1 Identifizierung und allgemeine Beschreibung der Sicherheitsfunktion	36
5.2 Spezifikation der Sicherheitsanforderungen	36
5.2.1 Allgemeine Anforderungen	36
5.2.2 Anforderungen an spezifische Sicherheitsfunktionen	39
5.2.3 Minimierung des Anreizes zum Umgehen von Sicherheitsfunktionen	44
5.2.4 Fernzugriff	45
5.3 Bestimmung des erforderlichen Performance Levels (PL _r) für jede Sicherheitsfunktion	45
5.4 Überprüfung der Spezifikation der Sicherheitsanforderungen (SRS)	45
5.5 Zerlegung eines SRP/CS in Teilsysteme	45
6 Entwurfsaspekte	47
6.1 Bewertung des erreichten Performance Levels	47
6.1.1 Allgemeine Übersicht der Performance Level	47
6.1.2 Zusammenhang zwischen dem Performance Level (PL) und dem Sicherheits- Integritätslevel (SIL)	49
6.1.3 Architektur — Kategorien und deren Beziehung zur MTTF _D jedes Kanals, zum durchschnittlichen Diagnosedeckungsgrad und zum Ausfall infolge gemeinsamer Ursache (CCF)	50
6.1.4 Mittlere Dauer bis zum gefahrbringenden Ausfall (MTTF _D)	58
6.1.5 Diagnosedeckungsgrad (DC)	59
6.1.6 Ausfälle infolge gemeinsamer Ursache (CCF)	60
6.1.7 Systematische Ausfälle	60
6.1.8 Vereinfachtes Verfahren für die Abschätzung des Performance Levels für Teilsysteme	61
6.1.9 Alternatives Verfahren für die Bestimmung des Performance Levels und der PFH ohne MTTF _D	63
6.1.10 Fehlerbetrachtung und Fehlerausschluss	64

6.1.11	Bewährtes Bauteil	66
6.2	Kombination von Teilsystemen zum Erreichen eines gesamten Performance Levels für die Sicherheitsfunktion	66
6.2.1	Allgemeines	66
6.2.2	Bekannte PFH-Werte	66
6.2.3	Unbekannte PFH-Werte	67
6.3	Softwarebasierte manuelle Parametrierung	68
6.3.1	Allgemeines	68
6.3.2	Einflüsse auf sicherheitsbezogene Parameter	68
6.3.3	Anforderungen an die softwarebasierte manuelle Parametrierung	69
6.3.4	Verifizierung des Parametrierungswerkzeugs	70
6.3.5	Dokumentation der softwarebasierten manuellen Parametrierung	70
7	Software-Sicherheitsanforderungen	71
7.1	Allgemeines	71
7.2	Programmiersprache mit eingeschränktem Sprachumfang (LVL) und Programmiersprache mit nicht eingeschränktem Sprachumfang (FVL)	72
7.2.1	Programmiersprache mit eingeschränktem Sprachumfang (LVL)	72
7.2.2	Programmiersprache mit nicht eingeschränktem Sprachumfang (FVL)	73
7.2.3	Entscheidung zwischen Programmiersprache mit eingeschränktem Sprachumfang (LVL) und Programmiersprache mit nicht eingeschränktem Sprachumfang (FVL)	73
7.3	Sicherheitsbezogene Embedded-Software (SRESW)	75
7.3.1	Entwurf der sicherheitsbezogenen Embedded-Software (SRESW)	75
7.3.2	Alternative Verfahren für nicht zugängliche Embedded-Software	76
7.4	Sicherheitsbezogene Anwendungssoftware (SRASW)	77
8	Verifizierung des erreichten Performance Levels	80
9	Ergonomische Entwurfsaspekte	80
10	Validierung	80
10.1	Grundsätze der Validierung	80
10.1.1	Allgemeines	80
10.1.2	Validierungsplan	83
10.1.3	Allgemeine Fehlerlisten	83
10.1.4	Spezielle Fehlerlisten	83
10.1.5	Angaben zur Validierung	84
10.2	Validierung der Spezifikation der Sicherheitsanforderungen (SRS)	85
10.3	Validierung durch Analyse	85
10.3.1	Allgemeines	85
10.3.2	Analysetechniken	86
10.4	Validierung durch Prüfung	86
10.4.1	Allgemeines	86
10.4.2	Messgenauigkeit	87
10.4.3	Zusätzliche Prüfanforderungen	87
10.4.4	Anzahl der Prüflinge	87
10.4.5	Prüfverfahren	88
10.5	Validierung der Sicherheitsfunktionen	88
10.6	Validierung der Sicherheitsintegrität des SRP/CS	89
10.6.1	Validierung von Teilsystem(en)	89
10.6.2	Validierung der Maßnahmen zur Vermeidung systematischer Ausfälle	90
10.6.3	Validierung der sicherheitsbezogenen Software	91
10.6.4	Validierung der Kombination von Teilsystemen	92
10.6.5	Gesamtvalidierung der Sicherheitsintegrität	92
10.7	Validierung der Umgebungsanforderungen	92
10.8	Aufzeichnung der Validierung	93
10.9	Validierung der Instandhaltungsanforderungen	93

11	Wartungsfreundlichkeit von SRP/CS	94
12	Technische Dokumentation.....	94
13	Benutzerinformation	95
13.1	Allgemeines	95
13.2	Informationen für die Integration des SRP/CS	95
13.3	Informationen für den Benutzer	96
Anhang A (informativ) Leitlinien für die Bestimmung des erforderlichen Performance Levels (PL _r).....		98
A.1	Allgemeines	98
A.2	Auswahl des erforderlichen Performance Levels (PL _r)	98
A.3	Anleitung für die Auswahl der Parameter S, F und P zur Einschätzung des Risikos	99
A.3.1	Schwere der Verletzung S1 und S2	99
A.3.2	Häufigkeit und/oder Dauer der Gefährdungsexposition F1 und F2	99
A.3.3	Möglichkeit zur Vermeidung oder Begrenzung eines Schadens, P1 und P2	100
A.4	Überlagerte Gefährdungen	102
Anhang B (informativ) Blockmethode und sicherheitsbezogenes Blockdiagramm.....		103
B.1	Blockmethode	103
B.2	Sicherheitsbezogenes Blockdiagramm.....	103
Anhang C (informativ) Berechnung oder Bewertung von MTTF _D -Werten für einzelne Bauteile		105
C.1	Allgemeines	105
C.2	Verfahren guter ingenieurmäßiger Praxis	105
C.3	Hydraulische Bauteile.....	107
C.4	MTTF _D von pneumatischen, mechanischen und elektromechanischen Bauteilen	107
C.4.1	Allgemeines	107
C.4.2	Berechnung der MTTF _D für Bauteile aus B _{10D}	108
C.4.3	Erläuterung der Gleichungen.....	109
C.4.4	Beispiel.....	109
C.5	MTTF _D -Daten für elektronische Bauteile	110
C.5.1	Allgemeines	110
C.5.2	Halbleiter	110
C.5.3	Passive Bauteile	111
Anhang D (informativ) Vereinfachtes Verfahren zur Abschätzung der MTTF _D für jeden Kanal.....		113
D.1	Parts-Count-Verfahren	113
D.2	MTTF _D für unterschiedliche Kanäle, Symmetrisierung der MTTF _D für jeden Kanal	114
Anhang E (informativ) Abschätzungen des Diagnosedeckungsgrades (DC) für Funktionen und Teilsysteme.....		115
E.1	Beispiele für den Diagnosedeckungsgrad (DC)	115
E.2	Abschätzung des durchschnittlichen Diagnosedeckungsgrads.....	118
Anhang F (informativ) Verfahren zur Quantifizierung von Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF).....		119
F.1	Allgemeines	119
F.2	Abschätzung der Auswirkung der Maßnahmen gegen CCF.....	119
F.3	Beschreibung der Maßnahmen von Tabelle F.1 gegen Ausfälle infolge gemeinsamer Ursache (CCF).....	120
F.3.1	Trennung/Abtrennung.....	120
F.3.2	Diversität.....	121
F.3.3	Gestaltung/Anwendung/Erfahrung.....	121
F.3.4	Beurteilung/Analyse	121
F.3.5	Ausbildung	122
F.3.6	Umgebung.....	122

