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)

www.din.de
www.beuth.de

3435657

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 integrety 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 — Sicherheitanforderungen — 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 Schaltmatten und Schaltplatten*

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

DIN EN ISO 14118:2018-07, *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)*

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN ISO 13849-1

Mai 2023

ICS 13.110

Ersetzt EN ISO 13849-1:2015

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

Ref. Nr. EN ISO 13849-1:2023 D

Inhalt

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 sicherheits-bezogenen 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 sicherheits-bezogenen 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)/Unter-abschnitt(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 Sicher-heitsfunktionen.

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

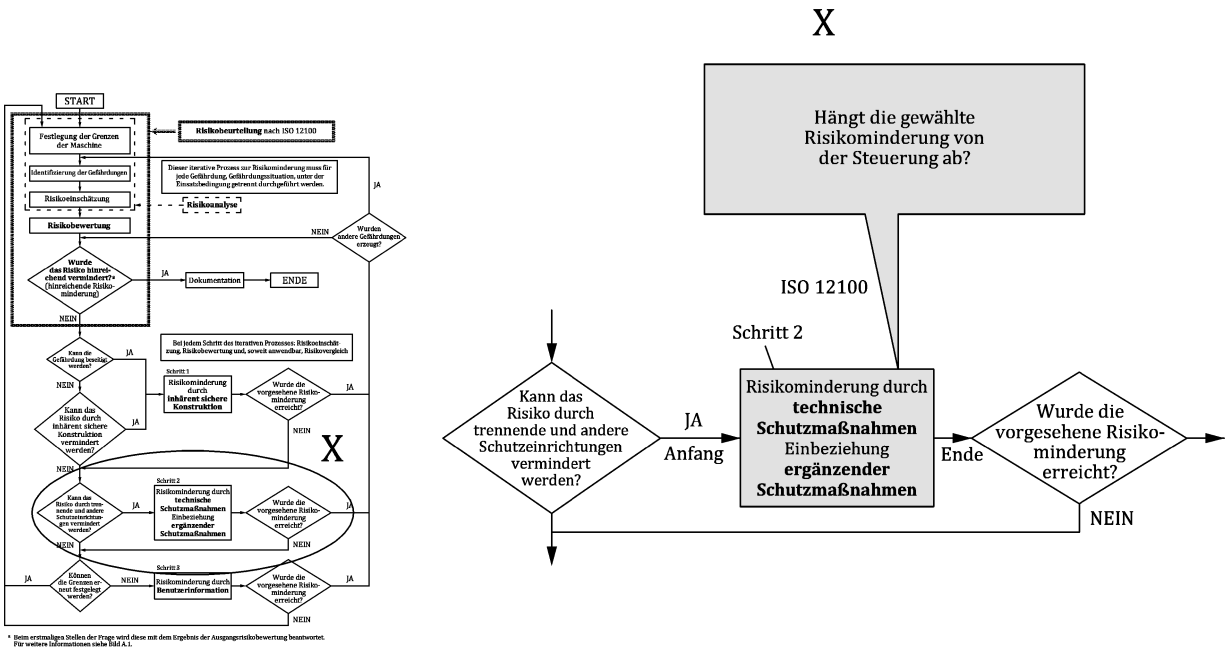
Ziel dieses Dokuments ist es, denjenigen Interessengruppen einen Leitfaden bereitzustellen, die an der Gestaltung und Beurteilung von Steuerungen beteiligt sind, sowie denjenigen, die Typ-B2- oder Typ-C-Normen erarbeiten.

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 *Risiko*minderung (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
gefahrbringender 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/Maschinenlage“ 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 *Sicherheits-funktionen* (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 *Schadens*quelle (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 *Risiko*einschätzung (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 Gesamt*ausfall*rate (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 *Ausfall*rate (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 Gefahrbereich 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, Ñ	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	Ausgabeeinheit, 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
$T_{10\mathrm{D}}$	mittlere Zeit bis 10 % der Bauteile gefahrbringend ausfallen	Anhang C

4 Überblick

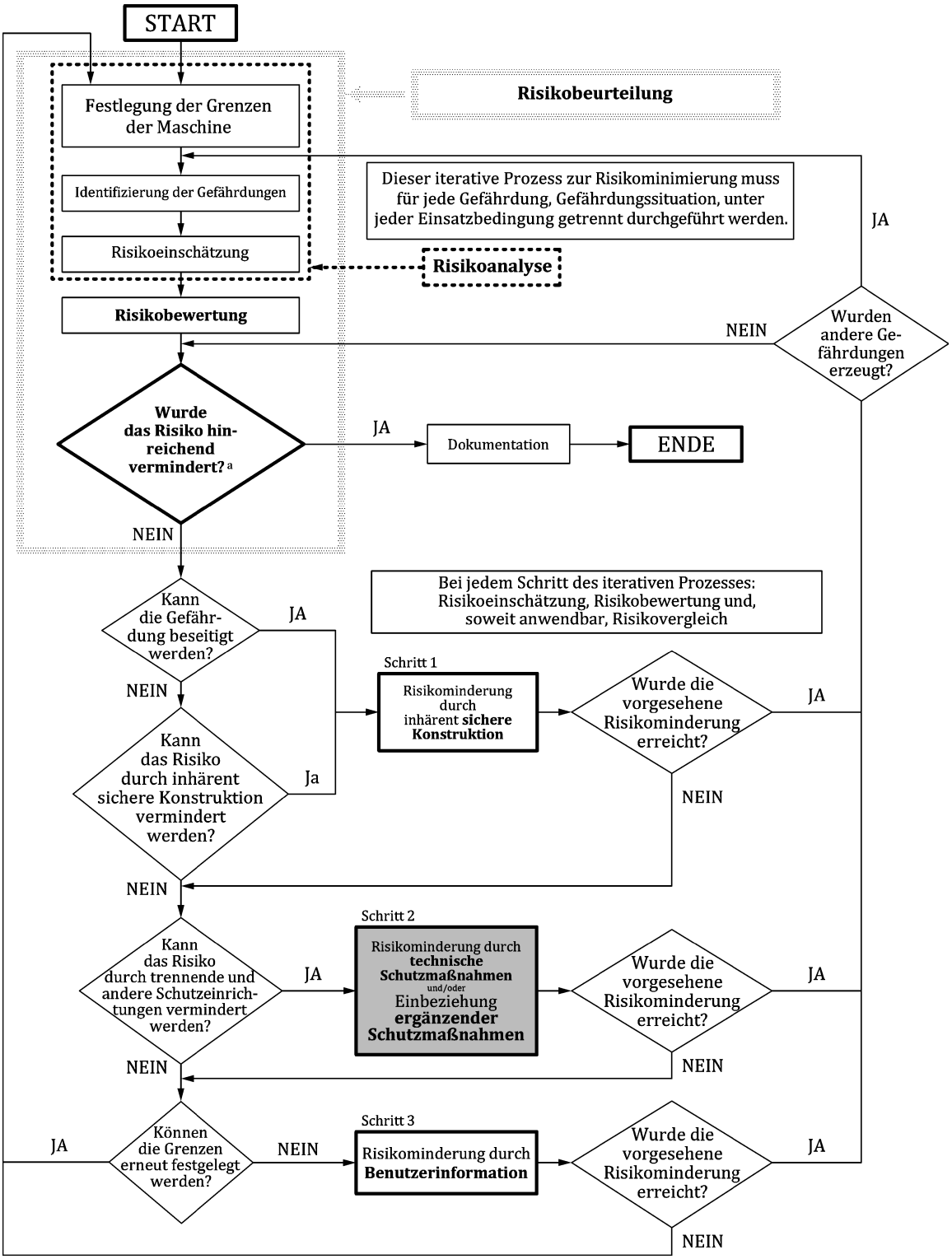
4.1 Prozess zur Risikobeurteilung und Risikominderung an der Maschine

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.

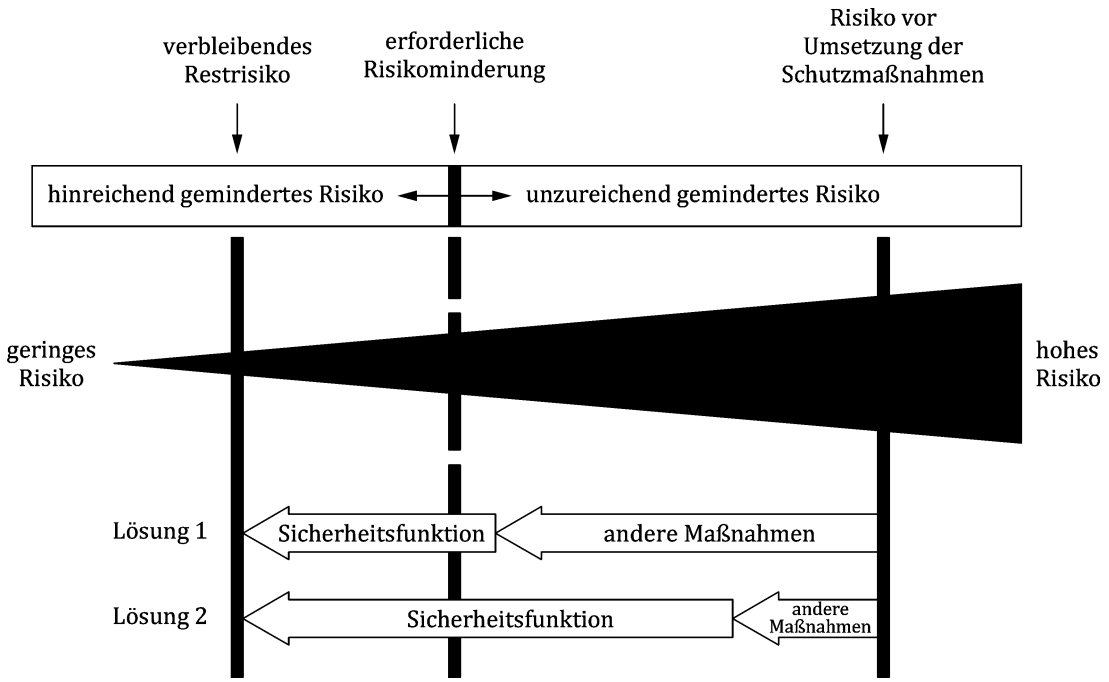
Bild 2 — Schematische Darstellung des dreistufigen iterativen Prozesses zur Risikominderung

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 Schutzeinrichtung 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.

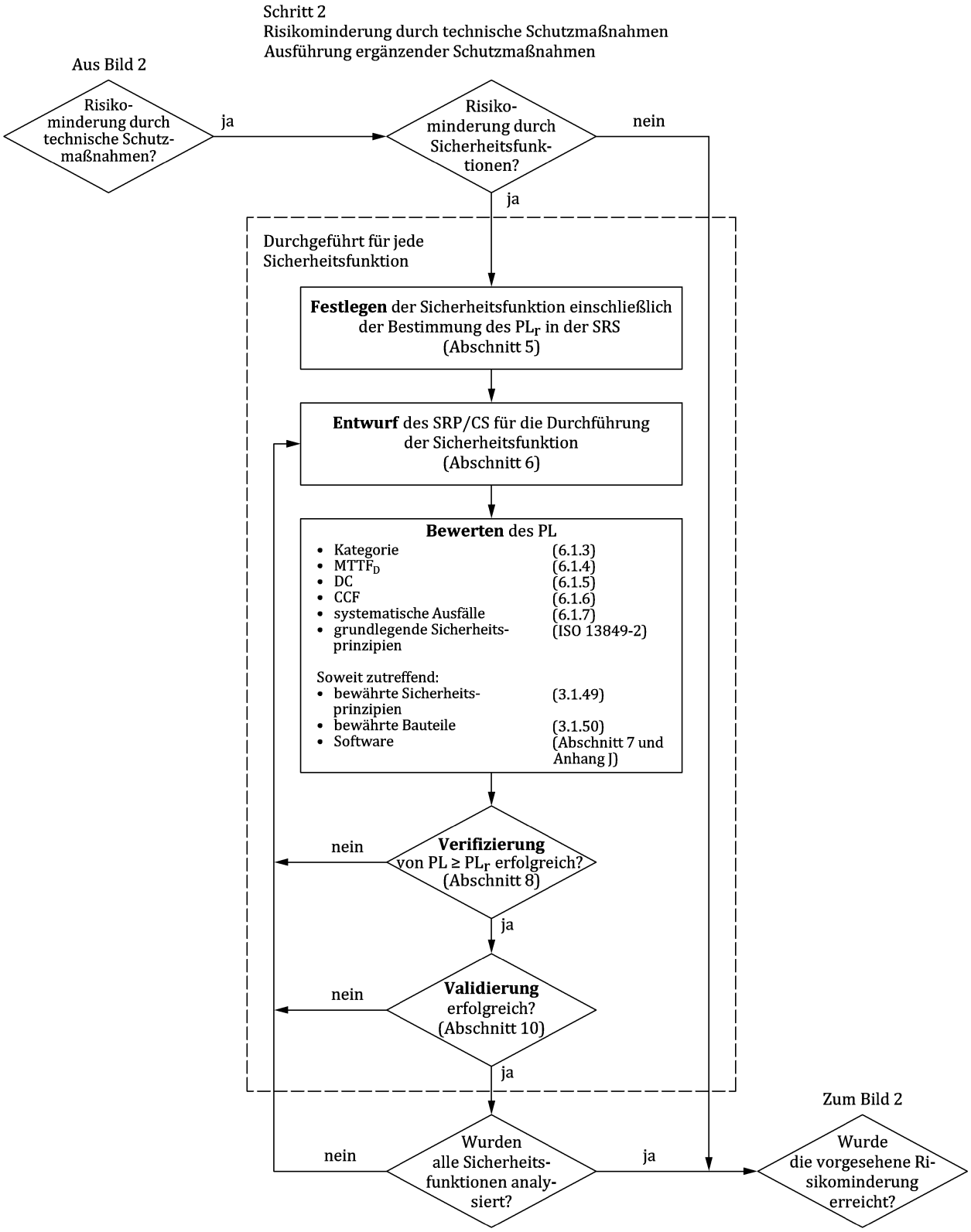


Bild 4 — Iterativer Prozess für den Entwurf von sicherheitsbezogenen Teilen von Steuerungen (SRP/CS)

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	$10^{-5} \leq \text{PFH} < 10^{-4}$
b	$3 \times 10^{-6} \leq \text{PFH} < 10^{-5}$
c	$10^{-6} \leq \text{PFH} < 3 \times 10^{-6}$
d	$10^{-7} \leq \text{PFH} < 10^{-6}$
e	$\text{PFH} < 10^{-7}$
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.

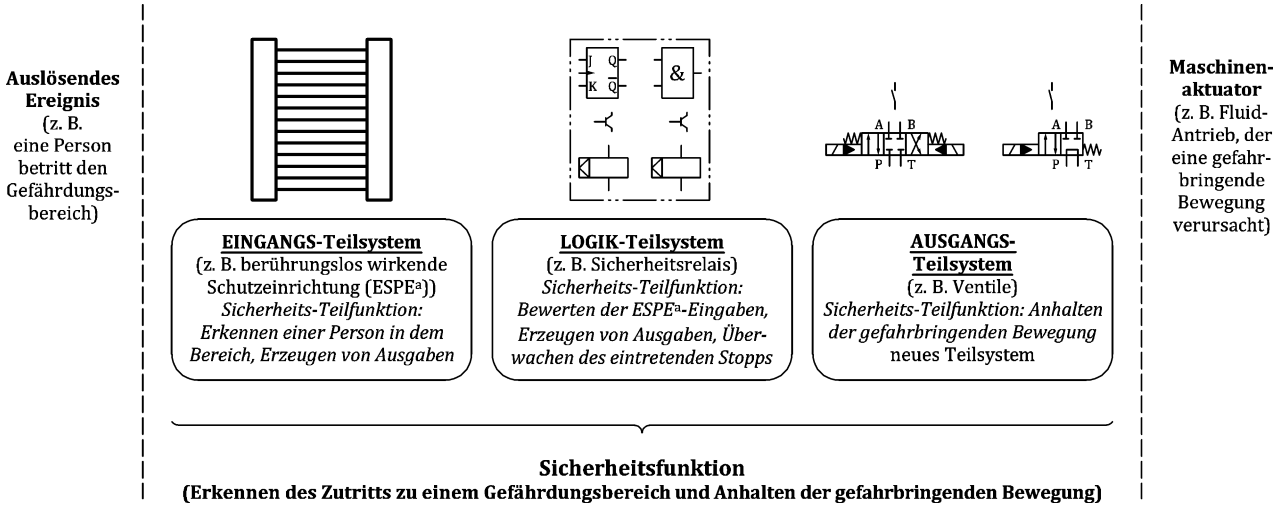
4.6 Ausführung von Sicherheitsfunktionen mithilfe von Teilsystemen

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

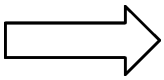
5.2.1 Allgemeine Anforderungen

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)
— 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		Erforderliche Sicherheitsfunktionen (Beispiele): 1) Verriegelungsfunktion — Betriebsart (alle) — Auslösung durch: Öffnen einer beweglichen trennenden Schutzeinrichtung — sicherheitsbezogene Reaktion: sicher abgeschaltetes Drehmoment (STO) aller Bewegungen — PL_r d — Ansprechzeit — usw. 2) sicher begrenzte Geschwindigkeit (SLS: en: safely limited speed) — 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 Hängebedienungstafel 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;

c) beim Wechsel zwischen Betriebsarten müssen Sicherheitsfunktionen und/oder risikomindernde Maßnahmen, die für die gewählte Betriebsart notwendig sind, aktiviert werden, ohne dabei während des Wechselns die beabsichtigte Risikominderung zu verlieren;

d) die Vorrichtungen für die Wahl der Betriebsart dürfen den PL der Sicherheitsfunktionen, die in dieser Betriebsart aktiv sind, nicht herabsetzen.

Siehe auch Tabelle M.1.

5.2.2.10 Sicherheitsfunktion(en) für Instandhaltungsaufgaben

Beim Entwurf der Maschine müssen die Instandhaltungsaufgaben berücksichtigt werden, die an der Maschine durchgeführt werden, und es müssen Sicherheitsfunktionen für diese Aufgaben vorgesehen werden. Die Ergebnisse der Risikobeurteilung für jede Instandhaltungsaufgabe müssen in der Spezifikation der Sicherheitsfunktionen berücksichtigt werden.

ANMERKUNG 1 Zu den Instandhaltungsaufgaben können unter anderem folgende gehören:

— Einrichten;

— Einlernen (Teachen)/Programmieren;

— Umrüsten;

— Reinigung und Sauberhaltung;

— Desinfizieren;

— geplante oder ungeplante vorbeugende Instandhaltung oder Instandsetzung;

— Fehlersuche/Fehlerbehandlung;

— Fehlerdiagnose.

Einige Instandhaltungsaufgaben erfordern eine vollständige Trennung der Maschine von allen Energiequellen und sind daher nicht vom SRP/CS abhängig. Ist für Instandhaltungsaufgaben, die entweder Energie oder Maschinenbewegungen oder beides erfordern, eine manuelle Aussetzung oder Überbrückung spezifischer Sicherheitsfunktionen erforderlich, während sich das Instandhaltungspersonal im Gefährdungsbereich aufhält, dann darf ein solcher Betrieb nur durch Bereitstellung geeigneter alternativer Sicherheitsfunktionen (z. B. Sicherheitsfunktion mit Zustimmungseinrichtung durch Sicherheitsfunktion mit Geschwindigkeitsbegrenzung) möglich sein.

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

Die folgenden Sicherheitsfunktionen, entweder einzeln oder in Kombination angewendet, sind Beispiele dafür, was häufig für Instandhaltungsaufgaben vorgesehen ist:

a) Steuerung mit Tippbetrieb;

b) Steuerung mit Zustimmeinrichtung;

c) Überwachung oder Begrenzung von z. B. der Geschwindigkeit, des Drehmoments, der Leistung, der Position, der Anordnung, der Temperatur, des Niveaus;

d) Verhindern des unerwarteten Anlaufs;

e) Abtrennen von der Energieversorgung und Energieableitung;

f) mechanische Rückhaltung oder Einhausung.

Siehe Anhang M für ergänzende Informationen.

Der Anreiz zum Aufheben bzw. Umgehen von risikomindernden Maßnahmen, die vom SRP/CS während der Instandhaltung der Maschine ausgeführt werden, muss bei der Spezifikation, beim Entwurf und bei der Auswahl des SRP/CS berücksichtigt werden (siehe 5.2.3).

Das Design von SRP/CS muss berücksichtigen, dass neben der/den vorgesehenen Bedienperson(en) weitere Personen eine Aufgabe durchführen, wie z. B.:

— ein Bediener führt Rückstell- und Wiederanlauffunktionen aus, während sich das Instandhaltungspersonal im Gefährdungsbereich aufhält;

— risikomindernde Maßnahmen, durch die eine Person geschützt werden soll, werden unangemessen für mehrere Personen eingesetzt.

In der Betriebsart für die Instandhaltung muss ein ferngesteuerter Zugriff (siehe 5.2.4) auf die Maschinensteuerung durch den Entwurf des SRP/CS verhindert werden, wenn keine angemessene Benachrichtigung oder Anzeige für Personen an der Maschine oder in deren Nähe vorhanden ist.

5.2.3 Minimierung des Anreizes zum Umgehen von Sicherheitsfunktionen

Der Anreiz zum Aufheben oder Umgehen einer Sicherheitsfunktion hängt vom Prozess, von der bestimmungsgemäßen Verwendung der Maschine (oder Teile der Maschine) und den Entwurfsdetails der risikomindernden Maßnahmen ab. Der Anreiz zum Umgehen einer Sicherheitsfunktion muss im Entwurf des SRP/CS minimiert werden.

ANMERKUNG 1 Forschungsarbeiten zum Thema Sicherheit haben gezeigt, dass viele Verletzungen entweder auf das Umgehen von Sicherheitsfunktionen oder von Schutzeinrichtungen oder beidem zurückzuführen sind. Siehe Literaturhinweise für ergänzende Informationen.

BEISPIEL Beim Entwurf von risikomindernden Maßnahmen und Sicherheitsfunktionen können folgende Sachverhalte einen Anreiz zum Umgehen geben und können berücksichtigt werden:

— die risikomindernde Maßnahme verhindert die Ausführung der Aufgabe;

— es besteht die Notwendigkeit, eine Aufgabe auszuführen, die nicht im Hinblick auf Gefährdungen und Risiken ermittelt und bewertet wurde;

— die risikomindernde Maßnahme verlangsamt die Produktion oder stört andere Aktivitäten oder Präferenzen des Benutzers;

— die risikomindernde Maßnahme ist schwierig anzuwenden;

— entweder die risikomindernde Maßnahme oder deren zugehörige Gefährdung oder beides wird vom Personal nicht als solche erkannt;

— die risikomindernde Maßnahme wird nicht als geeignet, notwendig oder angemessen für ihre Funktion angesehen;

— uneingeschränkter Zugriff auf die SRP/CS-Hardware- und -Softwaresysteme, die die Sicherheitsfunktionen umsetzen.

ANMERKUNG 2 Mithilfe von Maßnahmen zur einfachen Durchführung von Aufgaben und dem gleichzeitigen Schutz der Bediener kann der Anreiz zum Aufheben oder Umgehen von Sicherheitsfunktionen und/oder Schutzeinrichtungen gemindert werden.

ANMERKUNG 3 ISO 14119 beschreibt ein Verfahren und enthält Beispiele, wie die Möglichkeiten zum Umgehen einer Verriegelungseinrichtung minimiert werden.

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

5.2.4 Fernzugriff

Ist die Maschinensteuerung für den Fernzugriff ausgelegt, muss das SRP/CS betriebsbereit bleiben. Zusätzliche risikomindernde Maßnahmen können angewendet werden, wenn dies in den Benutzerinformationen angegeben ist.

Der Entwurf des SRP/CS darf den Fernzugriff auf eine Maschine nur dann erlauben, wenn besondere Maßnahmen vorhanden sind, die gefährliche Situationen verhindern, die durch die unbemerkte Anwesenheit von Personen im Inneren oder in der Nähe der Maschine entstehen können (z. B. siehe 5.2.2.2).

Sicherheitsbezogene Software des SRP/CS darf nicht durch Fernzugriff geändert werden können, es sei denn die lokale Validierung der Sicherheitsfunktionen wird durchgeführt.

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

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

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

ANMERKUNG 1 Es können andere Verfahren zur Bestimmung von PL_r angewendet werden (z. B. das Verfahren in IEC 62061:2021, Anhang A).

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

ANMERKUNG 3 Da das Verfahren zur Bestimmung von PL_r eine subjektive Einschätzung umfasst, ist eine gewisse Variabilität bei der praktischen Anwendung bestimmter Fälle zulässig.

ANMERKUNG 4 Der PL_r für eine Sicherheitsfunktion bestimmt die erforderliche Zuverlässigkeit, mit der die Steuerung diese Sicherheitsfunktion ausführt und die vorgesehene Risikominderung erreicht wird. Der PL_r wird mithilfe verschiedener Risikofaktoren bestimmt. Siehe auch Anhang A.

5.4 Überprüfung der Spezifikation der Sicherheitsanforderungen (SRS)

Vor dem Entwurf muss die SRS anhand der Risikobeurteilung überprüft werden. Durch die Überprüfung muss sichergestellt werden, dass alle Sicherheitsfunktionen festgelegt sind, um die vorgesehene Risikominderung an der Maschine zu erreichen. Siehe auch 10.2 für die Validierung der SRS.

Die SRS muss entsprechend den Anforderungen von 10.1.1 validiert werden.

5.5 Zerlegung eines SRP/CS in Teilsysteme

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

— die Sicherheitsanforderungen an jede Teilfunktion (Anforderungen an Funktion und Integrität);

— Eingänge und Ausgänge jeder Teilfunktion.

Ein SRP/CS kann Folgendes umfassen:

— ein oder mehrere zuvor validierte(s) Teilsystem(e);

— ein oder mehrere Teilsystem(e) basierend auf (einem) Teilsystemelement(en);

— eine Kombination der beiden vorstehenden Optionen.

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

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

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

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

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

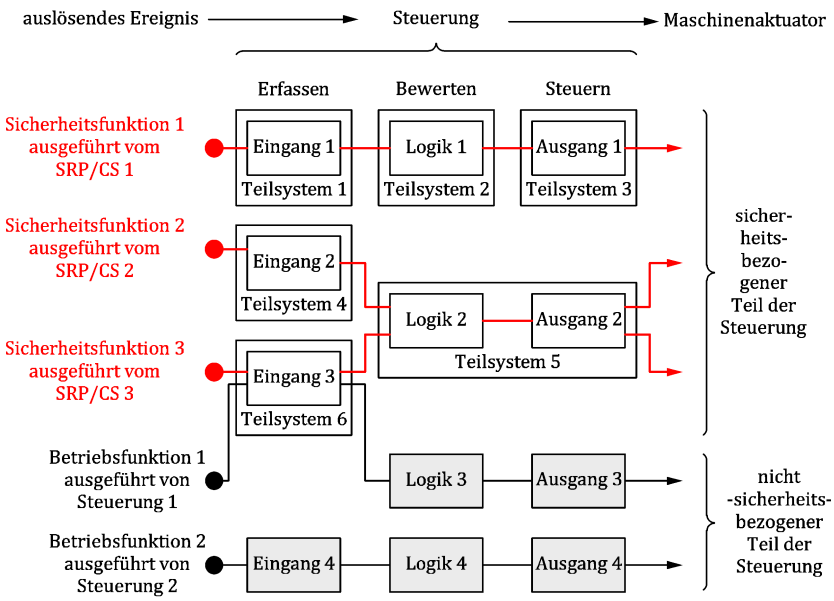


Bild 6 — Beispiel für die Zerlegung von Sicherheitsfunktionen und deren Zuordnung zu den Teilsystemen

Bild 6 zeigt ein Blockdiagramm von Teilsystemen, die zu (einem) SRP/CS kombiniert sind, mit:

— auslösendem Ereignis (z. B. Öffnen einer trennenden Schutzeinrichtung, Unterbrechen eines Strahls einer AOPD);

— Eingang (z. B. Endschalter, Sensor, AOPD) (Teilsysteme 1, 4 und 6);

— Logik/Verarbeitung (Teilsysteme 2 und 5);

— Ausgang/Leistungssteuerungselemente (z. B. Ventil, Schütz, Stromrichter, Bremsen) (Teilsysteme 3 und 5);

— Aktuator der Maschine (z. B. Motor, Zylinder);

— Verbindungen (z. B. elektrisch, optisch).

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

ANMERKUNG 4 Ein SRP/CS kann als ein einziges Teilsystem mit einem Sensor, Logikeinheiten und Leistungssteuerungselementen ausgeführt werden. Ein Beispiel für die Ausführung eines SRP/CS aus einem einzigen Teilsystem ist eine „intelligente" Sensoreinheit (z. B. Lichtvorhang, Laserscanner) mit integrierter Ausgangsschalteinrichtung (z. B. Relais zum Ausschalten einer gefährlichen Bewegung).

ANMERKUNG 5 Ein Teilsystem oder ein SRP/CS kann Sicherheitsfunktionen und normale Steuerungsfunktionen ausführen. Der Konstrukteur kann jede verfügbare Technologie, einzeln oder in Kombination, verwenden. Ein SRP/CS kann auch eine Betriebsfunktion bereitstellen (z. B. eine AOPD als Möglichkeit zur Auslösung eines Zyklus).

Der Konstrukteur eines zuvor validierten Teilsystems muss die entsprechenden Informationen nach 13.2 bereitstellen.

ANMERKUNG 6 Der Konstrukteur eines zuvor validierten Teilsystems kann ein Systemintegrator, ein Maschinenhersteller oder ein Bauteilhersteller sein.

6 Entwurfsaspekte

6.1 Bewertung des erreichten Performance Levels

6.1.1 Allgemeine Übersicht der Performance Level

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

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

a) der Architektur (siehe 6.1.3);

   1) Zuweisung einer Kategorie zum Teilsystem;

   2) Bewerten, ob die geltenden qualitativen (nicht quantifizierbaren) Anforderungen der Kategorie erfüllt sind, einschließlich:

      — grundlegende Sicherheitsprinzipien (ISO 13849-2:2012, Tabelle A.1, Tabelle B.1, Tabelle C.1 und Tabelle D.1);

      — bewährte Sicherheitsprinzipien (ISO 13849-2:2012, Tabelle A.2, Tabelle B.2, Tabelle C.2 und Tabelle D.2);

      — bewährte Bauteile (ISO 13849-2:2012, Tabelle A.3 und Tabelle D.3, Anhang B und Anhang C);

   3) Beurteilen, ob das erforderliche Verhalten unter Fehlerbedingungen eingehalten wird;

b) des $MTTF_D$-Werts einzelner Bauteile (siehe 6.1.4, Anhang C und Anhang D);

c) des DC (siehe 6.1.5 und Anhang E);

d) der CCF (siehe 6.1.6 und Anhang F);

e) des Einflusses des Entwurfs von sicherheitsbezogener Software auf die Funktion der Hardware (siehe Abschnitt 7 und Anhang J);

f) des Einflusses der Maßnahmen gegen systematische Ausfälle (siehe 6.1.7 und Anhang G).

ANMERKUNG 1 Weitere Parameter, z. B. funktionsbedingte Gesichtspunkte, Anforderungsrate, Testrate, können einen besonderen Einfluss haben.

ANMERKUNG 2 Für sicherheitsbezogene Werte von Bauteilen oder Komponenten der Steuerungen siehe Anhang O.

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

— quantifizierbare Aspekte ($MTTF_D$-Wert für einzelne Bauteile, DC, CCF, Architektur);

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

ANMERKUNG 3 Der Beitrag der Zuverlässigkeit (z. B. $MTTF_D$, Architektur) kann in Abhängigkeit von dem verwendeten SRP/CS variieren.

ANMERKUNG 4 Es gibt mehrere Verfahren zur Abschätzung der quantifizierbaren Aspekte des PL für beliebige Systemtypen (z. B. einer komplexen Struktur), z. B. Markov-Modelle, allgemeine stochastische Petri-Netze (GSPN), Zuverlässigkeitsblockdiagramme (siehe z. B. die Normenreihe IEC 61508, IEC 61078, die Normenreihe IEC 62021).

Um die Beurteilung des PL zu erleichtern, liefert dieses Dokument ein vereinfachtes Verfahren, das auf der Definition von fünf vorgesehenen Architekturen basiert, die spezielle Konstruktionsmerkmale aufweisen und ein spezielles Verhalten bei einem Fehler zeigen (siehe 6.1.3).

Die Anforderungen für die Bewertung des PL eines Teilsystems sind in 6.1 angegeben. Ein vereinfachter Ansatz für die Bewertung des PL eines Teilsystems ist in 6.1.8 (Bild 12) und 6.1.9 angegeben, zusammen mit dem Verfahren von Anhang B bis Anhang H, Anhang J, Anhang K und Anhang L. Für die Bewertung des PL von Kombinationen von Teilsystemen siehe 6.2.

Die qualitativen Aspekte des PL und das Vermeiden von systematischen Ausfällen müssen durch Erfüllen der in diesem Dokument angegebenen Anforderungen und Anleitungen erreicht werden. Siehe 6.1.7 für systematischen Ausfall und Anhang G für Leitlinien.

Wenn in produktspezifischen Normen, wie der Normenreihe IEC 61496 für berührungslos wirkende Schutzeinrichtungen (ESPE, en: electrosensitive protective equipment) oder der Normenreihe ISO 13856 für druckempfindliche Schutzeinrichtungen, Anforderungen zum Vermeiden oder Steuern systematischer oder zufälliger Ausfälle festgelegt sind, müssen solche Teilsysteme zusätzlich zu den in diesem Dokument festgelegten Anforderungen die Anforderungen dieser Produktnormen erfüllen.