F.4	Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF) und weitere zutreffende Normen.....	122
Anhang G (informativ) Systematischer Ausfall		123
G.1	Allgemeines	123
G.2	Maßnahmen zur Beherrschung systematischer Ausfälle	123
G.3	Maßnahmen zur Vermeidung systematischer Ausfälle während des SRP/CS-Entwurfs.....	124
G.4	Maßnahmen zur Vermeidung systematischer Ausfälle während der Integration des SRP/CS	125
G.5	Management der funktionalen Sicherheit	125
Anhang H (informativ) Beispiel für eine Kombination von mehreren Teilsystemen.....		127
Anhang I (informativ) Beispiele für das vereinfachte Verfahren zur Abschätzung des PL von Teilsystemen		130
I.1	Allgemeines	130
I.2	Sicherheitsfunktion und erforderlicher Performance Level (PL _r)	130
I.3	Beispiel A — Einkanaliges System.....	131
I.3.1	Identifizierung der sicherheitsbezogenen Teile	131
I.3.2	Quantifizierung von MTTF _D , DC _{avg} , Maßnahmen gegen CCF, Kategorie und Performance Level	132
I.4	Beispiel B — Redundantes System.....	133
I.4.1	Identifizierung der sicherheitsbezogenen Teile	133
I.4.2	Quantifizierung von MTTF _D für jeden Kanal, durchschnittlichem Diagnosedeckungsgrad, Maßnahmen gegen CCF, Kategorie und Performance Level.....	135
Anhang J (informativ) Beispiel für die Ausführung einer SRESW		140
J.1	Beschreibung des Beispiels	140
J.2	Anwendung des V-Modells des Software-Sicherheitslebenszyklus.....	141
J.3	Verifizierung der Softwarespezifikation auf verschiedenen Ebenen (d. h. SDS, SSDS, MDS) ..	142
J.4	Beispiel für Programmierregeln.....	143
Anhang K (informativ) Numerische Darstellung von Bild 12		145
Anhang L (informativ) Elektromagnetische Störfestigkeit (EMI)		149
Anhang M (informativ) Ergänzende Informationen zur Spezifikation der Sicherheitsanforderungen (SRS)		153
Anhang N (informativ) Vermeiden eines systematischen Ausfalls durch den Entwurf von Software		155
N.1	Auswahl von Maßnahmen zur Fehlervermeidung für den Entwurf von sicherheitsbezogener Software.....	155
N.2	Beispiel für eine Software-Validierung	160
N.2.1	Allgemeines	160
N.2.2	Codierungsrichtlinien.....	160
N.2.3	Spezifikation der Sicherheitsfunktionen.....	160
N.2.4	Eingangsinformationen aus der Spezifikation des Hardware-Entwurfs	161
N.2.5	Anwendungsprogramm	164
N.2.6	Validierung der eingesetzten SRASW	164
Anhang O (informativ) Sicherheitsbezogene Werte von Bauteilen oder Komponenten der Steuerungen		175
O.1	Definition der Gerätetypen.....	175
O.1.1	Allgemeines	175
O.1.2	Gerätetyp 1	176
O.1.3	Gerätetyp 2	176
O.1.4	Gerätetyp 3	177
O.1.5	Gerätetyp 4	177

0.2 **Zusätzliche Informationen**..... 177

0.2.1 **Software** 177

0.2.2 **Grundlegende Sicherheitsprinzipien**..... 177

0.2.3 **Bewährte Sicherheitsprinzipien** 177

Literaturhinweise..... 178

Europäisches Vorwort

Dieses Dokument (EN ISO 13849-1:2023) 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.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis November 2023, und etwaige entgegenstehende nationale Normen müssen bis Mai 2026 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Dieses Dokument ersetzt EN ISO 13849-1:2015.

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

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

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.

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

Anerkennungsnotiz

Der Text von ISO 13849-1:2023 wurde von CEN als EN ISO 13849-1:2023 ohne irgendeine Abänderung genehmigt.

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 Mandats „M/396 Auftrag an CEN und CENELEC betreffend die Normung 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 den zugehörigen EFTA-Vorschriften.

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

Die relevanten grundlegenden Anforderungen der Richtlinie 2006/42/EG	Abschnitt(e)/Unter- abschnitt(e) dieser EN	Erläuterungen/Anmerkungen
1.1.6	9	
1.2.1	6, 7, 10	
1.2.3	5.2.2.4	Dieser Unterabschnitt befasst sich nur mit der Wiederanlauffunktion.
1.2.4.1	5.2.2.2	Dieser Unterabschnitt befasst sich nur mit derjenigen sicherheitsbezogenen Stopp-Funktion, mit der die Stopp-Kategorie 0 oder 1 erzielt wird.
1.2.4.2	5.2.2.2	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 (SRS) einer Not-Halt-Funktion.
1.2.5	5.2.2.9	
1.2.6	5.2.1.3 Listenpunkt i), 5.2.2.8	
1.6.1	11	

Die relevanten grundlegenden Anforderungen der Richtlinie 2006/42/EG	Abschnitt(e)/Unterabschnitt(e) dieser EN	Erläuterungen/Anmerkungen
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.

Tabelle ZA.2 — Anwendbare Normen, die die in diesem Anhang ZA beschriebene Konformitätsvermutung begründen

Verweisung in Abschnitt 2	Ausgabe der Internationalen Norm	Titel	Ausgabe der entsprechenden Europäischen Norm
ISO 12100:2010	ISO 12100:2010	<i>Sicherheit von Maschinen — Allgemeine Gestaltungsleitsätze — Risikobeurteilung und Risikominderung</i>	EN ISO 12100:2010
ISO 13849-2:2012	ISO 13849-2:2012	<i>Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen — Teil 2: Validierung</i>	EN ISO 13849-2:2012
ISO 13855:2010	ISO 13855:2010	<i>Sicherheit von Maschinen — Anordnung von Schutzeinrichtungen im Hinblick auf Annäherungsgeschwindigkeiten von Körperteilen</i>	EN ISO 13855:2010
ISO 20607:2019	ISO 20607:2019	<i>Sicherheit von Maschinen — Betriebsanleitung — Allgemeine Gestaltungsgrundsätze</i>	EN ISO 20607:2019
IEC 61508-3:2010	IEC 61508-3:2010	<i>Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 3: Anforderungen an Software</i>	IEC 61508-3:2010
IEC 62046:2018	IEC 62046:2018	<i>Sicherheit von Maschinen — Anwendung von Schutzeinrichtungen zur Anwesenheitserkennung von Personen</i>	EN IEC 62046:2018
IEC 62061:2021	IEC 62061:2021	<i>Sicherheit von Maschinen — Funktionale Sicherheit sicherheitsbezogener Steuerungssysteme</i>	EN IEC 62061:2021
IEC/IEEE 82079-1:2019	IEC/IEEE 82079-1:2019	<i>Erstellung von Nutzungsinformationen (Gebrauchsanleitungen) für Produkte — Teil 1: Grundsätze und allgemeine Anforderungen</i>	EN IEC/IEEE 82079-1:2019

Auf die in Spalte 1 von Tabelle ZA.2 aufgeführten Dokumente wird in diesem Dokument teilweise oder als Ganzes normativ verwiesen, so dass sie für die Anwendung dieses Dokuments erforderlich sind. Für das Erreichen der Konformitätsvermutung ist die Anwendung der in Spalte 4 aufgeführten Normenausgabe oder, wenn keine Europäische Normenausgabe existiert, der in Spalte 2 von Tabelle ZA.2 angegebenen Internationalen Normausgabe erforderlich.

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-Directives, 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-Directives, 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*, in Zusammenarbeit mit dem Europäischen Komitee für Normung (CEN), Technisches Komitee CEN/TC 114, *Sicherheit von Maschinen*, in Übereinstimmung mit der Vereinbarung zur technischen Zusammenarbeit zwischen ISO und CEN (Wiener Vereinbarung) erarbeitet.

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

Die wesentlichen Änderungen sind folgende:

- das gesamte Dokument wurde neu strukturiert, um den Entwurfs- und Entwicklungsprozess für Steuerungen besser nachvollziehen zu können;
- ein neuer Abschnitt 4 mit Empfehlungen für die Risikobeurteilung;
- Spezifikation der Sicherheitsfunktionen (aktualisierter Abschnitt 5);
- Kombination von verschiedenen Teilsystemen (aktualisiert in Abschnitt 6);
- ein neuer Abschnitt 7 mit Software-Sicherheitsanforderungen;
- ein neuer Abschnitt 9 zu ergonomischen Entwurfsaspekten;
- Validierung (Abschnitt 8 aktualisiert und nach Abschnitt 10 verschoben);
- ein neuer Abschnitt G.5 zum Management der funktionalen Sicherheit;

- ein neuer Anhang L zur elektromagnetischen Störfestigkeit (EMI, en: electromagnetic interference);
- ein neuer Anhang M mit zusätzlichen Informationen zur Spezifikation der Sicherheitsanforderungen;
- ein neuer Anhang N zu den Maßnahmen zur Fehlervermeidung für das sicherheitsrelevante Softwaredesign;
- ein neuer Anhang O mit sicherheitsbezogenen Werten von Bauteilen oder Komponenten der Steuerungen.

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

Sicherheitsnormen im Bereich von Maschinen sind wie folgt aufgebaut.

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

Dieses Dokument ist eine Typ-B1-Norm, wie in ISO 12100:2010 festgelegt.

Die erste Ausgabe dieses Dokuments wurde 1999 veröffentlicht und basierte auf EN 954-1:1996 (Norm zurückgezogen). Die zweite Ausgabe wurde 2006 überarbeitet und die dritte Ausgabe wurde 2015 überarbeitet.

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 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 (d. h. Maschinen, die 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, wie in ISO 12100:2010 festgelegt.

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 Beispiele und die Grundlage für den Großteil des Inhalts bilden stationäre Maschinen in industriellen Anwendungen. Dies schließt jedoch andere Maschinen nicht aus. Dieses Dokument wurde erarbeitet, ohne dabei zu berücksichtigen, ob für bestimmte Maschinen (z. B. ortsveränderliche Maschinen) spezifische Anforderungen gelten. Dieses Dokument ist jedoch dafür vorgesehen, in vielen Maschinenbranchen und als Grundlage für Entwickler von Typ-C-Normen verwendet zu werden, soweit dies möglich ist.

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.

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

ISO 12100:2010 wird für die Risikobeurteilung der Maschine angewendet. Mithilfe von Anhang A dieses Dokuments kann der erforderliche Performance Level (PL_r) einer Sicherheitsfunktion, die vom SRP/CS ausgeführt wird, bestimmt werden, wenn kein PL_r in der zutreffenden Typ-C-Norm festgelegt ist. Dieses Dokument ist maßgebend für die Sicherheitsfunktionen eines SRP/CS, die ausgeführt werden, um Risiken abzudecken, für die eine Risikobeurteilung nach ISO 12100:2010 ergibt, dass eine risikomindernde Maßnahme erforderlich ist, die auf einer Sicherheitsfunktion basiert (z. B. verriegelnde trennende Schutzeinrichtung). In solchen Fällen führt die sicherheitsbezogene Steuerung eine Sicherheitsfunktion aus. Dieses Dokument ist für den Entwurf und die Bewertung von SRP/CS vorgesehen. Nur derjenige Teil der Steuerung, das in Bezug zur Sicherheit steht (sicherheitsbezogen ist), wird vom Anwendungsbereich dieses Dokuments abgedeckt.

Bild 1 zeigt den Zusammenhang zwischen ISO 12100:2010 und diesem Dokument. Für eine ausführliche Übersicht siehe Bild 2.

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

ANMERKUNG Basierend auf ISO/TR 22100-2:2013, Bild 2.

Bild 1 — Integration dieses Dokuments (ISO 13849-1) in den Prozess zur Risikominderung nach ISO 12100:2010

ANMERKUNG 3 Bild 1 zeigt auf, wo das SRP/CS zum Prozess der Risikominderung von ISO 12100:2010, Schritt 2, beiträgt. Durch die Ausführung von Sicherheitsfunktionen unterstützt das SRP/CS die kombinierten risikomindernden Maßnahmen. Die Fähigkeit sicherheitsbezogener Teile von Steuerungen, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen, wird einer von fünf Stufen zugeordnet, den so genannten Performance Level (PL). Der erforderliche Performance Level (PL_r) für eine bestimmte Sicherheitsfunktion (in Abhängigkeit von der geforderten Risikominderung) wird durch Risikoeinschätzung ermittelt.

Der informative Anhang A dieses Dokuments enthält ein Verfahren für die Risikoeinschätzung und kann zur Bestimmung des PL_r einer von der SRP/CS ausgeführten Sicherheitsfunktion verwendet werden. Jedes Verfahren zur Risikoeinschätzung weist aufgrund der Subjektivität der Bewertungskriterien eine Varianz auf. Im Vergleich zu Anhang A können Typ-C-Normen spezifischere Methoden zur Risikoeinschätzung für spezifische Maschinenanwendungen enthalten.

Die Häufigkeit 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 ($MTTF_D$)], Ausfall infolge gemeinsamer Ursache (CCF)], dem Gestaltungsprozess, der Betriebsbeanspruchung, 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 (z. B. $MTTF_D$, DC_{avg}) 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 Häufigkeit eines gefahrbringenden Ausfalls je Stunde (PFH; en: frequency of dangerous failure per hour) angegeben.

Die Performance Level und die Kategorien können für die SRP/CS angewendet werden, z. B.:

- Steuerungsbaugruppen (z. B. eine Logikeinheit für Steuerungsfunktionen, Datenverarbeitung, Überwachung);
- berührungslos wirkende Schutzeinrichtungen (z. B. Lichtschranken), druckempfindliche Schutzeinrichtungen.

Die Performance Level und die Kategorien können für Teilsysteme von SRP/CS definiert und bestimmt werden, die Sicherheitsteile (Komponenten) nutzen, z. B.:

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

Die von diesem Dokument abgedeckten 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 beide 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).

1 Anwendungsbereich

Dieses Dokument legt ein Verfahren fest und enthält zugehörige Anforderungen, Empfehlungen und einen Leitfaden für die Gestaltung und Integration sicherheitsbezogener Teile von Steuerungen (SRP/CS), die Sicherheitsfunktionen ausführen, einschließlich des Entwurfs von Software.

Dieses Dokument ist anwendbar für SRP/CS in der Betriebsart mit hoher Anforderungsrate und der Betriebsart mit kontinuierlicher Anforderung einschließlich ihrer Teilsysteme, ungeachtet der Art der Technologie und der Energie (z. B. elektrisch, hydraulisch, pneumatisch und mechanisch). Dieses Dokument ist nicht anwendbar für Betriebsarten mit niedriger Anforderungsrate.

ANMERKUNG 1 Siehe 3.1.44 und die Normenreihe IEC 61508 für die Betriebsart mit niedriger Anforderungsrate.

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

ANMERKUNG 2 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.

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

Dieses Dokument enthält keine spezifischen Maßnahmen für weitere Sicherheitsaspekte (z. B. physische Sicherheit, IT-Sicherheit, Cybersicherheit).

ANMERKUNG 3 Securityaspekte können einen Einfluss auf Sicherheitsfunktionen haben. Siehe ISO/TR 22100-4 und IEC/TR 63074 für weitere Informationen.

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*

ISO 20607:2019, *Safety of machinery — Instruction handbook — General drafting principles*

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 62061:2021, *Safety of machinery — Functional safety of safety-related control systems*

IEC/IEEE 82079-1:2019, *Preparation of information for use (instructions for use) of products — Part 1: Principles and general requirements*

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:

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

3.1.1

sicherheitsbezogenes Teil einer Steuerung

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

Teil einer Steuerung, das eine *Sicherheitsfunktion* (3.1.27) 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 dem Ausgang der Leistungssteuerungselemente (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 requirements specification

Spezifikation der Anforderungen an die *Sicherheitsfunktionen* (3.1.27), die von der sicherheitsbezogenen Steuerung erfüllt werden müssen; die Spezifikation erfolgt im Hinblick auf die Eigenschaften der Sicherheitsfunktionen (funktionale Eigenschaften) und die *erforderlichen Performance Level* (PL_r) (3.1.6)

[QUELLE: IEC 61508-4:2010, 3.5.11, modifiziert, Angaben aus IEC 61508-4:2010, 3.5.12 wurden integriert.]

3.1.4

Kategorie

Einstufung des *Teilsystems* (3.1.45) bezüglich seines Widerstands gegen *Fehler* (3.1.8) 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* (SRP/CS) (3.1.1) spezifiziert, eine *Sicherheitsfunktion* (3.1.27) unter vorhersehbaren Bedingungen auszuführen

Anmerkung 1 zum Begriff: Siehe 6.1 für eine allgemeine Übersicht der Performance Level.

3.1.6

erforderlicher Performance Level

PL_r, en: required performance level

Performance Level (3.1.5), der erforderlich ist, um die erforderliche *Risikominderung* (3.1.19) für jede *Sicherheitsfunktion* (3.1.27) zu erreichen

Anmerkung 1 zum Begriff: Siehe 5.3 und Bild A.1 für weitere Informationen zum erforderlichen Performance Level (PL_r).

3.1.7

Sicherheits-Integritätslevel

SIL

diskrete Stufe (eine von vier möglichen) zur Festlegung der Anforderungen an die Sicherheitsintegrität der *Sicherheitsfunktionen* (3.1.27), 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 — „die den sicherheitsbezogenen Systemen zugeordnet werden“ wurde der Definition hinzugefügt, die ANMERKUNGEN wurden gestrichen und eine neue Anmerkung 1 zum Begriff wurde hinzugefügt.]

3.1.8

Fehler

Fehlzustand

anomaler Zustand, der dazu führen kann, dass die Fähigkeit der funktionalen Einheit zur Ausführung einer erforderlichen Funktion verringert wird oder verloren geht

Anmerkung 1 zum Begriff: Ein Fehler ist oft das Ergebnis eines *Ausfalls* (3.1.10) 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* (3.1.14) hervorgerufener Fehler“.

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

3.1.9

Fehlerausschluss

Ausschluss von bestimmten *Fehlern* (3.1.8) innerhalb eines sicherheitsbezogenen Teils einer Steuerung (SRP/CS), wenn dieser Ausschluss durch die vernachlässigbare Wahrscheinlichkeit dieser Fehler gerechtfertigt werden kann

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* (3.1.8).

Anmerkung 2 zum Begriff: Der „Ausfall“ ist ein Ereignis, im Unterschied zum „Fehler“, der einen Status 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 hinzugefügt.]

3.1.11

permanenter Fehlzustand

Fehler (3.1.8) einer Einheit, der so lange besteht, bis eine Instandsetzung ausgeführt worden ist

[QUELLE: IEC 60050-192:2015]

3.1.12

gefährbringender Ausfall

Ausfall (3.1.10) eines Elements und/oder *Teilsystems* (3.1.45) und/oder Systems, das Anteil an der Ausführung der *Sicherheitsfunktion* (3.1.27) hat, der:

- a) verhindert, dass eine Sicherheitsfunktion bei Anforderung ausgeführt wird (Anforderungsbetriebsart) oder den Ausfall einer Sicherheitsfunktion verursacht (Betriebsart mit kontinuierlicher Anforderung), so dass die Maschine/Maschinenanlage 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 „Maschine/Maschinenanlage“ ersetzt.]

3.1.13

Ausfall infolge gemeinsamer Ursache

CCF, en: common cause failure

Ausfall (3.1.10), der das Ergebnis eines oder mehrerer Ereignisse ist, die gleichzeitige Ausfälle von zwei oder mehreren getrennten *Kanälen* (3.1.47) in einem mehrkanaligen *Teilsystem* (3.1.45) verursachen und zu einem Ausfall einer *Sicherheitsfunktion* (3.1.27) 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, modifiziert — „Systemausfall“ wurde durch „Ausfall einer Sicherheitsfunktion“ ersetzt. Anmerkung 1 zum Begriff wurde hinzugefügt.]