Es müssen risikomindernde Maßnahmen angewendet werden und Folgendes muss erfüllt sein:

— Verringerung der Wahrscheinlichkeit von Fehlern auf Bauteilebene, welche die Sicherheitsfunktion beeinflussen. Dies kann erreicht werden durch Erhöhung der Zuverlässigkeit der Bauteile, z. B. durch entweder die Auswahl von bewährten Bauteilen oder durch die Anwendung von bewährten Sicherheitsprinzipien oder durch beides, um damit kritische Fehler oder Ausfälle zu minimieren oder auszuschließen (siehe auch ISO 13849-2:2012);

— Verbesserung der Architektur des Teilsystems, um den gefährlichen Einfluss eines Fehlers zu vermeiden. Einige Fehler können eine Erkennung erfordern, wodurch entweder eine redundante oder eine überwachte Struktur oder beides notwendig wird.

Die Reduzierung der Fehlerwahrscheinlichkeit und die Vermeidung gefährlicher Auswirkungen von Fehlern können separat oder in Kombination ausgeführt werden. In Abhängigkeit von den Technologien kann dies erreicht werden durch:

— die Auswahl von zuverlässigen Bauteilen und durch Fehlerausschluss; oder

— die Sicherheitsfunktion mit entweder einer redundanten oder einer überwachten Struktur oder beidem.

Die Struktur einschließlich der Fehlertoleranz und der Fehlererkennung sind wichtige Parameter für die Bestimmung des PL. Architektureinschränkungen begrenzen den maximal erreichbaren PL der Kategorie B, 1 und 2. Für diese Architektureinschränkungen siehe 6.1.3.2.2 bis 6.1.3.2.4.

Anforderungen an die Verhinderung oder Vermeidung von CCFs müssen erfüllt sein.

Für Teilsysteme, deren PL- oder SIL-Werte und PFH-Werte vom Hersteller angegeben werden, ist keine weitere Einschätzung (z. B. Bewertung von DC, $MTTF_D$, CCF, SRESW) notwendig. Siehe auch Tabelle O.1.

6.1.2 Zusammenhang zwischen dem Performance Level (PL) und dem Sicherheits-Integritätslevel (SIL)

Wenn eine Sicherheitsfunktion mit einem oder mehreren Teilsystem(en) entworfen wird, muss jedes Teilsystem entweder mithilfe von PL nach diesem Dokument oder mithilfe von SIL nach IEC 62061:2021 oder nach der Normenreihe IEC 61508 gestaltet werden. Teilsysteme, die nach der Normenreihe IEC 61508 oder nach IEC 62061:2021 entworfen sind, dürfen verwendet werden, sind aber auf solche Teilsysteme zu beschränken, die für Betriebsarten mit hoher Anforderungsrate oder Betriebsarten mit kontinuierlicher Anforderung, die Pfad 1_H nutzen, ausgelegt sind (siehe IEC 61508-2:2010, 7.4.4.2). Teilsysteme sind nach 6.2 zusammenzufassen. Siehe Tabelle 4 für die Zusammenhänge zwischen PL und SIL.

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

PL	SIL (siehe IEC 62061:2021 für Informationen) Betriebsart mit hoher Anforderungsrate/mit kontinuierlicher Anforderung
a	keine Entsprechung
b	1
c	1
d	2
e	3

ANMERKUNG 1 PL a besitzt keine Entsprechung auf der SIL-Skala und wird hauptsächlich verwendet, um das Risiko leichter, üblicherweise reversibler Verletzungen zu reduzieren.

ANMERKUNG 2 PL e entspricht SIL 3, der als der höchste Level definiert ist, der üblicherweise für Maschinen verwendet wird.

6.1.3 Architektur — Kategorien und deren Beziehung zur $MTTF_D$ jedes Kanals, zum durchschnittlichen Diagnosedeckungsgrad und zum Ausfall infolge gemeinsamer Ursache (CCF)

6.1.3.1 Allgemeines

Die nach diesem Dokument entworfenen Teilsysteme müssen den Anforderungen einer der in 6.1.3.2 festgelegten Kategorien entsprechen. Die Kategorien bilden die Grundlage für das Erreichen eines spezifischen PL. Die Kategorien beschreiben das geforderte Verhalten des Teilsystems hinsichtlich seiner Widerstandsfähigkeit gegenüber Fehlern, basierend auf den in 6.1.1 beschriebenen Entwurfsaspekten.

Kategorie B ist die grundlegende Kategorie. Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen. In Kategorie 1 wird der verbesserte Widerstand gegen Fehler überwiegend durch Anwendung qualitativ hochwertiger Bauteile erreicht. In den Kategorien 2, 3 und 4 wird eine verbesserte Leistungsfähigkeit vorwiegend durch die Verbesserung von entweder der Fehlertoleranz oder den Diagnosemaßnahmen oder von beidem erreicht. In Kategorie 2 wird dies durch wiederkehrende Überprüfung, ob die spezifizierte Teilfunktion ordnungsgemäß (fehlerfrei) ausgeführt wird, erreicht. In den Kategorien 3 und 4 wird dies erreicht, indem sichergestellt wird, dass ein einzelner Fehler nicht zum Verlust der Teilfunktion führt. In Kategorie 4 und wann immer dies in Kategorie 3 vernünftigerweise möglich ist, werden solche Fehler erkannt. Kategorie 4 ist widerstandsfähig gegenüber einer Anhäufung von Fehlern. Tabelle 5 gibt eine Übersicht über die Kategorien des Teilsystems, die Anforderungen und das Verhalten der Teilfunktion beim Auftreten von Fehlern.

Bei der Betrachtung der Ausfallursachen können für einige Bauteile bestimmte Fehler ausgeschlossen werden (siehe 6.1.10.3).

Tabelle 5 — Übersicht über die Anforderungen für Kategorien

Kategorie	Zusammenfassung der Anforderungen an die Teilsysteme	Verhalten der Teilfunktion	Prinzip zum Erreichen der Sicherheit	$MTTF_D$ jedes Funktionskanals	DC_{avg}	CCF
B (siehe 6.1.3.2.2)	Entweder die Teilsysteme oder deren Schutzeinrichtungen oder beide sowie deren Bauteile müssen in Übereinstimmung mit den zutreffenden Normen so entworfen, gebaut, ausgewählt, zusammengebaut und kombiniert werden, dass sie den zu erwartenden Einflüssen standhalten können. Grundlegende Sicherheitsprinzipien müssen angewendet werden.	Das Auftreten eines Fehlers kann zum Verlust der Teilfunktion führen.	überwiegend durch die Auswahl von Bauteilen charakterisiert	niedrig bis mittel	keiner	nicht relevant
1 (siehe 6.1.3.2.3)	Die Anforderungen von Kategorie B müssen erfüllt sein. Bewährte Bauteile und bewährte Sicherheitsprinzipien müssen angewendet werden.	Das Auftreten eines Fehlers kann zum Verlust der Teilfunktion führen, aber die Wahrscheinlichkeit des Auftretens ist geringer als in Kategorie B.	überwiegend durch die Auswahl von Bauteilen charakterisiert	hoch	keiner	nicht relevant

Kategorie	Zusammenfassung der Anforderungen an die Teilsysteme	Verhalten der Teilfunktion	Prinzip zum Erreichen der Sicherheit	$MTTF_D$ jedes Funktionskanals	DC_{avg}	CCF
2 (siehe 6.1.3.2.4)	Die Anforderungen von Kategorie B müssen erfüllt sein und bewährte Sicherheitsprinzipien müssen angewendet werden. Teilsysteme müssen in geeigneten Abständen getestet werden.	Zwischen den Tests kann das Auftreten eines Fehlers zum Verlust der Teilfunktion führen. Der Verlust der Teilfunktion wird durch den Test erkannt.	überwiegend durch die Struktur charakterisiert	niedrig bis hoch	niedrig bis mittel	siehe Anhang F
3 (siehe 6.1.3.2.5)	Die Anforderungen von Kategorie B müssen erfüllt sein und bewährte Sicherheitsprinzipien müssen angewendet werden. Ein Teilsystem muss so gestaltet werden, dass — ein einzelner Fehler in keinem dieser Teile zum Verlust der Teilfunktion führt, und — wenn immer vernünftigerweise durchführbar, der einzelne Fehler erkannt wird.	Wenn ein einzelner Fehler auftritt, bleibt die Teilfunktion immer erhalten. Einige, aber nicht alle Fehler werden erkannt. Eine Anhäufung von unerkannten Fehlern kann zum Verlust der Teilfunktion führen.	überwiegend durch die Struktur charakterisiert (Redundanz)	niedrig bis hoch	niedrig bis mittel	siehe Anhang F
4 (siehe 6.1.3.2.6)	Die Anforderungen von Kategorie B müssen erfüllt sein und bewährte Sicherheitsprinzipien müssen angewendet werden. Ein Teilsystem muss so gestaltet werden, dass — ein einzelner Fehler in keinem dieser Teile zum Verlust der Teilfunktion führt, und — der einzelne Fehler bei oder vor der nächsten Anforderung der Teilfunktion erkannt wird; wenn diese Erkennung jedoch nicht möglich ist, darf eine Anhäufung von unerkannten Fehlern nicht zum Verlust der Teilfunktion führen.	Wenn ein einzelner Fehler auftritt, bleibt die Teilfunktion immer erhalten. Durch das Erkennen von Fehleranhäufungen wird die Wahrscheinlichkeit des Verlustes der Teilfunktion verringert (hoher DC). Die Fehler werden rechtzeitig erkannt, um einen Verlust der Teilfunktion zu verhindern.	überwiegend durch die Struktur charakterisiert (Redundanz)	hoch	hoch, einschließlich der Fehleranhäufung	siehe Anhang F
ANMERKUNG Für vollständige Anforderungen siehe 6.1.3.2.						

Die Auswahl einer Kategorie für ein bestimmtes Teilsystem hängt hauptsächlich von Folgendem ab:

a) der Risikominderung, die durch die Sicherheitsfunktion erreicht werden soll, zu der dieses Teilsystem beiträgt;

b) dem erforderlichen Performance Level (PL_r);

c) der verwendeten Technologie;

d) den Auswirkungen im Fall eines Fehlers/von Fehlern in einem Element des Teilsystems;

e) den Möglichkeiten, (einen) Fehler in diesem Teilsystem zu vermeiden (systematischer Ausfall);

f) der mittleren Dauer bis zum gefahrbringenden Ausfall ($MTTF_D$);

g) dem Diagnosedeckungsgrad (DC); und

h) den CCFs bei Kategorien 2, 3 und 4.

6.1.3.2 Vorgesehene Architekturen — Spezifikation von Kategorien

6.1.3.2.1 Allgemeines

Die folgenden vorgesehenen Architekturen erfüllen die Anforderungen der zugehörigen Kategorie.

Die vorgesehenen Architekturen zeigen eine logische Darstellung der Struktur der Teilsysteme für jede Kategorie.

ANMERKUNG 1 Für Kategorie 3 und Kategorie 4 sind nicht notwendigerweise alle Teile physisch redundant, sondern es stehen redundante Mittel bereit, um sicherzustellen, dass ein einzelner Fehler nicht zum Verlust der Teilfunktion führen kann. Deshalb kann die technische Umsetzung (z. B. das Schaltbild) von der logischen Darstellung der Architektur abweichen.

Bild 7 bis Bild 11 zeigen keine Beispiele, sondern allgemeine vorgesehene Architekturen. Eine Abweichung von diesen Architekturen ist immer möglich, aber jede Abweichung muss durch angemessene analytische Werkzeuge wie z. B. Markov-Modelle, Fehlerbaumanalyse (FTA) begründet werden, sodass das Teilsystem den erforderlichen Performance Level (PL_r) erreicht. Für ein Teilsystem, das von den vorgesehenen Architekturen abweicht, muss eine ausführliche Berechnung durchgeführt werden, um das Erreichen des PL_r nachzuweisen.

Die Linien und Pfeile in Bild 7 bis Bild 11 stellen logische Verbindungsmittel und, soweit zutreffend, logische Diagnosemaßnahmen dar.

ANMERKUNG 2 Die Struktur eines Teilsystems ist ein Schlüsselmerkmal mit großem Einfluss auf den PL. Auch wenn die Vielfalt der möglichen Strukturen groß ist, sind die grundlegenden Konzepte oft ähnlich. So können die meisten Strukturen, die im Bereich der Maschinen existieren, auf eine der Kategorien abgebildet werden. Für jede Kategorie kann eine typische Darstellung in Form eines sicherheitsbezogenen Blockdiagramms gemacht werden. Diese typischen Ausführungen werden vorgesehene Architektur genannt und im Zusammenhang mit den folgenden Kategorien aufgelistet.

Wenn das vereinfachte Verfahren von 6.1.8 angewendet wird, um den PL abzuschätzen, muss die Architektur des Teilsystems der vorgesehenen Architektur der geforderten Kategorie entsprechen.

6.1.3.2.2 Kategorie B

Ein Teilsystem der Kategorie B muss mindestens nach den zutreffenden Normen entworfen, gebaut, ausgewählt, zusammengestellt und kombiniert worden sein und die grundlegenden Sicherheitsprinzipien (siehe auch ISO 13849-2:2012) für die spezifische Anwendung nutzen, um Folgendem standzuhalten:

— den zu erwartenden Betriebsbeanspruchungen, z. B. die Zuverlässigkeit bezüglich des Schaltvermögens und der Schalthäufigkeit;

— dem Einfluss des verarbeiteten Materials, z. B. die Reinigungsmittel in einer Waschmaschine; und

— anderen relevanten äußeren Einflüssen, z. B. mechanische Schwingungen, elektromagnetische Störungen (EMI, en: electromagnetic interference), Unterbrechungen oder Störungen der Energieversorgung.

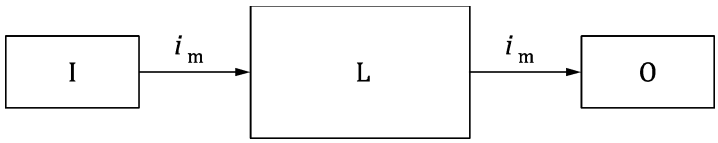
Die $MTTF_D$ des Kanals muss mindestens niedrig sein.

Der maximale PL, der mit Kategorie B erreicht werden kann, ist PL b.

ANMERKUNG 1 In Architekturen der Kategorie B gibt es keinen durchschnittlichen Diagnosedeckungsgrad (DC_{avg} = keiner). In solchen Strukturen ist die Betrachtung von CCF nicht relevant.

ANMERKUNG 2 Bei Auftreten eines Fehlers kann dies zum Verlust der Teilfunktion führen.

Spezifische Anforderungen an die elektromagnetische Verträglichkeit (Anforderungen an die Störfestigkeit) sind in den maßgebenden Produktnormen bzw. Fachgrundnormen enthalten. Anforderungen an die Störfestigkeit sind für Teilsysteme besonders wichtig. Teilsysteme mit aktiven elektronischen Bauteilen müssen ausgehend von ihrer Umgebung den Anforderungen an die elektromagnetische Störfestigkeit entsprechen, soweit angemessen. Für einen praktischen Leitfaden siehe Anhang L.



Legende
i_m Verbindungsmittel
I Eingabegerät, z. B. Sensor
L Logik
O Ausgabegerät, z. B. Hauptschütz

Bild 7 — Vorgesehene Architektur für Kategorie B

6.1.3.2.3 Kategorie 1

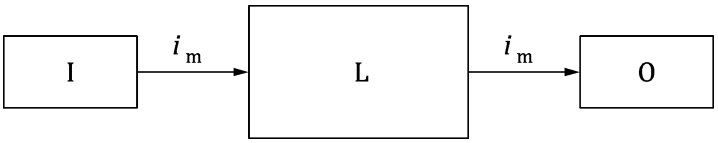
Für Kategorie 1 müssen die gleichen Anforderungen erfüllt sein wie für Kategorie B nach 6.1.3.2.2. Zusätzlich gilt Folgendes.

Teilsysteme der Kategorie 1 müssen unter Verwendung bewährter Bauteile nach 6.1.11 und bewährter Sicherheitsprinzipien (siehe 3.1.49 und ISO 13849-2:2012) entworfen und gebaut werden. Die $MTTF_D$ des Kanals muss hoch sein.

ANMERKUNG 1 In Architekturen der Kategorie 1 gibt es keinen durchschnittlichen Diagnosedeckungsgrad (DC_{avg} = keiner). In solchen Strukturen (Einkanalsysteme) ist die Betrachtung von CCF nicht relevant.

Der maximale PL, der mit Kategorie 1 erreicht werden kann, ist PL c.

ANMERKUNG 2 Bei Auftreten eines Fehlers kann dies zum Verlust der Sicherheitsfunktion führen. Jedoch ist die $MTTF_D$ in dem einzelnen Kanal der Kategorie 1 größer als in Kategorie B. Folglich ist der Verlust der Sicherheitsfunktion weniger wahrscheinlich.



Legende
i_m Verbindungsmittel
I Eingabegerät, z. B. Sensor
L Logik
O Ausgabegerät, z. B. Hauptschütz

Bild 8 — Vorgesehene Architektur für Kategorie 1

6.1.3.2.4 Kategorie 2

Für Kategorie 2 müssen die gleichen Anforderungen erfüllt sein wie für Kategorie B nach 6.1.3.2.2. „Bewährte Sicherheitsprinzipien“ nach 3.1.49 und ISO 13849-2:2012 müssen ebenfalls befolgt werden. Zusätzlich gilt Folgendes.

Teilsysteme der Kategorie 2 müssen so entworfen werden, dass deren Funktionskanal (I, L, O) in geeigneten Abständen getestet wird. Das Testen der Teilfunktion(en) muss entweder vor oder zumindest bei Anforderung der Sicherheitsfunktion erfolgen, bevor eine Gefährdungssituation eintritt, z. B.:

a) vor dem Beginn eines neuen Zyklus;

b) vor dem Anlauf anderer Bewegungen;

c) unmittelbar bei Anforderung der Sicherheitsfunktion;

d) regelmäßig während des Betriebs, wenn die Risikobeurteilung und die Betriebsart die Notwendigkeit hierfür zeigen.

Der Test selbst darf nicht zu einer Gefährdungssituation führen (z. B. aufgrund einer Erhöhung der Ansprechzeit). Die Testeinrichtung darf als Bestandteil des/der sicherheitsbezogenen Teile(s), das/die die Sicherheitsfunktion ausführt/ausführen, oder getrennt davon vorhanden sein.

Basierend auf der Risikobeurteilung der Maschine oder eines Teils davon darf das Einleiten dieses Tests manuell erfolgen. Jeder Test der Teilfunktion(en) muss entweder

— den Betrieb zulassen, wenn keine Fehler erkannt wurden, oder

— eine Ausgabe (Ausgabe der Testeinrichtung (OTE, en: output of the test equipment)) für das Auslösen geeigneter Steuerungsmaßnahmen erzeugen, wenn ein Fehler erkannt wird.

Für PL_r d muss die OTE einen sicheren Zustand einleiten, der bis zur Behebung des Fehlers beibehalten wird.

Für einen PL_r bis PL_r c muss die Ausgabe (OTE), wenn möglich, einen sicheren Zustand einleiten, der bis zur Behebung des Fehlers beibehalten wird. Wenn das Einleiten eines sicheren Zustands nicht möglich ist (z. B. durch Verschweißen des Kontakts des finalen Schaltglieds), kann es ausreichen, wenn die OTE eine Warnung ausgibt.

Die Berechnung von DC_{avg} darf nur die Blöcke des Funktionskanals berücksichtigen (d. h. I, L und O in Bild 9) und nicht die Blöcke des Testkanals.

Für Kategorie 2 muss Folgendes angewendet werden:

— Anforderungsrate ≤ 0,01 Testrate (siehe Tabelle K.1, ANMERKUNG 1); oder der Test erfolgt unmittelbar bei Anforderung der Sicherheitsfunktion und die Gesamtzeit zum Erkennen des Fehlers und zur Überführung der Maschine in einen nicht gefahrbringenden Zustand (in der Regel wird die Maschine angehalten) ist kürzer als die Zeit bis zum Erreichen der Gefährdung (siehe auch ISO 13855:2010);

— die $MTTF_D$ des Testkanals (TE und OTE in Bild 9) ist größer als die Hälfte der $MTTF_D$ des Funktionskanals.

Der DC aller Teile des Funktionskanals (I, L, O) muss mindestens niedrig sein. Die $MTTF_D$ des Funktionskanals muss, abhängig vom erforderlichen Performance Level (PL_r), niedrig bis hoch sein. Es müssen Maßnahmen gegen CCF des Funktionskanals und des Testkanals angewendet werden (siehe 6.1.6 und Anhang F).

Der maximale PL, der mit Kategorie 2 erreicht werden kann, ist PL d.

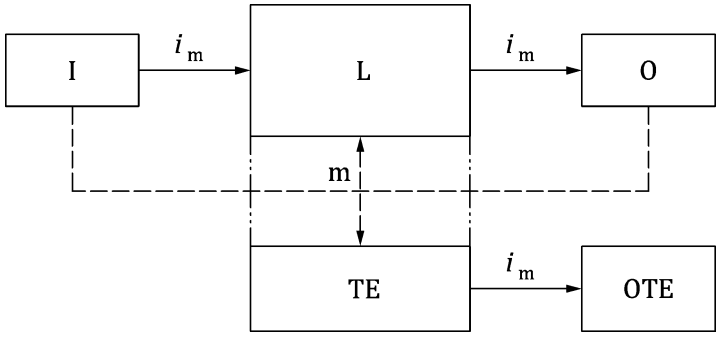
ANMERKUNG 1 Das Testen der Blöcke im Funktionskanal kann z. B. anhand einer Überwachung erfolgen.

ANMERKUNG 2 Das Systemverhalten in Kategorie 2 ist dadurch gekennzeichnet, dass

— zwischen den Tests das Auftreten eines Fehlers zum Verlust der Teilfunktion führen kann, und

— der Verlust der Teilfunktion durch die Tests erkannt wird.

ANMERKUNG 3 Das Prinzip, das die Gültigkeit einer Funktion in Kategorie 2 stützt, ist, dass die angewendeten technischen Maßnahmen, z. B. die Wahl der Testrate und die Zuverlässigkeit der Testeinrichtung, die Eintrittswahrscheinlichkeit eines gefährlichen Fehlers verringern können.



Legende

i_m	Verbindungsmittel	O	Ausgabegerät, z. B. Hauptschütz
I	Eingabegerät, z. B. Sensor	TE	Testeinrichtung
L	Logik	OTE	Ausgang der TE
m	Überwachen/Testen		

Die gestrichelten Linien zeigen die vernünftigerweise durchführbare Fehlererkennung.

Bild 9 — Vorgesehene Architektur für Kategorie 2

6.1.3.2.5 Kategorie 3

Für Kategorie 3 müssen die gleichen Anforderungen erfüllt sein wie für Kategorie B nach 6.1.3.2.2. Die bewährten Sicherheitsprinzipien nach 3.1.49 und ISO 13849-2:2012 müssen ebenfalls befolgt werden. Zusätzlich gilt Folgendes.

Der maximale PL, der mit Kategorie 3 erreicht werden kann, ist PL e.

Teilsysteme der Kategorie 3 müssen so entworfen werden, dass ein einzelner Fehler nicht zum Verlust der Teilfunktion führt. Wann immer vernünftigerweise durchführbar, muss ein einzelner Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt werden.

Der DC des gesamten Teilsystems muss mindestens niedrig sein. Die $MTTF_D$ jedes redundanten Kanals muss, abhängig vom PL_r, niedrig bis hoch sein. Es müssen Maßnahmen gegen CCF angewendet werden (siehe Anhang F).

ANMERKUNG 1 Die Anforderung zur Erkennung einzelner Fehler bedeutet nicht, dass auch alle Fehler erkannt werden. Folglich kann die Anhäufung unentdeckter Fehler zu einem unbeabsichtigten Ausgangssignal und zu einer Gefährdungssituation an der Maschine führen. Typische Beispiele für durchführbare Maßnahmen zur Fehlererkennung sind die Verwendung der Rückmeldungen von zwangsgeführten Relaiskontakten und die Überwachung von redundanten elektrischen Ausgängen (siehe Anhang E).

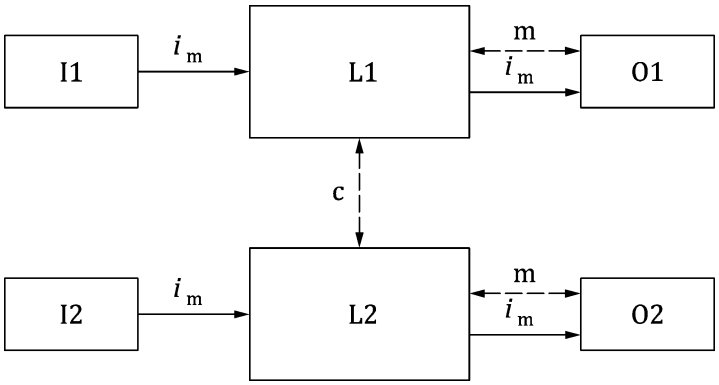
ANMERKUNG 2 Falls aufgrund der Technologie und Anwendung notwendig, kann das Normungsgremium, das Typ-C-Normen erarbeitet, weitere Einzelheiten zur Fehlererkennung nennen.

ANMERKUNG 3 Das Teilsystemverhalten in Kategorie 3 ist dadurch gekennzeichnet, dass

— bei Auftreten eines einzelnen Fehlers die Teilfunktion weiterhin ausgeführt wird,

— einige, aber nicht alle Fehler erkannt werden, und

— durch die Anhäufung unerkannter Fehler die Teilfunktion verloren gehen kann.



Legende

i_m	Verbindungsmittel	L1, L2	Logik
c	Kreuzvergleich	m	Überwachung
I1, I2	Eingabegerät, z. B. Sensor	O1, O2	Ausgabegerät, z. B. Hauptschütz oder Antriebssystem

Die gestrichelten Linien zeigen die vernünftigerweise durchführbare Fehlererkennung.

Bild 10 — Vorgesehene Architektur für Kategorie 3

6.1.3.2.6 Kategorie 4

Für Kategorie 4 müssen die gleichen Anforderungen erfüllt sein wie für Kategorie B nach 6.1.3.2.2. Die bewährten Sicherheitsprinzipien nach 3.1.49 und ISO 13849-2:2012 müssen ebenfalls befolgt werden. Zusätzlich gilt Folgendes.

Der maximale PL, der mit Kategorie 4 erreicht werden kann, ist PL e. Ein Teilsystem der Kategorie 4 muss so gestaltet werden, dass

— ein einzelner Fehler nicht zum Verlust der Sicherheitsfunktion führt, und

— der einzelne Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktionen erkannt wird, z. B. unmittelbar beim Einschalten oder am Ende des Betriebszyklus der Maschine, aber wenn diese Erkennung nicht möglich ist, darf eine Anhäufung von unerkannten Fehlern nicht zum Verlust der Sicherheitsfunktion führen.

ANMERKUNG 1 Basierend auf einem Analysenverfahren wie z. B. FMEA brauchen unerkannte Ausfälle mit einer sehr geringen Wahrscheinlichkeit nicht bei der Fehleranhäufung berücksichtigt zu werden, wenn dies dokumentiert und verifiziert wird.

Der durchschnittliche Diagnosedeckungsgrad (DC_{avg}) des gesamten Teilsystems muss hoch sein. Die $MTTF_D$ jedes redundanten Kanals muss hoch sein. Es müssen Maßnahmen gegen CCF angewendet werden (siehe Anhang F).

ANMERKUNG 2 Das Systemverhalten in Kategorie 4 ist dadurch gekennzeichnet, dass

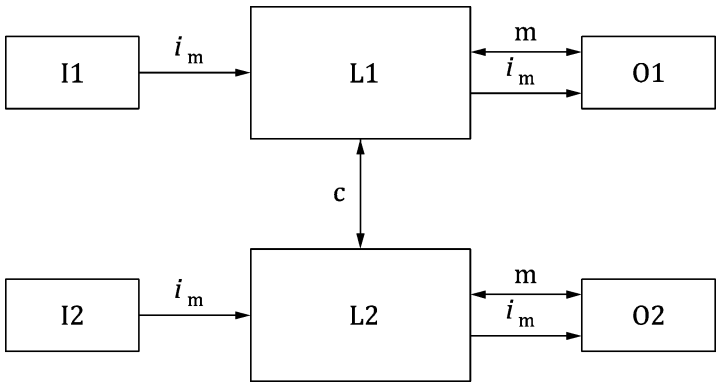
— bei Auftreten eines einzelnen Fehlers die Sicherheitsfunktion weiterhin ausgeführt wird,

— Fehler rechtzeitig erkannt werden, um den Verlust der Sicherheitsfunktion zu verhindern, und

— eine Anhäufung von unerkannten Fehlern in Betracht gezogen wird.

ANMERKUNG 3 Der Unterschied zwischen Kategorie 3 und Kategorie 4 ist ein höherer DC_{avg} in Kategorie 4 und eine erforderliche $MTTF_D$ jedes Kanals von nur „hoch“.

In der Praxis kann die Betrachtung einer Fehlerkombination aus zwei Fehlern ausreichend sein.



Legende

i_m	Verbindungsmittel	L1, L2	Logik
c	Kreuzvergleich	m	Überwachung
I1, I2	Eingabegerät, z. B. Sensor	O1, O2	Ausgabegerät, z. B. Hauptschütz oder Antriebssystem

Die durchgezogenen Linien für die Überwachung (m) stellen einen höheren DC als bei der vorgesehenen Architektur der Kategorie 3 dar.

Bild 11 — Vorgesehene Architektur für Kategorie 4

6.1.4 Mittlere Dauer bis zum gefahrbringenden Ausfall ($MTTF_D$)

Die mittlere Dauer bis zum gefahrbringenden Ausfall ($MTTF_D$) ist eine Größe mit der Dimension der Zeit, mit der die grundlegende Zuverlässigkeit der verwendeten Bauteile charakterisiert wird. Bei konstanter gefahrbringender Ausfallrate ist die $MTTF_D$ der Kehrwert der gefahrbringenden Ausfallrate (z. B. bei Ausfällen in 10^9 Stunden, umgerechnet in Jahre zwischen den Ausfällen).

Für die Abschätzung der $MTTF_D$ eines Bauteils ist die Prioritätenfolge wie folgt:

a) Verwendung von Herstellerdaten;

ANMERKUNG 1 Wenn $MTTF_D$-Daten von Bauteilen (z. B. elektromechanischen Bauteilen) vom Hersteller bereitgestellt werden, wird die vom Hersteller angegebene Anzahl der Bedienungen so berücksichtigt, dass die Anzahl der Bedienungen in der tatsächlichen Anwendung nicht größer ist als die vom Hersteller angegebene Anzahl der Bedienungen.

b) Anwendung der Verfahren von Anhang C;

c) Feld-Daten über Ausfallraten bei identischen Bauteilanwendungen in vergleichbaren Umgebungen, die über einen aussagekräftigen Zeitraum gesammelt wurden und deren Erfassung und Auswertung ein vernünftiges Vertrauensniveau der Werte ergeben;

ANMERKUNG 2 Weitere Informationen über Feld-Daten sind in IEC 61508-7:2010, B.5.4, ausführlicher beschrieben.

d) 10 Jahre auswählen.

Anhang C enthält einen praktischen Leitfaden darüber, wie die $MTTF_D$-Werte für einzelne Bauteile berechnet oder bewertet werden. Anhang D beschreibt, wie die $MTTF_D$ jedes Kanals daraus abgeleitet wird, einschließlich des Parts-Count-Verfahrens und der Symmetrisierung.

Für jedes Teilsystem nach Tabelle 5 ist der maximale Wert der $MTTF_D$ für jeden Kanal auf 100 Jahre begrenzt. Für Teilsysteme der Kategorie 4 ist der maximale Wert der $MTTF_D$ für jeden Kanal auf 2 500 Jahre begrenzt.

ANMERKUNG 3 Dieser höhere Wert ist dadurch begründet, dass sich in Kategorie 4 die anderen quantifizierbaren Aspekte, die Struktur und der DC, auf ihrem Höchststand befinden, und dies erlaubt, in Kategorie 4 mehr als 3 Teilsysteme seriell zu kombinieren, um den PL e nach 6.2 zu erreichen.

Der Wert der $MTTF_D$ jedes Kanals wird in drei Stufen angegeben (siehe Tabelle 6) und muss für jeden Kanal individuell berücksichtigt werden (z. B. einzelner Kanal, jeder Kanal eines redundanten Systems).

Tabelle 6 — Mittlere Dauer bis zum gefahrbringenden Ausfall ($MTTF_D$) jedes Kanals

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre $\leq MTTF_D <$ 10 Jahre
mittel	10 Jahre $\leq MTTF_D <$ 30 Jahre
hoch	30 Jahre $\leq MTTF_D \leq$ 100 Jahre[a]

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
ANMERKUNG 1 Die Wahl der $MTTF_D$-Bereiche jedes Kanals basiert auf Ausfallraten, die nach dem Stand der Technik in der Praxis festgestellt wurden und eine Art logarithmische Skala bilden, die sich der logarithmischen Skala des PL anpasst. Es wird davon ausgegangen, dass für ein reales Teilsystem kein $MTTF_D$-Wert eines Kanals kleiner als drei Jahre festgestellt werden kann, denn das würde bedeuten, dass nach einem Jahr etwa 30 % aller Systeme auf dem Markt defekt sind und ersetzt werden müssen. Ein $MTTF_D$-Wert eines Kanals größer als 100 Jahre wird nicht akzeptiert, denn Teilsysteme für hohe Risiken sollten nicht von der Zuverlässigkeit von Bauteilen alleine abhängig sein. Um ein Teilsystem gegen systematische und zufällige Ausfälle zu stärken, sind zusätzliche Mittel wie Redundanzen und Tests notwendig. Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf drei beschränkt. Die Beschränkung der $MTTF_D$ jedes Kanals auf ein Maximum von 100 Jahren bezieht sich auf den einzelnen Kanal des Teilsystems, der die Sicherheitsfunktion ausführt. Höhere $MTTF_D$-Werte können für einzelne Bauteile verwendet werden (siehe Tabelle D.1). ANMERKUNG 2 Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.	
[a] Für Kategorie 4 ist die $MTTF_D$ auf 2 500 Jahre begrenzt.	