3.1.14

systematischer Ausfall

Ausfall (3.1.10) mit deterministischem Bezug zu einer bestimmten Ursache, die nur durch Änderung der Gestaltung oder des Herstellungsprozesses, der Betriebsverfahren, der Dokumentation oder anderer zugehöriger 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* (SRS) (3.1.3),
- dem Entwurf, der Herstellung, der Installation und des Betriebs der Hardware,
- dem Entwurf, der Realisierung der Software, und
- der unzureichenden Festlegung von Umgebungsbedingungen.

[QUELLE: IEC 60050-192:2015]

3.1.15

Überbrückungsfunktion en muting

vorübergehende automatische Überbrückung einer *Sicherheitsfunktion* bzw. von *Sicherheitsfunktionen* (3.1.27) durch das SRP/CS

[QUELLE: IEC 61496-1:2020, 3.16]

3.1.16

Schaden

physische Verletzung oder Gesundheitsschädigung

[QUELLE: ISO 12100:2010, 3.5]

3.1.17

Gefährdung

potenzielle *Schadensquelle* (3.1.16)

Anmerkung 1 zum Begriff: Der Begriff „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.]

3.1.18

Gefährdungssituation

Sachlage, bei der eine Person mindestens einer *Gefährdung* (3.1.17) ausgesetzt ist

Anmerkung 1 zum Begriff: Diese Situation kann unmittelbar oder über eine Zeitspanne hinweg zu einem *Schaden* (3.1.16) führen.

[QUELLE: ISO 12100:2010, 3.10]

3.1.19

Risiko

Kombination der Wahrscheinlichkeit des Eintritts eines *Schadens* (3.1.16) und des Schadensausmaßes

[QUELLE: ISO 12100:2010, 3.12]

3.1.20

Restrisiko

Risiko (3.1.19), das verbleibt, nachdem *risikomindernde Maßnahmen* (*Schutzmaßnahmen*) (3.1.22) umgesetzt wurden

Anmerkung 1 zum Begriff: Siehe Bild 3.

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

3.1.21

Risikobeurteilung

Gesamtheit des Verfahrens, das eine *Risikoanalyse* (3.1.23) und *Risikobewertung* (3.1.24) umfasst

[QUELLE: ISO 12100:2010, 3.17]

3.1.22

risikomindernde Maßnahme

Schutzmaßnahme

Handlung oder Mittel zur Beseitigung von *Gefährdungen* (3.1.17) oder zur Verminderung von *Risiken* (3.1.19)

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

[QUELLE: ISO/IEC Guide 51:2014, 3.13]

3.1.23

Risikoanalyse

Kombination aus Festlegung der Grenzen der Maschine, Identifizierung der *Gefährdungen* (3.1.17) und *Risikoeinschätzung* (3.1.19)

[QUELLE: ISO 12100:2010, 3.15]

3.1.24

Risikobewertung

auf der *Risikoanalyse* (3.1.23) beruhende Beurteilung, ob die Ziele zur Risikominderung erreicht wurden

[QUELLE: ISO 12100:2010, 3.16]

3.1.25

bestimmungsgemäße Verwendung der Maschine

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

[QUELLE: ISO 12100:2010, 3.23]

3.1.26

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]

3.1.27

Sicherheitsfunktion

Funktion einer Maschine, wobei ein *Ausfall* (3.1.10) dieser Funktion zur unmittelbaren Erhöhung des *Risikos* (der *Risiken*) (3.1.19) führen kann

Anmerkung 1 zum Begriff: Eine Sicherheitsfunktion ist eine Funktion, die von einem sicherheitsbezogenen Teil einer Steuerung ausgeführt wird 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, modifiziert — Anmerkung 1 zum Begriff wurde hinzugefügt.]

3.1.28

Teilfunktion

Teil einer *Sicherheitsfunktion* (3.1.27), dessen *Ausfall* (3.1.10) zu einem Ausfall der Sicherheitsfunktion führt

Anmerkung 1 zum Begriff: Eine Teilfunktion ist eine Funktion, die von einem *Teilsystem* (3.1.45) des sicherheitsbezogenen Teils einer Steuerung (SRP/CS) ausgeführt wird. 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.

3.1.29

Überwachung

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

Anmerkung 1 zum Begriff: Überwachung wird durch die folgenden Verfahren realisiert, wie z. B. *Plausibilitätsprüfung* (3.1.52), direkter, indirekter oder *Kreuzvergleich* (3.1.30) (siehe Anhang E), zyklischer Testimpuls.

3.1.30

Kreuzvergleich

Diagnosemaßnahme zur Überprüfung der Plausibilität von redundanten Signalen in beiden *Kanälen* (3.1.47) eines redundanten *Teilsystems* (3.1.45)

3.1.31

programmierbares elektronisches System

PE-System

System zur Steuerung, zum Schutz oder zur *Überwachung* (3.1.29), 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 Aktuatoren und anderer Ausgabeeinrichtungen

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

3.1.32

mittlere Dauer bis zum gefahrbringenden Ausfall

MTTF_D, en: mean time to dangerous failure

Erwartungswert der mittleren Zeit 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 62061:2021, 3.2.38, modifiziert — Anmerkung 1 zum Begriff wurde geändert.]

3.1.33

MTBF, en: mean time between failures

mittlere Zeit zwischen Ausfällen

Erwartungswert der Betriebsdauer zwischen aufeinanderfolgenden *Ausfällen* (3.1.10)

3.1.34

RDF, en: ratio of dangerous failures

Anteil gefahrbringender Ausfälle

Anteil der *Gesamtausfallrate* (3.1.10) eines Elements, der zu einem *gefahrbringenden Ausfall* (3.1.12) führen kann

3.1.35

Diagnosedeckungsgrad

DC, en: diagnostic coverage

Maß für die Wirksamkeit der Diagnosemaßnahmen, bestimmt als das Verhältnis der *Ausfallrate* (3.1.10) der erkannten *gefahrbringenden Ausfälle* (3.1.12) 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 kann ein Diagnosedeckungsgrad für die Sensoren und/oder Logiksysteme und/oder für die Leistungssteuerungselemente vorhanden sein.

3.1.36

Gebrauchsdauer

T_M

Zeitraum, der die bestimmungsgemäße Verwendung eines sicherheitsbezogenen Teils einer Steuerung (SRP/CS) abdeckt

3.1.37

Testrate

r_t

Häufigkeit der Tests, um *Fehler* (3.1.8) in einem sicherheitsbezogenen Teil einer Steuerung (SRP/CS) zu erkennen

Anmerkung 1 zum Begriff: Testrate wird auch als Kehrwert des Diagnose-Testintervalls verwendet.

3.1.38

Anforderungsrate

r_d

Häufigkeit von Anforderungen für eine von dem sicherheitsbezogenen Teil einer Steuerung (SRP/CS) auszuführende *Sicherheitsfunktion* (3.1.27)

3.1.39

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 *Spezifikationen der Sicherheitsanforderungen (SRS)* (3.1.3) zu implementieren

Anmerkung 1 zum Begriff: Eine LVL bietet eine enge funktionale Übereinstimmung 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 Kontaktplan, eine Funktionsbausteinsprache und eine Ablaufsprache. Anweisungslisten 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 62061:2021, 3.2.62]

3.1.40

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, Anweisungsliste, Assembler-Sprachen, C++, Java, SQL.

[QUELLE: IEC 62061:2021, 3.2.61]

3.1.41

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, die notwendig sind, um die Anforderungen des sicherheitsbezogenen Teils einer Steuerung (SRP/CS) zu erfüllen

3.1.42

sicherheitsbezogene Embedded-Software

SRESW, en: safety-related embedded software

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

Anmerkung 1 zum Begriff: Embedded-Software wird auch als System-Software oder Firmware bezeichnet. Siehe *Programmiersprachen mit nicht eingeschränktem Sprachumfang (FVL)* (3.1.40).

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

3.1.43

Betriebsart mit hoher Anforderungsrate oder Betriebsart mit kontinuierlicher Anforderung

Betriebsart, in der die Häufigkeit von Anforderungen an ein sicherheitsbezogenes Teil einer Steuerung (SRP/CS) für die Ausführung seiner *Sicherheitsfunktion* (3.1.27) 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]

3.1.44

Betriebsart mit niedriger Anforderungsrate

Betriebsart, in der die Häufigkeit von Anforderungen an ein sicherheitsbezogenes Teil einer Steuerung (SRP/CS) für die Ausführung seiner *Sicherheitsfunktion* (3.1.27) nicht mehr als einmal je Jahr beträgt

Anmerkung 1 zum Begriff: Die Betriebsart mit niedriger Anforderungsrate wird in diesem Dokument nicht berücksichtigt. Siehe Abschnitt 1 für weitere Einzelheiten.

[QUELLE: IEC 61508-4:2010, 3.5.16, modifiziert — Anmerkung 1 zum Begriff wurde hinzugefügt.]

3.1.45

Teilsystem

Einheit, die aus der Zerlegung eines sicherheitsbezogenen Teils einer Steuerung (SRP/CS) auf erster Ebene resultiert und deren *gefahrbringender Ausfall* (3.1.12) zu einem gefahrbringenden Ausfall einer *Sicherheitsfunktion* (3.1.27) 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.

3.1.46

Teilsystemelement

Teil eines *Teilsystems* (3.1.45), 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.

Anmerkung 2 zum Begriff: Für die sicherheitsbezogenen Werte von Bauteilen oder Teilen von Steuerungen siehe Anhang O.

3.1.47

Kanal

Element oder Gruppe von Elementen, das bzw. die eine *Sicherheitsfunktion* (3.1.27) oder einen Teil davon unabhängig ausführt

Anmerkung 1 zum Begriff: Ein Kanal kann ein Funktionskanal oder ein Testkanal sein.

[QUELLE: IEC 61508-4:2010, 3.3.6, modifiziert — „oder einen Teil davon“ wurde zur Definition hinzugefügt und Anmerkung 1 zum Begriff wurde hinzugefügt.]

3.1.48

Betriebsart

Betriebsweise einer Maschine (z. B. Automatikbetrieb, manueller Betrieb, Instandhaltungsbetrieb) zur Auswahl vordefinierter Maschinenfunktionen und mit ihnen verbundener Sicherheitsmaßnahmen

Anmerkung 1 zum Begriff: Für jede spezifische Betriebsart werden die maßgebenden *Sicherheitsfunktionen* (3.1.27) und/oder *risikomindernden Maßnahmen* (3.1.22) ausgeführt.

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

3.1.49

bewährtes Sicherheitsprinzip

Prinzip, das sich in der Vergangenheit bei der Gestaltung oder Integration von sicherheitsbezogenen Steuerungen als wirkungsvoll erwiesen hat, und so kritische *Fehler* (3.1.8) oder *Ausfälle* (3.1.10), welche die Leistungsfähigkeit einer *Sicherheitsfunktion* (3.1.27) beeinflussen können, vermeidet oder beherrscht

Anmerkung 1 zum Begriff: Neu entwickelte Sicherheitsprinzipien können nur dann als gleichwertig mit den „bewährten Sicherheitsprinzipien“ angesehen werden, wenn sie anhand von Verfahren verifiziert 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* (3.1.14), 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: ISO 13849-2:2012, Tabelle A.2, Tabelle B.2, Tabelle C.2 und Tabelle D.2 behandeln bewährte Sicherheitsprinzipien für unterschiedliche Technologien.

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 13849-2:2012 für eine Liste anerkannter bewährter Bauteile.

3.1.51

dynamisches Testen

entweder Ausführung der Software oder Betrieb der Hardware oder beides in kontrollierter und systematischer Weise, um nachzuweisen, dass das geforderte Verhalten vorliegt und dass kein unerwünschtes Verhalten vorliegt

Anmerkung 1 zum Begriff: Der Test ist nicht bestanden, wenn die Signaländerung nicht wie erwartet bei der *Überwachung* (3.1.29) 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.

3.1.52

Plausibilitätsprüfung

Diagnosemaßnahme, die *überwacht* (3.1.29), ob der Status eines Eingangs (Ausgangs) zu dem Status des Systems oder anderer Eingänge (Ausgänge) passt

3.1.53

Verifizierung

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

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

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

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

[QUELLE: ISO 9000:2015, 3.8.12]

3.1.54

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 Einsatzbedingungen für die Validierung können echt oder simuliert sein.

[QUELLE: IEC 61508-4:2010, 3.8.2]

3.1.55

Fachkraft

Person, die aufgrund ihrer Weiterbildung, ihrer Ausbildung und ihrer Erfahrung fähig ist, *Risiken* (3.1.19) zu erkennen und *Gefährdungen* (3.1.17) 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 — in der Definition wurde „Elektrizität“ durch „der jeweiligen Ausrüstung“ ersetzt und Anmerkung 1 zum Begriff wurde hinzugefügt.]

3.1.56

Black Box

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

3.1.57

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.

3.1.58

mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde

PFH, en: average frequency of a dangerous failure per hour

mittlere Häufigkeit eines gefahrbringenden Ausfalls eines *sicherheitsbezogenen Teils eines Systems (SRP/CS)* (3.1.1), die festgelegte Sicherheitsfunktion über einen gegebenen Zeitraum auszuführen

[QUELLE: IEC 61508-4:2010, 3.6.19, modifiziert — „E/E/PE-“ wurde gestrichen.]

3.2 Symbole und Abkürzungen

Tabelle 1 — Symbole und Abkürzungen

Symbol oder Abkürzung	Beschreibung	Unterabschnitt oder Abschnitt
a, b, c, d, e	Bezeichnung für die Performance Level	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 5
B_{10D}	Anzahl der Zyklen bis 10 % der Bauteile gefahrbringend ausgefallen sind (für Bauteile mit mechanischem Verschleiß)	Anhang C
Kat.	Kategorie	3.1.4
CC	Stromrichter (en: current converter)	Anhang I
CCF	Ausfall infolge gemeinsamer Ursache (en: common cause failure)	3.1.13
DC	Diagnosedeckungsgrad	3.1.35
DC_{avg}	durchschnittlicher Diagnosedeckungsgrad (en: average diagnostic coverage)	E.2
EMI	elektromagnetische Störung (en: electromagnetic interference)	F.3.6.1
ETA	Ereignisbaumanalyse (en: event tree analysis)	10.3.2
F, F1, F2	Häufigkeit und/oder Dauer der Gefährdungsexposition	A.3.2
FB	Funktionsblock (en: function block)	Anhang J
FVL	Programmiersprache mit nicht eingeschränktem Sprachumfang	3.1.40
FMEA	Ausfalleffektanalyse (en: failure modes and effects analysis)	6.1.5
FMECA	Ausfalleffekt- und Kritikalitätsanalyse (en: failure modes, effects and critically analysis)	10.3.2

Symbol oder Abkürzung	Beschreibung	Unterabschnitt oder Abschnitt
FTA	Fehlerbaumanalyse (en: fault tree analysis)	10.3.2
$F_D(t)$	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
I/O	Eingänge/Ausgänge	Tabelle E.1
i_m	Verbindungsmittel	Bild 7, Bild 8, Bild 9, Bild 10
K1A, K1B	Schütze	Anhang I
L, L1, L2	Logik	6.1
LVL	Programmiersprache mit eingeschränktem Sprachumfang	3.1.39
λ_D	gefahrbringende Ausfallrate eines Bauteils	Anhang C
M	Motor	Anhang I
MTTF	mittlere Dauer bis zum Ausfall	Anhang C
MTTF _D	mittlere Dauer bis zum gefahrbringenden Ausfall	3.1.32
MTTR	mittlere Dauer bis zur Wiederherstellung	Anhang D
$n, N, \tilde{N}$	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	Ausabeeinheit, Ausgabe der Testeinrichtung, z. B. Leistungssteuerungselemente	6.1
P, P1, P2	Möglichkeit zur Vermeidung oder Begrenzung eines Schadens	A.3.3
PE-System	programmierbares elektronisches System	3.1.31, Anhang H
PFH	mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde	3.1.58, Tabelle 2, Tabelle K.1
PL	Performance Level	3.1.5
SPS	speicherprogrammierbare Steuerung	Anhang I
PL_{niedrig}	niedrigster Performance Level eines Teilsystems in einer Kombination von Teilsystemen	6.2
PL_r	erforderlicher Performance Level	3.1.6
r_d	Anforderungsrate	3.1.38
r_t	Testrate	3.1.37
RDF	Anteil gefahrbringender Ausfälle	3.1.34
RS	Drehgeber (en: rotation sensor)	Anhang I

Symbol oder Abkürzung	Beschreibung	Unterabschnitt oder Abschnitt
S, S1, S2	Schwere der Verletzung	A.3.1
SB	Teilsystem	Bild 13, Bild H.1, Bild H.2
SOS	sicherer Betriebshalt	5.2.2.2
SS2	sicherer Stopp 2	5.2.2.2
SW1A, SW1B, SW2	Positionsschalter	Anhang I
SIL	Sicherheits-Integritätslevel	3.1.7, Abschnitt 6
SLS	sicher begrenzte Geschwindigkeit (en: safely limited speed)	Tabelle 3
SRASW	sicherheitsbezogene Anwendungssoftware (en: safety-related application software)	3.1.41
SRESW	sicherheitsbezogene Embedded-Software (en: safety-related embedded software)	3.1.42
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)	3.1.3
STO	sicher abgeschaltetes Drehmoment (en: safe torque off)	Tabelle 3 und Tabelle N.2
TE	Testeinrichtung (en: test equipment)	6.1
T_M	Gebrauchsdauer	3.1.36
T_{10D}	mittlere Zeit bis 10 % der Bauteile gefahrbringend ausfallen	Anhang C