6.1.5 Diagnosedeckungsgrad (DC)

Der Diagnosedeckungsgrad (DC) wird als das Verhältnis zwischen der Rate von erkannten gefahrbringenden Ausfällen und der Rate aller gefahrbringenden Ausfälle bestimmt. Der DC muss in den Kategorien 2, 3 und 4 berücksichtigt werden.

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{Dtotal}} \quad (1)$$

Dabei ist

$\sum \lambda_{DD}$ die Summe aller Ausfallraten erkannter gefahrbringender Ausfälle;

$\sum \lambda_{Dtotal}$ die Summe aller Ausfallraten aller gefahrbringenden Ausfälle.

Der DC muss entweder auf der Ausfalleffektanalyse (FMEA, siehe IEC 60812:2018) oder auf einer vereinfachten Abschätzung des DC nach E.1 und Tabelle E.1 beruhen. E.2 beschreibt, wie der durchschnittliche Diagnosedeckungsgrad (DC_{avg}) abgeschätzt werden kann.

ANMERKUNG 1 Zur Abschätzung des DC kann in den meisten Fällen die FMEA (siehe IEC 60812 und EN 50495:2010, Anhang B) oder ein ähnliches Verfahren angewendet werden, um entweder alle maßgebenden Fehler oder Ausfallarten oder beides zu berücksichtigen. Siehe auch ISO 13849-2:2012, E.5.3.

ANMERKUNG 2 Oftmals übernehmen Logikeinheiten die Diagnosefunktionen der Eingabe- und Ausgabegeräte.

ANMERKUNG 3 Die verwendete Technologie hat Einfluss auf die Möglichkeiten zur Realisierung der Fehlererkennung.

Der Wert für den DC wird in vier Stufen angegeben, wie in Tabelle 7 angegeben.

Tabelle 7 — Diagnosedeckungsgrad (DC)

DC	
Bezeichnung	**Bereich**
keiner	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	99 % ≤ DC

ANMERKUNG 1 Für Teilsysteme, die aus mehreren Teilen bestehen, wird in Bild 12, Abschnitt 7 und E.2 ein Durchschnittswert DC_{avg} für den DC verwendet.

ANMERKUNG 2 Die Wahl der DC-Bereiche basiert auf den Schlüsselwerten 60 %, 90 % und 99 %, die ebenfalls in anderen Normen, die sich mit dem DC von Tests beschäftigen, aufgeführt sind. Untersuchungen zeigen, dass (1 − DC) eher als der DC selbst eine typische Maßeinheit für die Effektivität eines Tests ist. (1 − DC) für die Schlüsselwerte 60 %, 90 % und 99 % bildet eine Art logarithmische Skala, die sich der logarithmischen Skala des PL anpasst. Ein DC-Wert kleiner als 60 % hat nur geringen Einfluss auf die Zuverlässigkeit eines getesteten Systems und wird deshalb mit „keiner“ bezeichnet. Für komplexe Systeme ist ein DC-Wert größer als 99 % nur sehr schwer zu erreichen. Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

6.1.6 Ausfälle infolge gemeinsamer Ursache (CCF)

Die Wahrscheinlichkeit, dass zwei oder mehr getrennte Fehler eine gemeinsame Ursache haben, muss für Teilsysteme der Kategorien 2, 3 und 4 berücksichtigt werden. In Kategorie 2 bezieht sich CCF auf Ausfälle infolge gemeinsamer Ursache im Funktionskanal und im Testkanal. In Kategorie 3 und Kategorie 4 bezieht sich CCF auf Ausfälle infolge gemeinsamer Ursache in beiden Funktionskanälen. Es müssen ausreichende Maßnahmen gegen CCF umgesetzt werden (für einen Leitfaden siehe Anhang F).

6.1.7 Systematische Ausfälle

Systematische Ausfälle treten aus den unterschiedlichsten Gründen auf; dazu zählen z. B.:

— fehlerhafte Spezifikation des Entwurfs;

— Produktionsausfälle;

— Auswirkungen von Umweltbelastungen (z. B. Temperatur, Schwingung und EMI);

— Betriebsausfälle;

— menschliche Fehler bei der SRS, dem Entwurf von Hardware und Software.

Um eine ausreichende systematische Integrität zu schaffen, muss der Ansatz für den Entwurf und die Umsetzung von Sicherheitsfunktionen systematisch sein.

Aktivitäten, die für das Erreichen der erforderlichen funktionalen Sicherheit des SRP/CS notwendig sind, müssen in einem Plan der funktionalen Sicherheit festgelegt sein. Der Plan der funktionalen Sicherheit soll Maßnahmen zur Vermeidung fehlerhafter Spezifikationen, Umsetzung oder Modifikationen enthalten.

Im Entwurfsprozess sind insbesondere die Beherrschung und Vermeidung von systematischen Ausfällen zu implementieren (siehe Abschnitt 10 und Anhang G.)

6.1.8 Vereinfachtes Verfahren für die Abschätzung des Performance Levels für Teilsysteme

Dieser Unterabschnitt beschreibt ein vereinfachtes Verfahren, um den PL eines Teilsystems auf der Basis vorgesehener Architekturen abzuschätzen. Andere Architekturen dürfen auf diesen vorgesehenen Architekturen abgebildet werden, um eine Abschätzung des PL zu ermöglichen (siehe 6.1.1).

Die vorgesehenen Architekturen werden als Blockdiagramme dargestellt und sind in 6.1.3.2 für jede Kategorie aufgeführt. Informationen über das Blockverfahren und die sicherheitsbezogenen Blockdiagramme sind in 6.1.3.2 und Anhang B gegeben. Siehe auch IEC 61078:2016.

Eine vorgesehene Architektur ist stets einem Teilsystem zugeordnet. Falls das SRP/CS aus einem einzigen Teilsystem besteht, ist die vorgesehene Architektur für das gesamte SRP/CS dieselbe. Falls das SRP/CS aus mehreren Teilsystemen besteht, muss jedem Teilsystem eine vorgesehene Architektur zugeordnet werden, wodurch ein einziges SRP/CS mehrere Architekturen enthalten kann.

Der vereinfachte Ansatz basiert auf Folgendem:

a) der Gebrauchsdauer (T_M), 20 Jahre (siehe 3.1.36);

b) den konstanten Ausfallraten innerhalb der Gebrauchsdauer;

c) ausreichenden Maßnahmen, um CCF zu verhindern (β-Faktor von 2 %). Für Leitlinien siehe Anhang F oder IEC 61508-6:2010, Anhang D.

ANMERKUNG Die Gebrauchsdauer (T_M) wird mit 20 Jahren angenommen, in denen die Zuverlässigkeit der Bauteile durch konstante Ausfallraten beschrieben oder angenähert werden kann. Dies erfolgt in der Regel in elektronischen Teilsystemen. Das SRP/CS wird ausgetauscht, wenn die Gebrauchsdauer verstrichen ist, oder es werden gleichwertige Maßnahmen umgesetzt, um sicherzustellen, dass der geschätzte PL noch gültig ist.

Um eine Gebrauchsdauer von 20 Jahren zu beanspruchen, müssen die Anforderungen von 6.1.3.2.2 für Kategorie B eingehalten werden. Bei der Verwendung von Bauteilen mit stärkerem Verschleiß oder aus anderen technischen Gründen, die dokumentiert werden sollten, darf die tatsächliche Gebrauchsdauer weniger als 20 Jahre betragen. Siehe auch C.4.

Das Verfahren sieht die Kategorien als Architekturen mit definiertem DC_{avg}. Der PL jedes Teilsystems hängt von der Architektur, von der $MTTF_D$ jedes Kanals und vom DC_{avg} ab.

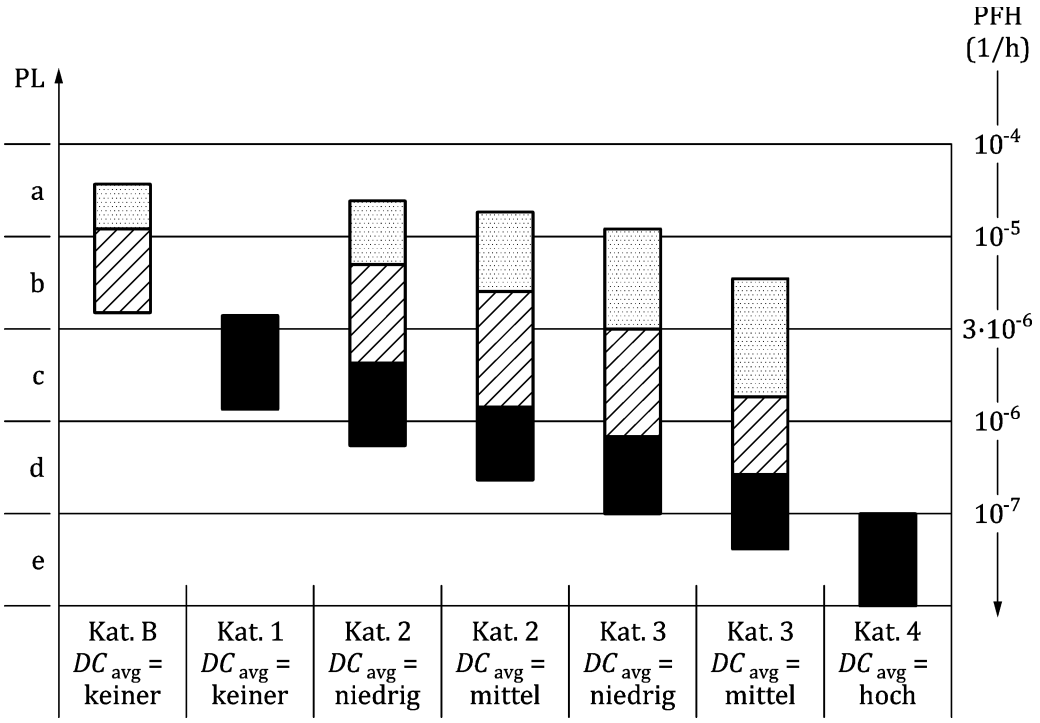
Enthalten die Teilsysteme Software, gelten die Anforderungen von Abschnitt 7. Die Kombination mehrerer Teilsysteme wird in 6.2 betrachtet.

Bild 12 zeigt, mit welcher Kombination aus Kategorie, $MTTF_D$ für jeden Kanal und DC_{avg} der erforderliche PL erreicht werden kann. Bild 12 zeigt die unterschiedlichen Möglichkeiten der Kombinationen von Kategorien und dem DC_{avg} (Horizontalachse) und der $MTTF_D$ jedes Kanals (Säulen) zur Abschätzung des PL. Die Säulen im Diagramm zeigen die drei $MTTF_D$-Bereiche jedes Kanals (niedrig, mittel und hoch), die gewählt werden können, um den erforderlichen PL zu erreichen.

Bevor dieser vereinfachte Ansatz von Bild 12 angewendet wird (der die Ergebnisse verschiedener Markov-Modelle auf der Basis vorgesehener Architekturen aus 6.1.3 zeigt), muss die Kategorie des Teilsystems (siehe 6.1.3.2) ebenso wie der DC_{avg} (siehe 6.1.5) und die $MTTF_D$ jedes Kanals (siehe 6.1.4) bestimmt worden sein (siehe Anhang C bis Anhang E). In den Kategorien 2, 3 und 4 müssen ausreichende Maßnahmen gegen CCF erfüllt werden (für einen Leitfaden siehe 6.1.6 und Anhang F). Unter Berücksichtigung dieser Parameter liefert das Bild 12 ein graphisches Verfahren zur Bestimmung des PL, der durch das Teilsystem erreicht wird. Die Kombination von Kategorie (einschließlich CCF) und DC_{avg} bestimmt, welche Säule in Bild 12 zu wählen ist. Entsprechend der $MTTF_D$ jedes Kanals muss einer der drei unterschiedlich schraffierten Bereiche der zutreffenden Säule gewählt werden.

Die vertikalen Bänder in Bild 12 zeigen den Leistungsbereich, der für jede Kombination von $MTTF_D$, Kategorie und DC_{avg} erwartet werden kann. Das Feststellen der geeigneten Bereiche für jede dieser Variablen in den Bändern von Bild 12 und das Ablesen an der vertikalen Achse ergibt den PL, der mithilfe dieser Kombination erreicht werden kann. Für eine genauere, numerische Auswahl des PL auf der Basis des genauen Werts der $MTTF_D$ jedes Kanals siehe Anhang K.

Ein ausführliches Beispiel für dieses vereinfachte Verfahren zur Einschätzung des Performance Levels für Teilsysteme ist in Anhang I angegeben.



Legende
PFH mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde
PL Performance Level
niedrige $MTTF_D$ jedes Kanals
mittlere $MTTF_D$ jedes Kanals
hohe $MTTF_D$ jedes Kanals

Bild 12 — Zusammenhang zwischen Kategorien, DC_{avg}, $MTTF_D$ jedes Kanals und dem PL

6.1.9 Alternatives Verfahren für die Bestimmung des Performance Levels und der PFH ohne $MTTF_D$

6.1.9.1 Allgemeines

Das alternative Verfahren für die Bestimmung des PL ohne die $MTTF_D$ beschränkt sich auf Teilsysteme, die mechanische, hydraulische, pneumatische, elektrohydraulische oder elektropneumatische Bauteile enthalten und für die keine Zuverlässigkeitsdaten verfügbar sind, und bei denen die in C.2 angegebenen Verfahren guter ingenieurmäßiger Praxis nicht angewendet werden können. In diesem Fall darf der Maschinenhersteller alternative Verfahren anwenden, die in 6.1.9.2 bis 6.1.9.4 beschrieben sind, um den PL ohne jegliche $MTTF_D$-Berechnung zu bewerten.

Die Kombination mehrerer Teilsysteme wird in 6.2 betrachtet.

6.1.9.2 Voraussetzungen

Wenn für mechanische, hydraulische oder pneumatische Bauteile (oder für Bauteile, die gemischte Technologien enthalten) keine anwendungsspezifischen Zuverlässigkeitsdaten oder Zuverlässigkeitsdaten des Herstellers vorhanden sind und die Verfahren guter ingenieurmäßiger Praxis von C.2 nicht angewendet werden können, darf der Hersteller der Maschine die quantifizierbaren Aspekte des PL ohne eine $MTTF_D$-Berechnung abschätzen. Wenn keine $MTTF_D$-Daten verfügbar sind, kann der sicherheitsbezogene Performance Level (PL) durch die Architektur, den DC und die Maßnahmen gegen CCF umgesetzt werden.

Als Worst-Case-Annahme ist der T_{10D}-Wert auf 10 Jahre begrenzt. Für bewährte Bauteile darf eine Annahme für T_{10D} von 20 Jahren gemacht werden. Bei diesem Verfahren wird die Berechnung von DC_{avg} auf den arithmetischen Mittelwert aus allen DC-Einzelwerten des Bauteils im Teilsystem reduziert.

Die Gebrauchsdauer (T_M) wird mit 20 Jahren angenommen. Für Kategorie 2 ist eine ausreichende Testrate erforderlich (siehe 6.1.3.2.4). Die Anforderungen, z. B. bezüglich DC_{avg} und CCF sowie systematischer Aspekte, müssen für jede Kategorie (siehe 6.1.3) erfüllt werden.

6.1.9.3 Eingänge oder Ausgangssubsystem

Tabelle 8 zeigt den Zusammenhang zwischen erreichbarem PL (wie in Bild 12) und den Kategorien. PL a und PL b können mit Kat. B erreicht werden, wenn die grundlegenden Sicherheitsprinzipien befolgt werden. PL c kann mit Kat. 1 oder Kat. 2 erreicht werden, wenn bewährte Bauteile, grundlegende und bewährte Sicherheitsprinzipien angewendet werden.

PL d kann mit Kat. 3 bzw. PL e kann mit Kat. 4 erreicht werden, wenn bewährte Bauteile, grundlegende und bewährte Sicherheitsprinzipien angewendet werden.