4 Überblick

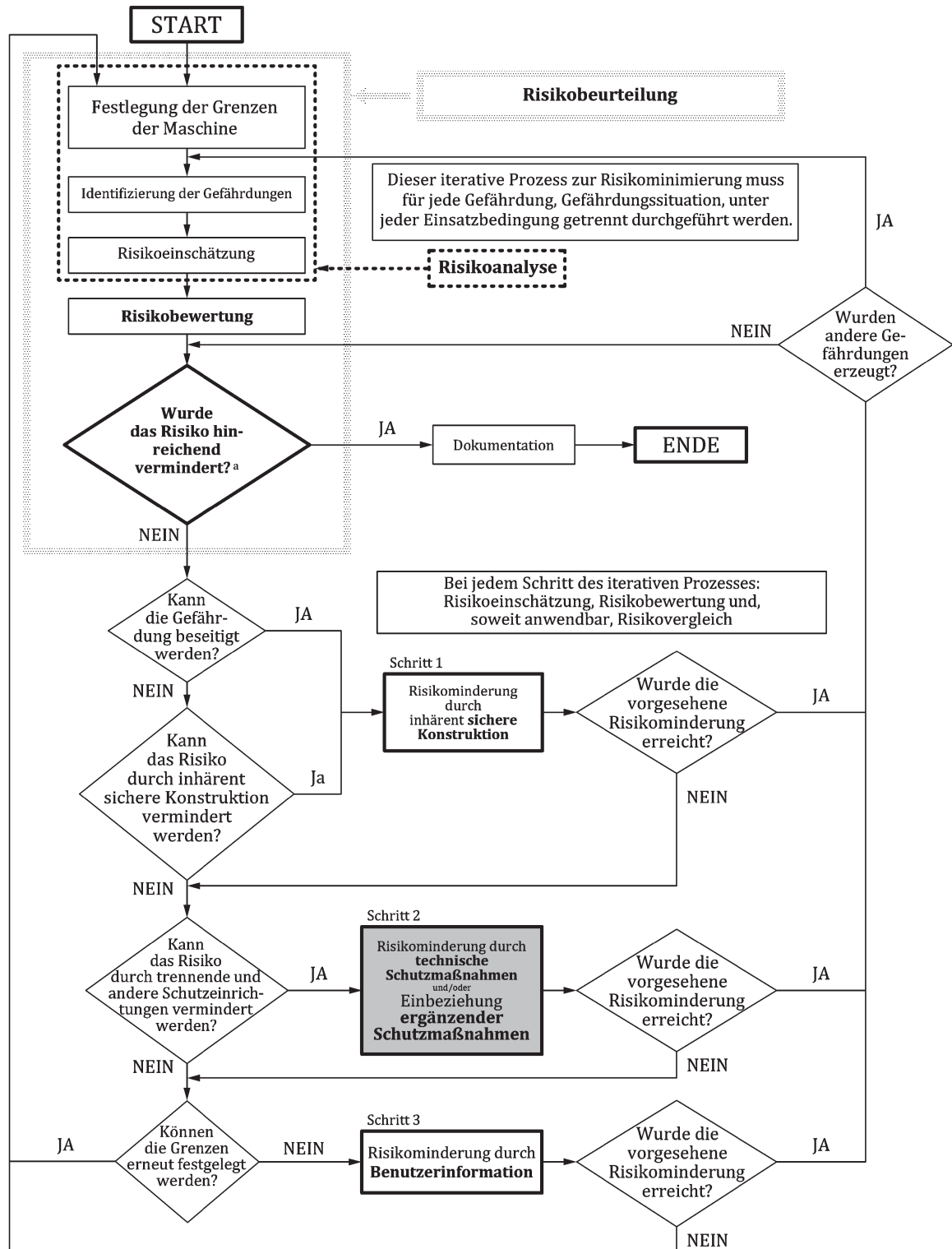
4.1 Prozess zur Risikobeurteilung und Risikominderung an der Maschine

Der Prozess zur Risikobeurteilung und Risikominderung wird in ISO 12100:2010 definiert und ist in Bild 2 dargestellt. ISO 13849-1 (dieses Dokument) ist Teil des Prozesses zur Risikominderung, wenn eine Sicherheitsfunktion und deren zugehöriges SRP/CS verwendet werden, um die Risikominderung durchzuführen.

ANMERKUNG 1 Für weitere Informationen siehe ISO/TR 22100-2:2013.

Bei der SRS 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 2 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 kann dieses Dokument angewendet werden.

ANMERKUNG Bild übernommen aus ISO 12100:2010, Bild 1.

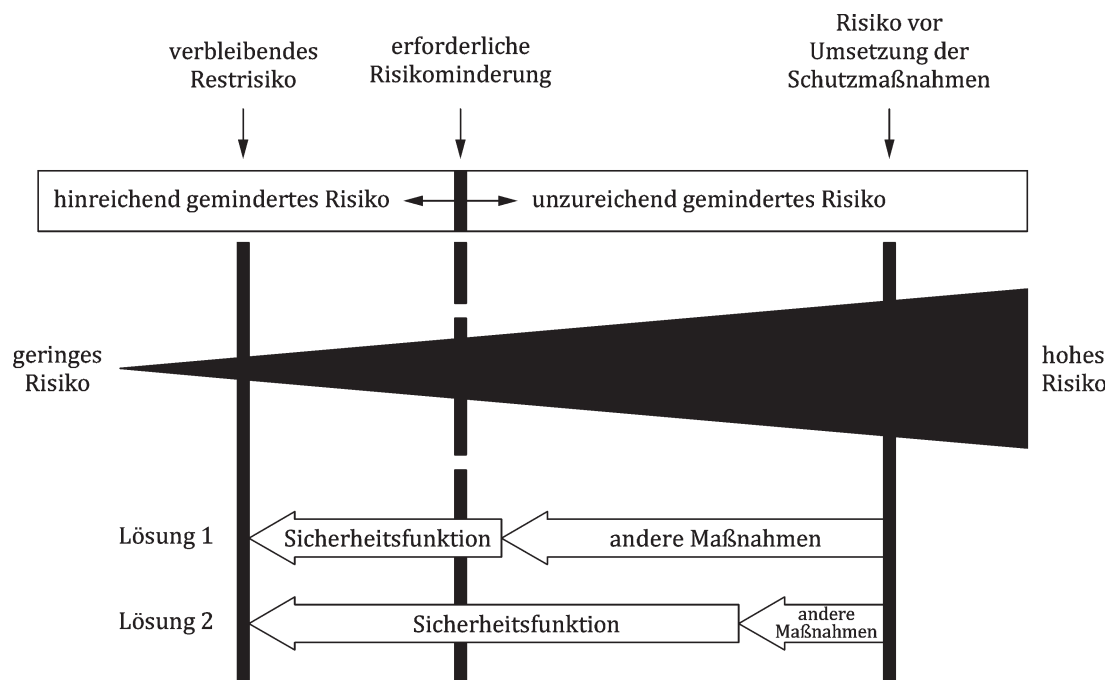
Bild 2 — Schematische Darstellung des dreistufigen iterativen Prozesses zur Risikominderung

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

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). Er bezieht sich nicht auf das Gesamtrisiko der gesteuerten Maschine.

BEISPIEL Die sicherheitsbezogene Stoppfunktion einer Presse, die mithilfe einer berührungslos wirkenden Schutzvorrichtung ausgelöst wird, oder die Sicherheitsfunktion zur Zuhaltung der Tür einer Waschmaschine.



Legende

- Lösung 1** Ein wesentlicher Teil der Risikominderung erfolgt durch andere Schutzmaßnahmen als durch die Sicherheitsfunktion (z. B. mechanische Maßnahmen), ein kleiner Beitrag zur Risikominderung erfolgt durch eine Sicherheitsfunktion (z. B. Schutz- oder Verriegelungsfunktion).
- Lösung 2** Ein wesentlicher Teil der Risikominderung erfolgt durch die Sicherheitsfunktion, ein kleiner Beitrag zur Risikominderung erfolgt durch andere Schutzmaßnahmen als durch die Sicherheitsfunktion.

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

Bild 3 — Überblick über die Maßnahmen 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.

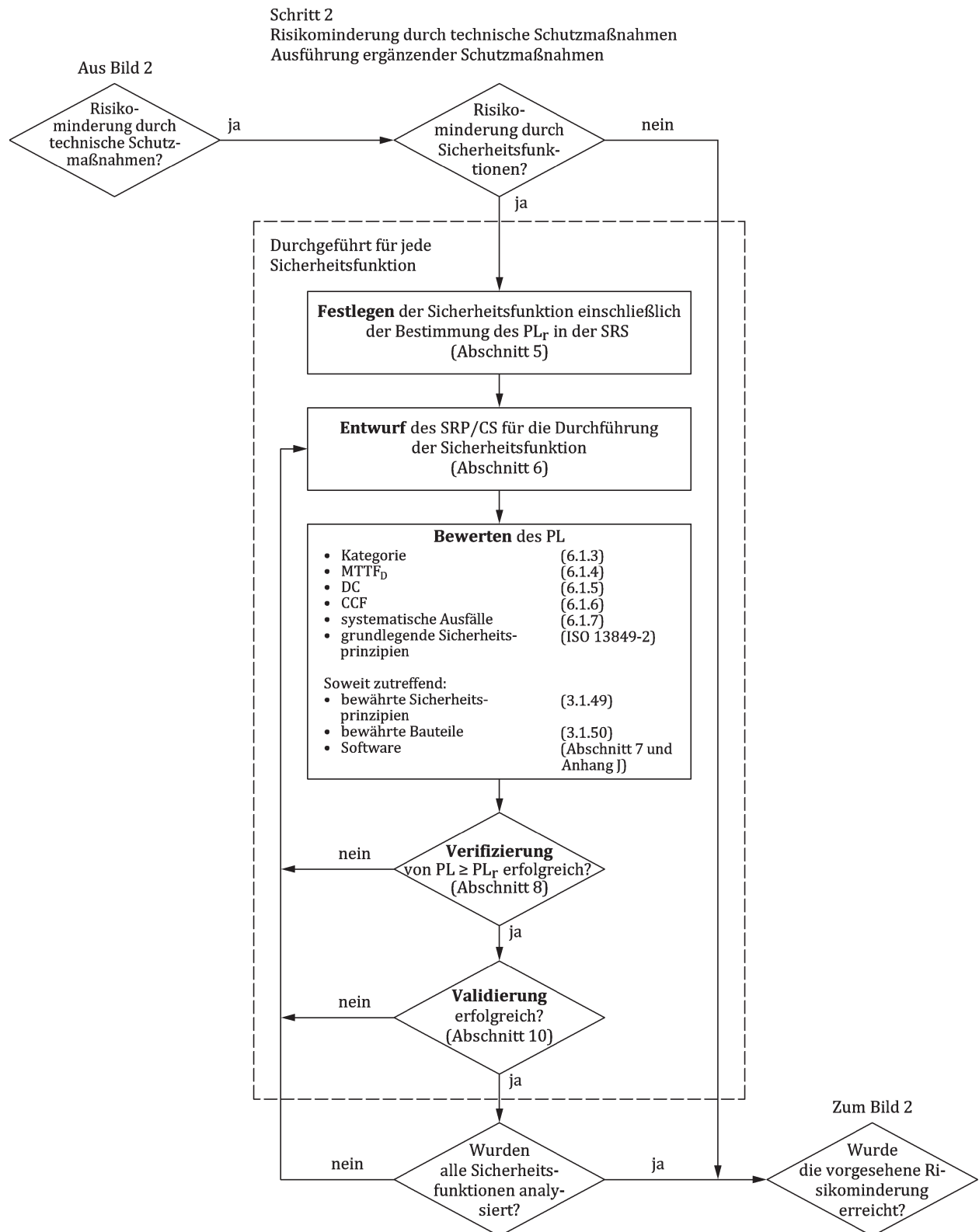


Bild 4 — Iterativer Prozess für den Entwurf von sicherheitsbezogenen Teilen von Steuerungen (SRP/CS)