Tabelle 8 — Abschätzung des Performance Levels und der PFH auf Grundlage der Kategorie- und Bauteilauswahl

Kategorie[a]	Zusätzliche Anforderungen		Abgeschätzte PFH (1/h)	Erreichbarer PL[b]
B		→	$5{,}0 \times 10^{-6}$	b
1		→	$1{,}7 \times 10^{-6}$	c
2	Es werden ausschließlich bewährte Bauteile verwendet	→	$1{,}7 \times 10^{-6}$	c
3	Es werden ausschließlich bewährte Bauteile verwendet	→	$2{,}9 \times 10^{-7}$	d
4	Es werden ausschließlich bewährte Bauteile verwendet	→	$4{,}7 \times 10^{-8}$	e

[a] Alle Anforderungen von 6.1.3.2.2 bis 6.1.3.2.6 für die jeweilige Kategorie müssen erfüllt sein, außer die $MTTF_D$.

[b] Der hier genannte erreichbare PL deckt nur die quantifizierbaren Aspekte ab. Zusätzliche Anforderungen für nicht quantifizierbare Aspekte wie systematischer Ausfall und Software (siehe 6.1.1) müssen erfüllt sein.

6.1.9.4 Logik-Teilsystem

Wenn keine $MTTF_D$-Daten verfügbar sind, kann ein konservativer Ansatz unter Anwendung einer geschätzten $MTTF_D$ angenommen werden:

— für die Kategorien B, 2 und 3 beträgt die $MTTF_D$ für jeden Kanal 10 Jahre;

— für Kategorie 1 kann eine $MTTF_D$ des Kanals von 30 Jahren angenommen werden, da bewährte Bauteile anzuwenden sind (siehe 6.1.3.2.3).

Der maximale erreichbare PL ist PL c (siehe Anhang K).

Für Kategorie 2 und Kategorie 3 müssen Ausfälle infolge gemeinsamer Ursache und der DC betrachtet werden. Der DC_{avg} muss mindestens 60 % für Kategorie 2 und Kategorie 3 betragen.

Kategorie 4 ist in diesem Verfahren ausgeschlossen.

Anhand der Kategorie, der $MTTF_D$ und des DC_{avg} können der PL und die PFH des Teilsystems mit Tabelle K.1 bestimmt werden.

6.1.10 Fehlerbetrachtung und Fehlerausschluss

6.1.10.1 Allgemeines

Bei der Gestaltung sicherer Teilsysteme müssen Fehler und deren Auswirkungen beurteilt werden. Jedes Element, dessen Fehler zu einem Ausfall der Sicherheitsfunktion in einem der Funktionskanäle eines Teilsystems führen kann, muss betrachtet werden. Der Konstrukteur muss eine Liste der Fehler erstellen, die in dem SRP/CS auftreten können. Diese Liste muss alle betrachteten Fehler enthalten sowie eine Erläuterung, wie diese Fehler beim Entwurf berücksichtigt wurden und, falls ein Fehlerausschluss geltend gemacht wird, die Gründe für diese Ausschlüsse. Für Teilsysteme, die vom Bauteilhersteller vorab validiert worden sind, besteht keine Notwendigkeit durch den Konstrukteur der Sicherheitsfunktionen interne Ausfälle des Bauteils/der Bauteile zu berücksichtigen, sondern nur Ausfälle der Schnittstellen.

ANMERKUNG Fehler in Elementen, die nicht unbedingt für die Ausführung der Sicherheitsfunktion notwendig sind, die sie aber unterstützen können (z. B. Filterelemente, Überspannungsschutz), leisten im Allgemeinen keinen Beitrag zur $MTTF_D$ jedes Kanals.

6.1.10.2 Fehlerbetrachtung

ISO 13849-2:2012 führt die wichtigen Fehler und Ausfälle für die verschiedenen Technologien auf. Die Fehlerlisten sind nicht vollständig und es müssen gegebenenfalls weitere Fehler berücksichtigt und aufgeführt werden. In solchen Fällen muss das Verfahren für die Bewertung ebenfalls verständlich ausgearbeitet werden. Für Bauteile, die nicht in ISO 13849-2:2012 aufgeführt sind, muss ein Verfahren durchgeführt werden, mit dem der Einfluss von entweder wahrscheinlichen Fehlern oder Ausfällen von Bauteilen oder beidem bewertet wird, z. B. FMEA (siehe IEC 60812), mit dem Ziel, Fehler zu erkennen, die für diese Bauteile zu betrachten sind.

Im Allgemeinen müssen folgende Fehlermerkmale in Betracht gezogen werden:

— wenn infolge eines Fehlers weitere Bauteile ausfallen, muss der erste Fehler zusammen mit allen Folgefehlern als ein Einzelfehler berücksichtigt werden;

— das gleichzeitige Auftreten von zwei oder mehr Fehlern mit unterschiedlichen Ursachen wird als höchst unwahrscheinlich angesehen und braucht deswegen nicht betrachtet zu werden.

Zwei oder mehr einzelne Fehler, die eine gemeinsame Ursache haben, müssen als ein CCF betrachtet werden (siehe Anhang F).

6.1.10.3 Fehlerausschluss

Es kann notwendig sein, Fehler auszuschließen, um die Teilsysteme zu bewerten. Der Fehlerausschluss ist ein Kompromiss zwischen den technischen Sicherheitsanforderungen und der theoretischen Möglichkeit des Auftretens eines Fehlers.

Der Fehlerausschluss kann basieren auf:

a) der technischen Unwahrscheinlichkeit des Auftretens einiger Fehler;

b) der allgemeinen anerkannten technischen Erfahrung, unabhängig von der betrachteten Anwendung; und

c) den technischen Anforderungen im Bezug zur Anwendung und der spezifischen Gefährdung.

Der Fehlerausschluss gilt nur für bestimmte Ausfälle eines Elements, und es obliegt dem Konstrukteur (Hersteller oder Integrator), den Ausschluss des jeweiligen Fehlers basierend auf den durch den Entwurf und die Verwendung festgesetzten Grenzen nachzuweisen. Solche Fehlerausschlüsse sind nur möglich, wenn auf der Grundlage bekannter physikalischer Gesetze begründet werden kann, dass deren Auftreten unwahrscheinlich ist. Jeder dieser Fehlerausschlüsse muss begründet und dokumentiert werden.

Der Ausschluss von bestimmten Fehlern für ein Element in einem Teilsystem schränkt die Notwendigkeit von Maßnahmen gegen systematische Ausfälle nicht ein.

Es ist möglich, dass einige Fehler vom Hersteller und einige vom Teilsystemintegrator ausgeschlossen werden.

Es muss eine spezifische Charakterisierung der Art des Fehlers, der ausgeschlossen wird, vorliegen. Es wäre nicht akzeptabel, einfach zu sagen, dass ein Bauteil nicht aufgrund von Verschleiß bricht, sich verzieht oder verschlechtert. Es ist notwendig anzugeben, unter welchem direkten Einfluss das Bauteil nicht aufgrund von Verschleiß bricht, sich verzieht oder verschlechtert. Beispielsweise weist das Bauteil keine Fehler auf, wenn es einer Kraft von X Newton aus Richtung Y ausgesetzt wird.

Der Fehlerausschluss muss unter allen erwarteten Umgebungsbedingungen, wie Temperatur, Druck, Vibration, Verschmutzung, korrosive Atmosphäre, begründet werden können.

Der PL e darf nicht allein auf Fehlerausschluss beruhen.

ANMERKUNG 1 Informationen zu Fehlerausschlüssen sind in ISO 13849-2:2012, Anhang A bis Anhang D, enthalten.

ANMERKUNG 2 Produktnormen können weitere Informationen enthalten.

6.1.11 Bewährtes Bauteil

Ein bewährtes Bauteil für sicherheitsbezogene Anwendungen ist ein Bauteil, das entweder

a) in der Vergangenheit mit dokumentierten erfolgreichen Ergebnissen in ähnlichen Anwendungen eingesetzt worden sein muss, oder

ANMERKUNG Siehe IEC 61508-2:2010, 7.4.10, unter „betriebsbewährt".

b) in ISO 13849-2:2012, Anhang A bis Anhang D aufgeführt sein muss, oder

c) nach Prinzipien hergestellt, verifiziert und validiert sein muss, die seine Eignung und Zuverlässigkeit für sicherheitsbezogene Anwendungen entsprechend den zutreffenden Produkt- und Anwendungsnormen belegen.

Die Entscheidung, ein bestimmtes Bauteil als „bewährt" zu akzeptieren, hängt von der Anwendung ab, wie beispielsweise von den Umgebungseinflüssen.

Komplexe Bauteile (z. B. SPS, Mikroprozessor und anwendungsspezifische integrierte Schaltung) dürfen nicht als gleichwertig zu „bewährt" betrachtet werden.

6.2 Kombination von Teilsystemen zum Erreichen eines gesamten Performance Levels für die Sicherheitsfunktion

6.2.1 Allgemeines

Ein SRP/CS darf mithilfe einer Kombination von Teilsystemen erstellt werden und ein Gesamt-PL darf mit den in diesem Unterabschnitt beschriebenen Verfahren erreicht werden. In diesem Fall ist die Validierung der Kombination von Teilsystemen zu einem SRP/CS erforderlich (siehe Bild 13). Diese Teilsysteme dürfen einer oder unterschiedlichen Kategorien zugewiesen sein.

Nach 6.1.3.2 beginnt die Kombination von Teilsystemen zu einem SRP/CS an den Punkten, an denen die sicherheitsbezogenen Signale erzeugt werden, und endet am Ausgang der Leistungssteuerungselemente. Die Kombination der Teilsysteme kann aus mehreren Teilen, die linear (Reihenschaltung) verbunden sind, bestehen. Um eine erneute komplexe Abschätzung des durch kombinierte Teilsysteme erreichten Performance Levels (PL) zu vermeiden, wenn die einzelnen PL bereits berechnet worden sind, werden für eine Kombination von Teilsystemen folgende Abschätzungen aufgeführt.

Wenn vorab nach IEC 62061:2021 oder nach der Normenreihe IEC 61508 (SIL) validierte Teilsysteme für Betriebsarten mit hoher Anforderungsrate oder Betriebsarten mit kontinuierlicher Anforderung, die Pfad 1_H nutzen (siehe IEC 61508-2:2010, 7.4.4.2), verwendet werden, kann der SIL nach 6.1.2 und 6.2.2 auf einen PL zugeordnet werden. Die nach der Normenreihe IEC 61508 oder nach IEC 62061:2021 berechneten PFH-Werte mit den vorstehenden Beschränkungen können als PFH-Werte nach diesem Dokument betrachtet werden.

Für ein Teilsystem, das nach IEC 62061:2021 oder der Normenreihe IEC 61508 validiert worden ist, kann die Kategorie nicht immer abgeleitet werden und ist nicht erforderlich.

6.2.2 Bekannte PFH-Werte

Werden Teilsysteme mit bekannten PFH-Werten miteinander kombiniert, können die PFH-Werte wie nachstehend beschrieben kombiniert werden, sofern *n* separate Teilsysteme SB_1 bis SB_n vorhanden sind. Diese Teilsysteme arbeiten in einer seriellen Kombination, die als Ganzes eine Sicherheitsfunktion ausführt. Für jedes Teilsystem SB_i wurde bereits ein PL_i bewertet. Diese Situation wird in Bild 13 dargestellt (siehe auch Bild 5 und Bild H.2).

Wenn die PFH-Werte aller Teilsysteme bekannt sind, dann ist die PFH des SRP/CS die Summe aller PFH-Werte der *n* einzelnen Teilsysteme. Der PL des SRP/CS wird beschränkt durch:

— den niedrigsten PL eines einzelnen kombinierten Teilsystems, das die Sicherheitsfunktion ausführt; und

— den PL, der der PFH des kombinierten SRP/CS nach Tabelle 2 entspricht.

ANMERKUNG Ein Beispiel dieses Verfahrens ist in Anhang H enthalten.

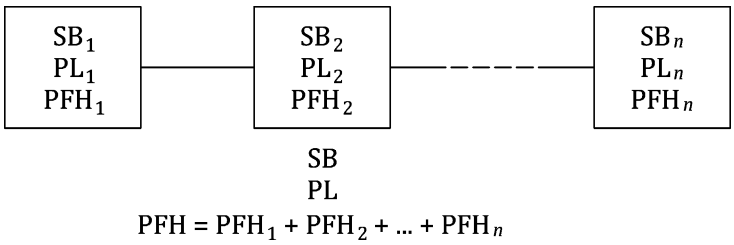


Bild 13 — Kombination von Teilsystemen zum Erreichen des Gesamt-PL

6.2.3 Unbekannte PFH-Werte

Wenn die PFH-Werte aller einzelnen SB_i nicht bekannt sind, dann darf alternativ zu 6.2.2 der PL des SRP/CS, das die Sicherheitsfunktion ausführt, nach 6.1 definiert oder mithilfe von Tabelle 9 wie folgt berechnet werden:

a) der niedrigste PL aller Teilsysteme wird bestimmt: dies ist $PL_{niedrig}$;

b) die Anzahl der Teilsysteme mit $PL_{niedrig}$ wird bestimmt: diese Anzahl ist $N_{niedrig}$;

c) der PL wird in Tabelle 9 nachgeschlagen.

Tabelle 9 — Bestimmung des PL für die Reihenschaltung von Teilsystemen

$PL_{niedrig}$	$N_{niedrig}$	⇒	PL des SRP/CS
a	> 3	⇒	keiner, nicht zulässig
	≤ 3	⇒	a
b	> 2	⇒	a
	≤ 2	⇒	b
c	> 2	⇒	b
	≤ 2	⇒	c
d	> 3	⇒	c
	≤ 3	⇒	d
e	> 3	⇒	d
	≤ 3	⇒	e
ANMERKUNG Diese Tabelle basiert auf den definierten PFH-Bereichen für jeden PL (siehe Tabelle 2), die eine Art logarithmische Skala bilden.			

6.3 Softwarebasierte manuelle Parametrierung

6.3.1 Allgemeines

Der Anwendungsbereich dieses Unterabschnitts ist ausschließlich auf manuelle, softwarebasierte Parametrierung beschränkt, die von einer befugten Person durchgeführt und kontrolliert wird. Siehe auch 5.2.2.6 sowie Tabelle M.2.

Einige sicherheitsbezogene Teilsysteme oder SRP/CS benötigen die Parametrierung für eine Sicherheitsfunktion oder eine Teilfunktion.

BEISPIEL Ein Umrichter mit integrierten Teilfunktionen kann über ein PC-gestütztes Konfigurationswerkzeug parametriert werden, um den Parameter für die obere Geschwindigkeitsgrenze einzustellen. Parameter wie Winkel und Abstand können anhand der Sicherheitsdokumentation des Herstellers und der Risikobeurteilung der Maschine konfiguriert werden, um den Abtastbereich eines Laserscanners einzustellen.

Ziel der Anforderungen an die softwarebasierte manuelle Parametrierung ist es, sicherzustellen, dass die sicherheitsbezogenen Parameter, die für eine Sicherheitsfunktion oder eine Teilfunktion festgelegt sind, ordnungsgemäß in die Hardware übermittelt werden, welche die Sicherheitsfunktion bzw. die Teilfunktion ausführt. Mithilfe verschiedener Verfahren können solche Parameter festgelegt werden, wie DIP-Schalterbasierte Parametrierung oder entsprechende Software für die Parametrierung (allgemein als Konfigurations- oder Parametrierungswerkzeug bezeichnet).

ANMERKUNG 1 Sicherheitsbezogene Parametrierung, die automatisch ohne Eingriff durch einen Menschen erfolgt, d. h. beispielsweise auf der Grundlage von Eingangssignalen, wird in diesem Unterabschnitt nicht betrachtet.

ANMERKUNG 2 Die direkte Steuerung einer Maschine durch einen Bediener, z. B. die Geschwindigkeitsregelung eines Gabelstaplers, wird nicht als manuelle Parametrierung nach diesem Unterabschnitt betrachtet.

Falls das Konfigurations- oder Parametrierungswerkzeug in Übereinstimmung mit diesem Dokument oder der Normenreihe IEC 61508 bereits entworfen ist, z. B. gemeinsam mit seinem dazugehörigen Teilsystem, dann wird davon ausgegangen, dass keine gefahrbringenden Ausfälle durch die in 6.3.2 angegebenen Einflüsse oder irgendeinen anderen vernünftigerweise vorhersehbaren Einfluss eintreten werden. Es gelten die Anforderungen von 6.3.5, wenn eine softwaregestützte manuelle Parametrierung mit dem bereits entworfenen Werkzeug durchgeführt wird.

Falls ein sicherheitsbezogenes Teilsystem oder SRP/CS nicht wie vorstehend beschrieben durch softwarebasierte manuelle Parametrierung parametriert werden kann, gilt 6.3 nicht.

6.3.2 Einflüsse auf sicherheitsbezogene Parameter

Sicherheitsbezogene Parameter müssen so ausgelegt sein, dass den auftretenden äußeren Einflüssen standgehalten wird. Während der softwarebasierten manuellen Parametrierung können die Parameter auf unterschiedliche Weise beeinflusst werden, wie beispielsweise durch:

a) Fehler bei der Eingabe von Daten durch die Person, die für die Parametrierung verantwortlich ist;

b) Softwarefehler des Parametrierungswerkzeugs;

c) Fehler in der sonstigen Software und/oder in sonstigen Diensten, die durch das Parametrierungswerkzeug bereitgestellt werden;

d) Hardwarefehler des Parametrierungswerkzeugs;

e) Fehler während der Übertragung von Parametern vom Parametrierungswerkzeug zum SRP/CS oder Teilsystem;

f) Fehler des SRP/CS oder eines Teilsystems bei der korrekten Speicherung der übertragenen Parameter;

g) systematische Störung während des Parametrierungsvorgangs, z. B. durch EMI oder Energieverlust;

h) Störung durch externe Einflüsse oder Faktoren, wie beispielsweise EMI oder (zufälliger) Energieverlust.

Ohne Maßnahmen zur Bekämpfung, Vermeidung oder Beherrschung potenzieller gefahrbringender Ausfälle, die durch die oben aufgeführten Einflüsse verursacht werden, kann ein solcher Einfluss zu Folgendem führen:

— die Parameter werden durch den Parametrierungsprozess vollständig oder teilweise nicht aktualisiert, ohne Rückmeldung an die für die Parametrierung verantwortliche Person;

— die Parameter sind vollständig oder teilweise nicht korrekt;

— die Parameter werden auf ein falsches Gerät angewendet, z. B. wenn die Übertragung von Parametern über ein drahtgebundenes oder drahtloses Netzwerk erfolgt.

6.3.3 Anforderungen an die softwarebasierte manuelle Parametrierung

Die softwarebasierte manuelle Parametrierung muss ein geeignetes Werkzeug nutzen, das vom Hersteller oder vom Lieferanten des SRP/CS oder des/der zugehörigen Teilsystems/Teilsysteme bereitgestellt wird. Das SRP/CS bzw. das/die zugehörige(n) Teilsystem(e) und das Parametrierungswerkzeug müssen in der Lage sein, unbefugte Änderungen zu verhindern, indem sie beispielsweise ein hierfür vorgesehenes Passwort benötigen.

Parametrierung bei laufender Maschine darf nur dann möglich sein, wenn dies nicht zu einem unsicheren Zustand führt.

Es besteht die Möglichkeit, die Anforderungen durch Anwendung eines bereits entworfenen Teilsystems zu erfüllen.

Bei Verwendung eines bereits entworfenen SRP/CS oder Teilsystems, das für die softwarebasierte manuelle Parametrierung geeignet ist, ist es das Ziel, gefahrbringende Ausfälle durch die in 6.3.2 angegebenen Einflüsse oder andere vernünftigerweise vorhersehbare Einflüsse zu verhindern. Die Validierung des bereits entworfenen Teilsystems muss den Aspekt der Parametrierung enthalten.

Wenn ein SRP/CS oder Teilsystem, das für die softwarebasierte manuelle Parametrierung geeignet ist, nach diesem Dokument entworfen wurde, dürfen keine unerkannten gefahrbringenden Ausfälle durch die oben angegebenen Einflüsse oder andere vernünftigerweise vorhersehbaren Einflüsse eintreten. Die folgenden Anforderungen müssen außerdem erfüllt sein:

a) der Entwurf der softwarebasierten manuellen Parametrierung muss als sicherheitsbezogener Aspekt des SRP/CS-Entwurfs betrachtet werden, der in einer SRS beschrieben wird;

b) das SRP/CS oder das Teilsystem muss über Maßnahmen zur Plausibilitätsprüfung von Daten verfügen, z. B. Überprüfen von Datengrenzen, Datenformaten und/oder logischen Eingangswerten;

c) die Integrität aller für die Parametrierung verwendeten Daten muss aufrechterhalten bleiben. Dies muss durch Anwendung folgender Maßnahmen erreicht werden:

   1) Kontrolle des Bereichs der konfigurierten Werte durch eine Überprüfung der Gültigkeit (des Gültigkeitsbereichs);

   2) Beherrschung von Datenverfälschungen vor der Datenübertragung;

   3) Beherrschung der Auswirkungen von Fehlern beim Prozess der Parameterübertragung;

4) Beherrschung der Auswirkungen beim unvollständigen Übertragen von Parametern;

5) Beherrschung der Auswirkungen von Fehlern und Ausfällen der Parametrierungs-Hardware und -Software;

6) Beherrschung der Auswirkung der Unterbrechung der Energieversorgung;

d) das Parametrierungswerkzeug muss alle zutreffenden Anforderungen an ein SRP/CS nach diesem Dokument oder nach der Normenreihe IEC 61508 erfüllen;

e) alternativ zu d) muss ein spezielles Verfahren für die Einstellung der sicherheitsbezogenen Parameter verwendet werden. Dieses Verfahren muss die Bestätigung von Eingabeparametern für das SRP/CS umfassen, entweder durch:

— Rückübertragen von modifizierten Parametern zum Parametrierungswerkzeug; oder

— andere Mittel zur Bestätigung der Integrität der Parameter;

— sowie nachträgliche Bestätigung, z. B. durch eine ausreichend geschulte Person und eine automatische Überprüfung durch ein Parametrierungswerkzeug. Neue Werte von sicherheitsbezogenen Parametern dürfen nicht für den sicherheitsbezogenen Betrieb eingesetzt werden, bevor die Änderungen anerkannt und bestätigt worden sind.

ANMERKUNG Dies ist von besonderer Wichtigkeit, wenn ein Softwaretool zur Parametrierung ein Gerät nutzt, das nicht speziell für diesen Zweck vorgesehen ist (z. B. Personal Computer (PC) oder Ähnliches).

Die Softwaremodule, die für die Codierung/Decodierung innerhalb des Übertragungs-/Rückübertragungsprozesses verwendet werden, und die Softwaremodule, die für die Anzeige von sicherheitsbezogenen Parametern für den Anwender verwendet werden, müssen mindestens Diversität in ihren Funktionen nutzen, um systematische Ausfälle zu verhindern.

6.3.4 Verifizierung des Parametrierungswerkzeugs

Die folgenden Verifizierungsaktivitäten müssen durchgeführt werden, um die grundlegende Funktionalität des Parametrierungswerkzeugs zu verifizieren:

— Verifizierung der korrekten Einstellung für jeden sicherheitsbezogenen Parameter (Mindestwert, Höchstwert und repräsentativer Wert);

— Verifizierung, dass die sicherheitsbezogenen Parameter auf Plausibilität überprüft werden, z. B. durch Erkennen ungültiger Werte;

— Verifizierung, dass Maßnahmen zum Verhindern unbefugter Änderungen von sicherheitsbezogenen Parametern vorhanden sind.

ANMERKUNG Dies ist von besonderer Wichtigkeit, wenn die Parametrierung unter Verwendung eines Geräts ausgeführt wird, das nicht speziell für diesen Zweck vorgesehen ist (z. B. Personal Computer oder Ähnliches).

6.3.5 Dokumentation der softwarebasierten manuellen Parametrierung

Softwarebasierte manuelle Parametrierung muss mithilfe des dafür vorgesehenen Parametrierungswerkzeugs durchgeführt werden, das vom Hersteller oder Lieferanten des SRP/CS oder des/der zugehörigen Teilsystems/Teilsysteme bereitgestellt wird, und muss entsprechend den in der Benutzerinformation angegebenen Anforderungen dokumentiert werden. Diese Informationen können von verschiedenen Parteien eingeholt werden, siehe auch Abschnitt 13 (Benutzerinformation). Schutzmaßnahmen gegen unbefugten Zugriff müssen aktiviert und angewendet werden.

Die Erst-Parametrierung sowie anschließende Änderungen an der Parametrierung müssen dokumentiert werden. Die Dokumentation muss Folgendes umfassen:

a) das Datum der Erst-Parametrierung bzw. der Änderung der Parametrierung;

b) das Datum oder die Versionsnummer des Datensatzes;

c) den Namen der Person, die die Parametrierung durchführt;

d) eine Angabe der Quelle der verwendeten Daten (z. B. vordefinierte Parametersätze);

e) eindeutige Identifizierung der sicherheitsbezogenen Parameter;

f) Auswirkungen und Grenzen für Fälle, in denen eine kontinuierliche Parametrierung möglich oder erforderlich ist;

g) eindeutige Identifizierung des SRP/CS oder des zugehörigen Teilsystems, für das bestimmte Parametrierungseinstellungen gelten.

7 Software-Sicherheitsanforderungen

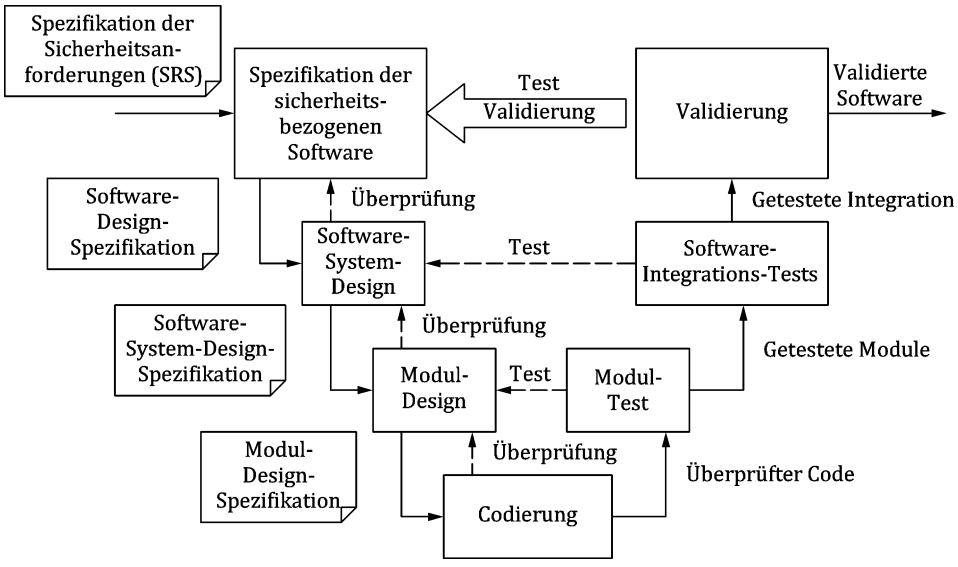
7.1 Allgemeines

Obwohl künstliche Intelligenz (KI) für SRP/CS eingesetzt werden kann, befasst sich dieser Abschnitt nicht mit zusätzlichen spezifischen Anforderungen, die für die KI-Technologie und deren Einsatz als Teil von SRP/CS erforderlich sind.

Aktivitäten in Zusammenhang mit der Entwicklung von sicherheitsbezogener Embedded-Software oder sicherheitsbezogener Anwendungssoftware müssen im Wesentlichen darauf abzielen, Fehler während des Software-Lebenszyklus zu vermeiden [siehe Bild 14 a)]. Das Hauptziel der folgenden Anforderungen ist es, eine lesbare, verständliche, testfähige und wartungsfreundliche Software zu erhalten.

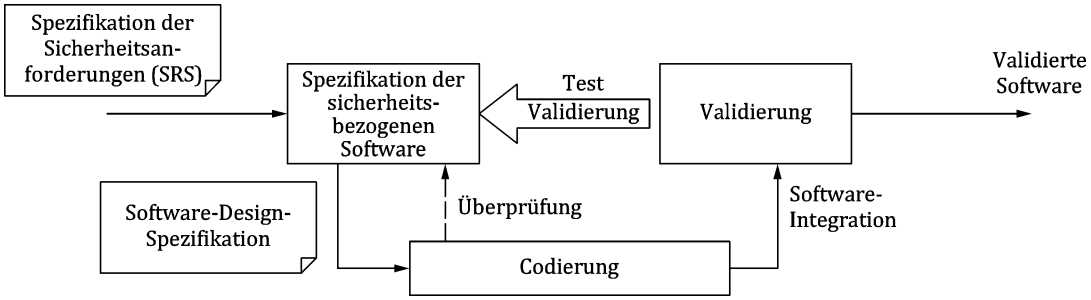
ANMERKUNG 1 Anhang J zeigt detailliertere Empfehlungen für Lebenszyklus-Aktivitäten.

ANMERKUNG 2 Anhang N gibt einen Überblick über die Maßnahmen, die für SRASW gelten, die unter Verwendung von LVL ausgeführt wird, und über die Maßnahmen, die für SRASW oder SRESW gelten, die unter Verwendung von FVL ausgeführt wird.



a) Vereinfachtes V-Modell des Software-Sicherheitslebenszyklus

Wenn zuvor beurteilte sicherheitsbezogene Hardware- und Softwaremodule in Kombination mit LVL verwendet werden, dann ist der in Bild 14 b) dargestellte vereinfachte Software-Lebenszyklus anwendbar.



b) Vereinfachtes V-Modell für Software, falls zuvor beurteilte sicherheitsbezogene Hardware- und Softwaremodule in Kombination mit LVL verwendet werden

Legende
⟶ Ergebnis
⇢ Verifizierung

ANMERKUNG Der vereinfachte Software-Lebenszyklus, in Bild 14 b) gezeigt, gilt normalerweise für die Verwendung der modulbasierten Programmierung mit LVL, bei der nur einfache Zusammenschaltungen konfiguriert werden müssen, wodurch die Eingangs- und Ausgangswerte auf einen vordefinierten Wertesatz beschränkt werden, einschließlich einer Kombination von Modulen.

Bild 14 — Vereinfachtes V-Modell

Wenn Sicherheitsfunktionen und nicht sicherheitsbezogene Funktionen in derselben Hardware-Umgebung vorhanden sind, muss nachgewiesen werden, dass die Sicherheitsfunktionen unter normalen oder Fehlerbedingungen nicht von den nicht sicherheitsbezogenen Funktionen beeinträchtigt werden, wozu zum Beispiel unter anderem die Blockierung oder Verzögerung einer Sicherheitsreaktion zählen kann, von der gefordert wird, dass sie jederzeit ausgeführt werden kann.

7.2 Programmiersprache mit eingeschränktem Sprachumfang (LVL) und Programmiersprache mit nicht eingeschränktem Sprachumfang (FVL)

7.2.1 Programmiersprache mit eingeschränktem Sprachumfang (LVL)

LVL ist eine Software-Programmiersprache, deren Notation textuell oder graphisch ist oder Eigenschaften von beidem enthält, für kommerzielle und industrielle programmierbare elektronische Steuerungen mit einer Reihe von Fähigkeiten, die auf ihre Anwendung beschränkt sind (siehe IEC 61508-4:2010, 3.2.14).

LVL sollte vom Softwareentwickler so entworfen werden, dass sie leicht verständlich ist, und sollte sich streng auf die durchzuführenden Anwendungen konzentrieren.

Im Folgenden sind Beispiele für LVLs aufgeführt:

a) Kontaktplan (siehe IEC 61131-3:2013, 8.2): eine graphische Sprache, die aus einer Serie von Eingangssymbolen (die ein Verhalten ähnlich dem eines Öffners oder Schließers darstellen) besteht, die durch Linien (die den Stromfluss andeuten) mit Ausgangssymbolen (die ein Verhalten ähnlich dem eines Relais darstellen) verbunden sind;

b) Funktionsbausteinsprache (siehe IEC 61131-3:2013, 8.3): erlaubt dem Anwender zusätzlich zu booleschen Operatoren die Verwendung komplizierterer Funktionen wie z. B. Datenübertragung, Blockübertragung Lesen/Schreiben, Schieberegister und sequentielle Anweisungen;

c) Ablaufsprache (siehe IEC 61131-3:2013, 6.7): eine graphische Darstellung eines sequentiellen Programms, die aus miteinander verbundenen Schritten, Aktionen und gezielten Verbindungen zu Transitionsbedingungen besteht;

d) Boolesche Algebra: eine maschinennahe Sprache basierend auf booleschen Operatoren wie z. B. UND, ODER und NICHT mit der Fähigkeit, einige mnemonische Anweisungen anzufügen.

7.2.2 Programmiersprache mit nicht eingeschränktem Sprachumfang (FVL)

Diese Art von Sprache wurde für Softwareentwickler entwickelt und bietet die Möglichkeiten, eine Vielzahl von Funktionen und Anwendungen zu implementieren. Diese Art von Sprache bietet alle möglichen Programmieroptionen und kann verwendet werden, um ein Anwendungsprogramm mit voller Flexibilität bei der Konstruktion der Logik zu erstellen.

ANMERKUNG Typische Beispiele für Systeme, die FVL verwenden, sind Computer für generelle Anwendungen.

Im Maschinenbereich wird FVL in Embedded-Software und gelegentlich in Anwendungssoftware eingesetzt.

BEISPIEL Ada, C, Pascal, Anweisungsliste, Assembler-Sprachen, C++, Java, MATLAB, Simulink, ST und SQL (ohne Anwendungsbeschränkung und mit einer Vielzahl von Anweisungen).

7.2.3 Entscheidung zwischen Programmiersprache mit eingeschränktem Sprachumfang (LVL) und Programmiersprache mit nicht eingeschränktem Sprachumfang (FVL)

In der Regel kann die Software mithilfe von FVL oder LVL programmiert werden. Der Konstrukteur des SRP/CS muss den Anweisungen von Bild 15 folgen, um zwischen den Programmiersprachen FVL und LVL zu entscheiden.