4.4 Verfahren

Dieses Dokument beschreibt das folgende Verfahren:

- a) Spezifikation der Sicherheitsfunktionen (Abschnitt 5);
- b) Entwurf und technische Umsetzung der Sicherheitsfunktionen einschließlich der Identifizierung der SRP/CS und deren Teilsysteme, die die jeweiligen Sicherheitsfunktionen ausführen;
 - 1) Entwurfsaspekte (Abschnitt 6);
 - 2) Software-Sicherheitsanforderungen (Abschnitt 7);
- c) Verifizierung, ob der erreichte PL dem PL_r entspricht (Abschnitt 8);
- d) ergonomische Entwurfsaspekte (Abschnitt 9);
- e) Validierung (Abschnitt 10 oder ISO 13849-2:2012);
- f) Instandhaltung (Abschnitt 11);
- g) technische Dokumentation (Abschnitt 12);
- h) Benutzerinformation (Abschnitt 13).

Der erforderliche Performance Level (PL_r) entspricht der von der Sicherheitsfunktion zu erbringenden Risikominderung. Je höher der Beitrag zur erforderlichen Risikominderung ist (in Abhängigkeit vom Ausgangsrisiko), desto höher muss die erforderliche sicherheitsbezogene Leistungsfähigkeit sein. Die Performance Level der Sicherheitsfunktion werden im Hinblick auf die mittlere Häufigkeit 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 festgelegten Bereiche der Häufigkeit eines gefahrbringenden Ausfalls je Stunde sind in Tabelle 2 angegeben.

Tabelle 2 — Performance Level

PL	Mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde (PFH) 1/h
a	$10^{-5} \leq PFH < 10^{-4}$
b	$3 \times 10^{-6} \leq PFH < 10^{-5}$
c	$10^{-6} \leq PFH < 3 \times 10^{-6}$
d	$10^{-7} \leq PFH < 10^{-6}$
e	$PFH < 10^{-7}$
ANMERKUNG Es wird davon ausgegangen, dass der PFH-Wert mit dem PFH nach IEC 62061:2021 und der Normenreihe 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, sind die folgenden Informationen notwendig:

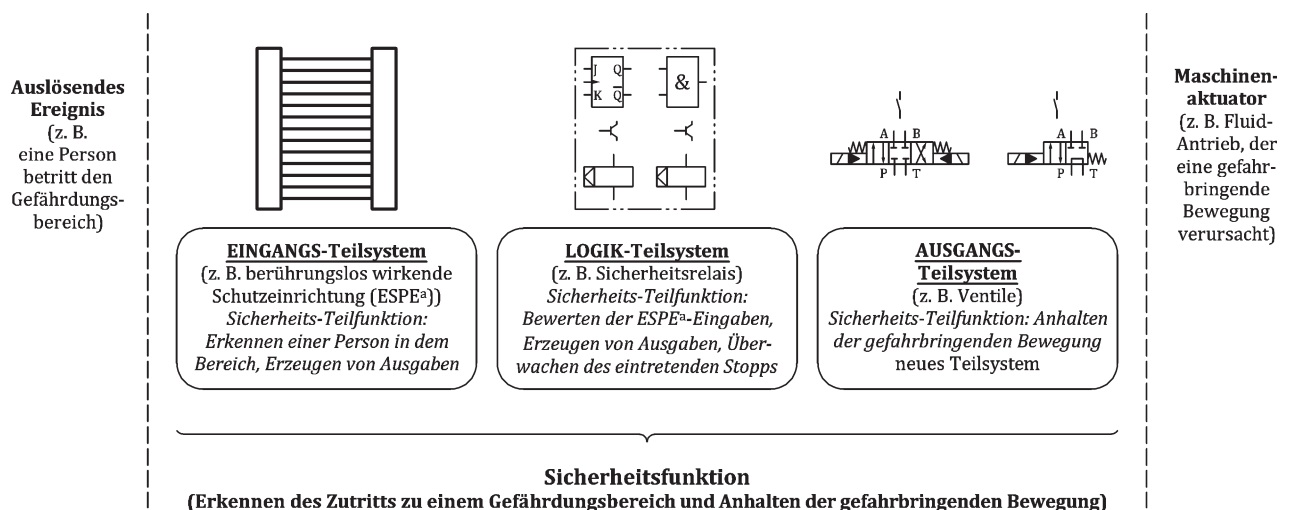
- die Ergebnisse der Risikobeurteilung der Maschine oder eines Teils davon;
- Informationen über alle Sicherheitsfunktionen (siehe Abschnitt 5), die für den Prozess zur Risikominderung bei jeder Gefährdung als notwendig ermittelt wurden. Dazu gehört:
 - eine ausführliche Beschreibung jeder Sicherheitsfunktion einschließlich ihres Beitrags zur Risikominderung (siehe 5.2);
 - die Bestimmung des erforderlichen Performance Levels (PL_r) für jede Sicherheitsfunktion (siehe 5.3).

ANMERKUNG Diese Informationen können in den zutreffenden Typ-C-Normen enthalten sein.

4.6 Ausführung von Sicherheitsfunktionen mithilfe von Teilsystemen

Die Ausführung einer Sicherheitsfunktion kann erfolgen:

- mithilfe von bereits zuvor nach diesem Dokument, nach IEC 62061:2021, nach der Normenreihe IEC 61508 oder nach sonstigen maßgebenden sicherheitsbezogenen Produktnormen (z. B. nach der Normenreihe IEC 61496 und nach 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 (ESPE, en: electrosensitive protective equipment)

Bild 5 — Beispiel für eine Kombination von Teilsystemen

5 Spezifikation der Sicherheitsfunktionen

5.1 Identifizierung und allgemeine Beschreibung der Sicherheitsfunktion

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 ausgeführt wird. Der Prozess zum Festlegen von Sicherheitsfunktionen erfordert ausführliche Angaben aus der Risikobeurteilung, die nach ISO 12100:2010 durchgeführt wurde.

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) Leistungssteuerungselement(e).

Die Spezifikation der Sicherheitsfunktion kann nach ISO 12100:2010, 6.2.11, erfolgen und einen Teil der Entwurfsspezifikation für das SRP/CS nach diesem Dokument darstellen.

Abschnitt 5 behandelt die folgenden Schritte:

- a) allgemeine Beschreibung der Sicherheitsfunktion (Verknüpfung der Gefährdungen mit den Sicherheitsfunktionen);
- b) ausführliche Beschreibung der Sicherheitsanforderungen (siehe 5.2);
- c) Bestimmung des PL_r für jede Sicherheitsfunktion (siehe 5.3);
- d) Überprüfung der SRS (siehe 5.4).

5.2 Spezifikation der Sicherheitsanforderungen

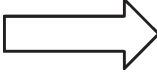
5.2.1 Allgemeine Anforderungen

5.2.1.1 Allgemeines

Die SRS bildet die Grundlage für alle SRP/CS-Entwurfstätigkeiten und muss Einzelheiten zu jeder auszuführenden Sicherheitsfunktion dokumentieren.

Die SRS liefert die notwendigen Informationen am Übergang vom Risikobeurteilungs- und -minderungsprozess nach ISO 12100:2010 zum SRP/CS-Entwurfs- und -Bewertungsprozess nach diesem Dokument, insbesondere wenn diese beiden Prozesse von unterschiedlichen Personen oder Organisationen durchgeführt werden (siehe Tabelle 3).

Tabelle 3 — Übergang vom Risikobeurteilungs- und -minderungsprozess nach ISO 12100:2010 zum SRP/CS-Entwurfs- und -Bewertungsprozess nach ISO 13849-1 (dieses Dokument)

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 und erforderliche Gesamtrisikominderung — Betriebseigenschaften der Maschine, z. B. bestimmungsgemäße Verwendung — Handlungen im Notfall — Beschreibung der Wechselwirkung verschiedener Arbeitsprozesse und manueller Aktionen, z. B. Instandsetzung — ergonomische Aspekte — Anwendungsgrenzen in Zusammenhang mit den Umgebungsbedingungen 		<p>Erforderliche Sicherheitsfunktionen (Beispiele):</p> <p>1) Verriegelungsfunktion</p> <ul style="list-style-type: none"> — Betriebsart (alle) — Auslösung durch: Öffnen einer beweglichen trennenden Schutzeinrichtung — sicherheitsbezogene Reaktion: sicher abgeschaltetes Drehmoment (STO) aller Bewegungen — PL_r d — Ansprechzeit — usw. <p>2) sicher begrenzte Geschwindigkeit (SLS: en: safely limited speed)</p> <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_r c — Ansprechzeit — usw.

5.2.1.2 Notwendige Informationen für die Erstellung der Spezifikation der Sicherheitsanforderungen (SRS)

ANMERKUNG 1 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 SRSs 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) der Betriebsarten (z. B. lokale Betriebsart, Automatikbetrieb, Betrieb mit Bezug zu einem Bereich oder Teil der Maschine);
 - 4) der/den Betriebsart(en), während der/denen die Sicherheitsfunktion aktiviert sein muss;
 - 5) der Zyklusdauer; und
 - 6) der Ansprechzeit nach ISO 13855:2010, 5.1, bis ein sicherer Zustand erreicht ist;

ANMERKUNG 2 Die Ansprechzeit der Steuerung ist Teil der Gesamt-Ansprechzeit der Maschine. Die erforderliche Gesamt-Ansprechzeit der Maschine kann den Entwurf des sicherheitsbezogenen Teils beeinflussen, z. B. die Notwendigkeit, eine Bremse bereitzustellen.

ANMERKUNG 3 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+AMD1:2021, 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 Abschnitt A.4).

5.2.1.3 Festlegung aller Sicherheitsfunktionen in der Spezifikation der Sicherheitsanforderungen (SRS)

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

- a) die Kurzbeschreibung/Bezeichnung der Sicherheitsfunktion;
- 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 (siehe 5.3);
- e) die Ansprechzeit der Maschine zum Erreichen eines sicheren Zustands, nachdem der Befehl im Zuge der Sicherheitsfunktion ausgelöst wurde, z. B. der Nachlauf des gesamten Systems (Reaktionszeit plus Nachlauf) nach ISO 13855:2010;
- f) die Betriebsart(en), während der/denen die Sicherheitsfunktion aktiviert sein muss;
- g) Schnittstellen der Sicherheitsfunktion mit der Maschinensteuerung und anderen 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 ein kontrollierter Halt ist nicht möglich, dann kann eine Reaktion auf einen Fehler ausgelöst werden, indem ein sofortiger unkontrollierter Halt verwendet wird.

- i) das Verhalten der Maschine bei Energieverlust (siehe 5.2.2.8);

BEISPIEL 3 Es kann notwendig sein, eine vertikale Achse in Position zu halten, um einen Absturz aufgrund der Schwerkraft 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. Eine geeignete konstruktive Lösung kann der Einbau von Rückschlagventilen an Zylindern oder zusätzliche mechanische Bremsen sein. Dies 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 Häufigkeit der Anforderung des SRP/CS;
- k) die Priorität der Sicherheitsfunktionen, die gleichzeitig aktiv sein können und dadurch zu Konflikten führen können;

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

BEISPIEL 5 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);
- m) die Bedingungen, um den Wiederanlauf nach der Aktivierung der Sicherheitsfunktion zu erlauben.

ANMERKUNG Das automatische Rückstellen einer Sicherheitsfunktion ist in Situationen angebracht, in denen die kontinuierliche Erkennung einer Person die Gefährdungssituation verhindert.

Siehe 5.2.2 und Anhang M für typische Sicherheitsfunktionen und deren Eigenschaften und sicherheitsbezogenen Parameter.

5.2.2 Anforderungen an spezifische Sicherheitsfunktionen

5.2.2.1 Allgemeines

Dieser Unterabschnitt enthält zusätzliche Anforderungen an spezifische Sicherheitsfunktionen, die allgemein in vielen SRP/CS angewendet werden.

5.2.2.2 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 entweder der übergeordneten Steuerung oder den anderen Maschinen oder beiden eine solche Stopp-Bedingung zu signalisieren.

Als Ergebnis der Risikobeurteilung können sicherheitsbezogene Stopp-Funktionen entsprechend den Stopp-Kategorien von IEC 60204-1:2016+AMD1:2021, 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 sichere Bedingungen für den Wiederanlauf gegeben sind. Siehe auch Tabelle M.1.

5.2.2.3 Manuelle Rückstellfunktion

Die Wiederherstellung der Sicherheitsfunktion durch die Rückstellung der Schutzeinrichtung hebt den Stopp-Befehl auf. Wenn die Risikobeurteilung dies ergibt, 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
- darf nur durch einen überwachten Signalwechsel erfolgen, um eine vorhersehbare Fehlanwendung zu vermeiden.

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

ANMERKUNG Oftmals ist die manuelle Rückstellfunktion keine separate zusätzliche Sicherheitsfunktion, wenn der sichere Zustand weiterhin von einer Sicherheitsfunktion aufrechterhalten wird (Sicherheitszustand), z. B. ausgelöst von einer Schutzeinrichtung (Abdeckung), die nicht hintertreten werden kann.

Der Aktuator 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. Ist ein spezifischer Ablauf für die Rückstellung oder eine Überwachung des Bereichs nicht möglich, müssen andere, gleichwertige risikomindernde Maßnahmen angewendet werden.

BEISPIEL Eine Lösung ist die Durchführung der Rückstellung in einer bestimmten Reihenfolge. Die Rückstellfunktion wird innerhalb des Gefährdungsbereichs durch den ersten Aktuator in Kombination mit einem zweiten Aktuator 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.

5.2.2.4 Wiederanlauffunktion

Ein Wiederanlauf darf nur dann automatisch erfolgen, wenn der sichere Zustand sichergestellt ist. Insbesondere muss ISO 12100:2010, 6.3.3.2.5, bei trennenden Schutzeinrichtungen mit Startfunktion angewendet werden.

BEISPIEL Während des Automatikbetriebs einer Maschine werden häufig Sensorrückmeldungen an die Steuerung genutzt, um den Prozessablauf zu steuern. Wenn ein Werkstück seine Position verlässt, wird der Prozessablauf gestoppt. Wenn die Überwachung der verriegelnden trennenden Schutzeinrichtung keinen Vorrang vor der automatischen Steuerung hat, kann eine Gefahr bestehen, dass die Maschine unerwartet wieder anläuft, wenn die Bedienperson der Maschine die Lage des Werkstücks korrigiert. Deshalb sollte der automatische Wiederanlauf nicht erlaubt werden, bis die trennende Schutzeinrichtung wieder geschlossen ist und der Bediener den Gefährdungsbereich verlassen hat. Der Beitrag zur Verhinderung eines unerwarteten Anlaufs (siehe ISO 14118:2017) durch die Steuerung hängt vom Ergebnis der Risikobeurteilung ab.

Siehe auch Tabelle M.1.

5.2.2.5 Lokale Steuerungsfunktion

Wird eine Maschine lokal gesteuert, z. B. durch eine tragbare Steuereinheit, die ein tragbares Gerät oder eine Hängebedienungs- oder -tafel sein kann, müssen folgende Anforderungen erfüllt werden:

- die Mittel zur Freigabe der lokalen Steuerung müssen außerhalb des Gefährdungsbereichs angebracht sein;
- das Erteilen eines Befehls durch einen lokalen Steuerstand darf nur in einem Bereich möglich sein, der durch die Risikobeurteilung definiert wurde, um Gefährdungssituationen zu vermeiden;
- die Umschaltung zwischen lokaler Steuerung und einer anderen Steuerung darf keine Gefährdungssituationen erzeugen;
- das Auslösen von Befehlen von mehreren Steuerständen (lokal oder entfernt) darf nicht zu einer Gefährdungssituation führen. Es kann notwendig sein, die Verwendung anderer Steuerstände auszuschließen, wenn ein lokaler Steuerstand ausgewählt wird oder wenn bestimmte Befehle ausgelöst werden.

Siehe auch Tabelle M.1.

5.2.2.6 Überbrückungsfunktion

Die Überbrückungsfunktion (en: muting) ist ein vorübergehendes, automatisches Deaktivieren einer Sicherheitsfunktion durch die sicherheitsbezogene Steuerung einer Maschine. Sie kann verwendet werden, um den Zugang von Personen oder das Zuführen 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 Zeitverhalten der Überbrückungssensoren oder -signale dürfen keinen Überbrückungszustand bewirken.

Das Teil bzw. die Teile der Steuerung, der/die die Überbrückungsfunktion ausführt/ausführen, muss/müssen eine angemessene sicherheitsbezogene Leistungsfähigkeit aufweisen (PL nach diesem Dokument oder SIL nach IEC 62061:2021) und darf/dürfen die sicherheitsbezogene Leistungsfähigkeit 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.

5.2.2.7 Sicherheitsbezogene Parameter

Wenn sicherheitsbezogene Parameter, z. B. Position, Geschwindigkeit, Temperatur, Zeit, Drehmoment oder Druck, von voreingestellten 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, muss eine Maßnahme zur Datenkontrolle vorhanden sein, z. B. für die Kontrolle von Grenzwerten, entweder Format oder Logik der Eingangswerte oder beides. Für ergänzende Anforderungen siehe 6.3 und Tabelle M.2.

5.2.2.8 Schwankungen, Verlust und Wiederkehr der Energieversorgung

Wenn Schwankungen des Energieniveaus auftreten, die außerhalb des vorgesehenen 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.

5.2.2.9 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 gleichzeitig aktiv sein; jede gewählte Betriebsart muss deutlich erkennbar sein bzw. angezeigt werden;
- b) durch die Betriebsartenwahl selbst darf keine Maschinenbewegung ausgelöst werden. Hierzu muss eine separate Betätigung der Starteinrichtung erforderlich sein;