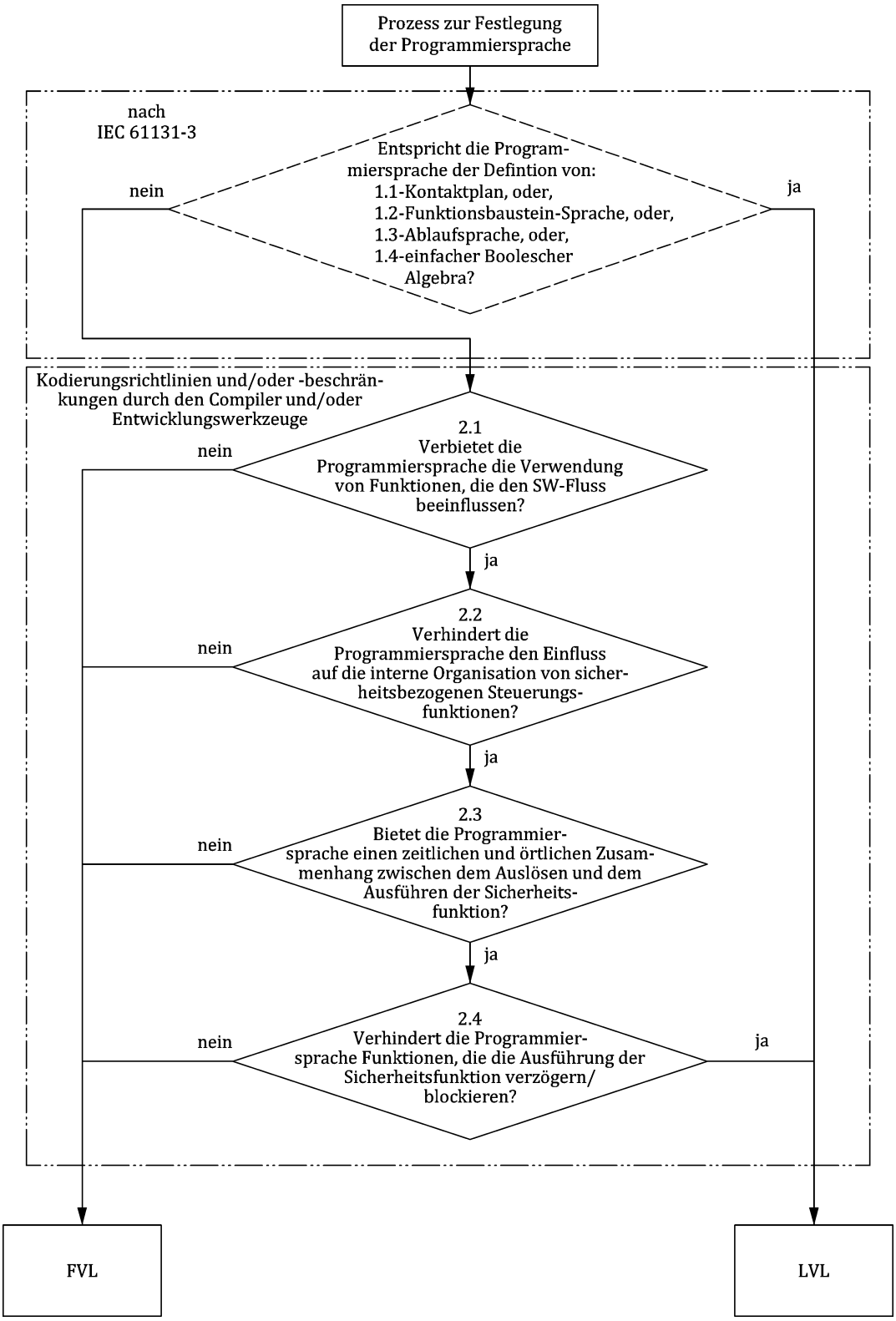


Bild 15 — Entscheidungshilfe bezüglich FVL bzw. LVL

BEISPIEL 1 Wenn Sprache C verwendet wird, besteht keine Übereinstimmung mit IEC 61131-3, und wird eine der Fragen 2.1 bis 2.4 in Bild 15 mit „nein“ beantwortet, dann ist das Ergebnis FVL.

BEISPIEL 2 Wenn eine Art strukturierter Text oder eine Teilmenge von Sprache C mit Beschränkungen entweder der Compiler- oder der Entwicklungstools oder von beidem und mit restriktiven Codierungsrichtlinien verwendet wird, die 7.4 a) und b) erfüllen, und wenn alle Fragen 2.1 bis 2.4 in Bild 15 mit „ja“ beantwortet werden können, ist das Ergebnis LVL.

BEISPIEL 3 Wenn Visual Basic verwendet wird, besteht keine Übereinstimmung mit IEC 61131-3, und werden die Fragen 2.1 bis 2.4 in Bild 15 mit „nein“ beantwortet, ist das Ergebnis FVL.

BEISPIEL 4 Wird der Software-Fluss von der Programmiersprache beeinflusst, z. B. durch Interrupts (Frage 2.1 in Bild 15), ist das Ergebnis FVL.

BEISPIEL 5 Wenn eine Funktionsbausteinsprache mit selbst deklarierten Funktionsbausteinen in strukturiertem Text nach IEC 61131-3 verwendet wird und die Einschränkungen von 7.4 a) und b) erfüllt sind, ist das Ergebnis LVL.

ANMERKUNG 1 Anhang N gibt einen Überblick über die Maßnahmen, die für SRASW und SRESW gelten, die entweder mithilfe von LVL oder FVL ausgeführt werden.

ANMERKUNG 2 Die technische Dokumentation, besonders das Sicherheitshandbuch von Produkten, kann sowohl für LVL als auch für FVL befolgt werden. Sowohl Beschränkungen durch interne Funktionen des Compilers als auch Beschränkungen durch eine Codierungsrichtlinie können angewendet werden.

7.3 Sicherheitsbezogene Embedded-Software (SRESW)

7.3.1 Entwurf der sicherheitsbezogenen Embedded-Software (SRESW)

Bei SRESW für Komponenten mit einem PL_r a bis d müssen die folgenden grundlegenden Maßnahmen angewendet werden:

a) Software-Sicherheitslebenszyklus mit Verifizierungs- und Validierungsaktivitäten, z. B. Prüfungen und Tests, siehe Bild 14 a);

b) Dokumentation der Spezifikation und des Designs, z. B. Software-Design-Spezifikation, Software-System-Design-Spezifikation (SSDS), Modul-Design-Spezifikation (MDS), Codelisten einschließlich Kommentaren;

c) modularer und strukturierter Entwurf und Codierung, z. B. Hierarchie und Einschränkung der Funktionalität, klare Programmstruktur, Definition von Schnittstellen, gut strukturierter Aufrufgraph, Vermeidung von Interrupts, Verwendung von Codierungsrichtlinien (siehe IEC 61508-7:2010, C.2.6.2);

d) Beherrschung systematischer Ausfälle, z. B. Programmablaufüberwachung, Beherrschung von Fehlern im Datenkommunikationsprozess (siehe G.2);

e) wenn softwarebasierte Diagnosemaßnahmen zur Beherrschung zufälliger Hardwareausfälle verwendet werden, wird die korrekte Umsetzung überprüft, z. B. korrekte Umsetzung von Diagnosemaßnahmen, RAM/ROM/CPU-Tests, Hardwaretests, Plausibilitätsprüfungen;

f) Funktionstests, z. B. durchgeführte Black-Box-Tests, z. B. durch Verifizierung von korrekten Ausgabedaten basierend auf den Eingabedaten (gültig, ungültig und Grenzwerte), Kompatibilität von Schnittstellen, Zeitvorgaben;

g) geeignete Aktivitäten im Lebenszyklus der Softwaresicherheit nach Änderungen, z. B. basierend auf einer Einfluss-Analyse.

Für SRESW in Komponenten mit einem PL_r c oder d müssen die folgenden zusätzlichen Maßnahmen angewendet werden:

h) Projektmanagement- und Qualitätsmanagement-Prozesse, vergleichbar mit z. B. der Normenreihe IEC 61508, z. B. Definition von Arbeitsabläufen, Verantwortlichkeiten;

i) Dokumentation aller maßgebenden Tätigkeiten während des Software-Sicherheitslebenszyklus, z. B. Dokumentation von Überprüfungen, Tests, Validierung und Verifizierung;

j) Konfigurationsmanagement zur Identifizierung aller Konfigurationselemente und Dokumente in Zusammenhang mit einer SRESW-Version, z. B. Versionskontrolle von Codelisten, Modulen, Entwurfsdokumenten, Testplänen, Freigabekontrolle, Archivierung, Systemkompatibilität der verschiedenen Versionen von Hardware, Software und Programmiertools;

k) strukturierte Spezifikation mit Sicherheitsanforderungen und strukturiertem Aufbau;

l) Verwendung geeigneter Programmiersprachen und rechnergestützter Tools mit Betriebsbewährung;

m) modulare und strukturierte Programmierung, Abgrenzung von der nicht sicherheitsbezogenen Software, beschränkte Modulgrößen mit vollständig definierten Schnittstellen, z. B. Verwendung von Entwurfs- und Codierungsrichtlinien;

n) Verifizierung der Codierung durch Walk-through/Überprüfen mit Kontrollflussanalyse, z. B. zur Überprüfung auf Fehler, Qualität der Kommentare, Einhaltung der Codierungsrichtlinien, Klarheit, Lesbarkeit, Vollständigkeit;

o) erweiterte Funktionstests, z. B. Grey-Box-Tests, Leistungstests oder Simulationen, z. B. durch Verwendung von nicht spezifizierten Eingabedaten, extremen Umgebungsbedingungen, Volllast, Tests basierend auf Kenntnissen der internen Codierung.

Für den Testkanal in Kategorie 2 werden die Anforderungen um einen Performance Level reduziert. Kommt in den Funktionskanälen der Kategorie 3 oder 4 Diversität zum Einsatz, werden die Anforderungen um einen Performance Level reduziert.

Die SRESW für Komponenten mit PL_r e muss mit den Anforderungen von IEC 61508-3:2010, Abschnitt 7, geeignet für SIL 3, übereinstimmen. Wenn Diversität in Spezifikation, Entwurf und Codierung in beiden Kanälen des Teilsystems der Kategorie 3 oder 4 verwendet wird, kann ein PL_r e mit den oben erwähnten zusätzlichen Maßnahmen für PL_r c oder d erreicht werden.

ANMERKUNG Für SRESW mit Diversität in Entwurf und Codierung für Komponenten von Teilsystemen der Kategorie 3 oder Kategorie 4 oder in Testkanälen der Kategorie 2 kann der Aufwand in Zusammenhang mit den zu treffenden Maßnahmen, um systematische Ausfälle zu vermeiden, vermindert werden durch z. B. Überprüfung von Teilen der Software nur durch Berücksichtigung der strukturellen Aspekte, statt durch Prüfen jeder Codezeile. Anhang G enthält einen Leitfaden zu den anwendbaren Maßnahmen für die Durchführung dieser Aspekte.

7.3.2 Alternative Verfahren für nicht zugängliche Embedded-Software

Wenn es dem Konstrukteur des SRP/CS nicht möglich ist, auf die Embedded-Software zuzugreifen, z. B. SPS ohne Sicherheitsbewertung durch den Hersteller, können die SRESW-Anforderungen von 7.3.1 nicht erfüllt werden. Diese Komponenten dürfen unter den folgenden alternativen Bedingungen verwendet werden:

— das Teilsystem ist auf PL a oder PL b begrenzt und verwendet Kategorie B, 2 oder 3;

— das Teilsystem ist auf PL c mit Kategorie 2 oder PL d mit Kategorie 3 begrenzt und es ist notwendig, die Diversitätsanforderungen des CCF zu erfüllen, wobei beide Kanäle voneinander verschiedene Technologien/Entwürfe oder physikalische Prinzipien nutzen;

— die zugehörige Hardware und die Anforderungen an die SRASW müssen in Übereinstimmung mit den Anforderungen dieses Dokuments beurteilt werden, insbesondere hinsichtlich CCF (siehe Anhang F).

7.4 Sicherheitsbezogene Anwendungssoftware (SRASW)

Die Aktivitäten im Lebenszyklus der Softwaresicherheit (siehe 7.1) gelten auch für SRASW.

SRASW geschrieben in LVL und in Übereinstimmung mit den folgenden Anforderungen kann einen PL a bis PL e erzielen. Wenn SRASW in FVL geschrieben ist, müssen die Anforderungen an SRESW erfüllt und PL a bis PL e kann erzielt werden. Entscheidungshilfen bezüglich FVL bzw. LVL sind in Bild 15 angegeben.

Wenn ein Teil der SRASW innerhalb einer Komponente irgendeinen Einfluss (z. B. bei Modifikation) auf verschiedene Sicherheitsfunktionen mit unterschiedlichen PL hat, dann müssen die Anforderungen des zugehörigen höchsten PL angewendet werden.

Bei SRASW für Komponenten mit einem PL_r von a bis e müssen die folgenden grundlegenden Maßnahmen angewendet werden:

— Entwicklungslebenszyklus mit Verifizierungs- und Validierungsaktivitäten, z. B. Prüfungen und Tests, siehe Bild 14 für LVL;

— Dokumentation der Spezifikation und des Entwurfs;

— modulare und strukturierte Programmierung;

— Funktionstests;

— geeignete Entwicklungsaktivitäten nach Änderungen.

Für SRASW in Komponenten mit einem PL_r von c bis e gelten die folgenden zusätzlichen Maßnahmen mit steigender Wirksamkeit (niedrigere Wirksamkeit für PL_r c, mittlere Wirksamkeit für PL_r d, höhere Wirksamkeit für PL_r e).

Für den Testkanal in Kategorie 2 werden die Anforderungen um einen Performance Level reduziert. Kommt in den Funktionskanälen der Kategorie 3 oder 4 Diversität zum Einsatz, werden die Anforderungen um einen Performance Level reduziert.

a) Die Software-Design-Spezifikation muss überprüft (siehe auch Anhang J) und allen Personen, die am Lebenszyklus beteiligt sind, zur Verfügung gestellt werden, und muss die Beschreibung enthalten von:

   1) Sicherheitsfunktionen mit erforderlichem PL und zugehörigen Betriebsarten;

   2) Leistungskriterien, z. B. Reaktionszeiten;

   3) Kommunikationsschnittstellen;

   4) Erkennung und Beherrschung von Hardware-Ausfällen, um den erforderlichen DC und die Reaktion auf einen Fehler zu erreichen.

b) Auswahl der Tools, Bibliotheken, Sprachen:

   1) Tools müssen für die jeweilige Anwendung geeignet sein. Technische Fähigkeiten, die Bedingungen erkennen, die zu systematischen Fehlern führen können (wie z. B. Datentyp-Unverträglichkeit, mehrdeutige dynamische Speicherzuordnung, unvollständiger Aufruf von Schnittstellen, Rekursion, Zeigerarithmetik), müssen verwendet werden. Überprüfungen müssen hauptsächlich während der Kompilierung durchgeführt werden und nicht nur während der Laufzeit. Tools sollten Sprachenteilmengen und Programmierrichtlinien erzwingen oder mindestens den Entwickler leiten oder führen. Bei einem PL e, der mit einer Komponente und dessen Tool erreicht wird, muss das Tool der zutreffenden Komponentennorm entsprechen. Falls zwei verschiedene Komponenten mit unterschiedlichen Tools verwendet werden, können Erfahrungen aus dem erfolgreichen Betrieb in früheren Projekten ausreichend sein.

2) Wann immer vernünftigerweise durchführbar, sollten validierte Funktionsblock (FB)-Bibliotheken verwendet werden — entweder vom Werkzeughersteller gelieferte sicherheitsbezogene Funktionsblock-Bibliotheken (besonders empfohlen für PL e) oder validierte anwendungsspezifische FB-Bibliotheken in Übereinstimmung mit diesem Dokument.

3) Eine begründete LVL-Teilmenge, geeignet für ein modulares Verfahren, sollte verwendet werden (siehe 7.2.1), z. B. eine anerkannte Teilmenge der IEC 61131-3-Sprachen.

c) Das Softwaredesign muss folgende Merkmale haben:

1) semiformale Verfahren, um den Daten- und Kontrollfluss zu beschreiben, z. B. Zustandsdiagramm oder Programmflussdiagramm;

2) modulare und strukturierte Programmierung, überwiegend realisiert durch die Bereitstellung validierter sicherheitsbezogener Funktionsblock-Bibliotheken oder anderer Modulstrukturen zum Erreichen einer einfachen Code-Lesbarkeit und -testfähigkeit;

3) Funktionsbausteine mit begrenzter Codelänge;

4) Ausführung des Codes innerhalb des Funktionsbausteins mit nur einem Eingangspunkt und nur einem Ausgangspunkt;

5) dreistufiges Architektur-Modell: Eingänge ⇒ Verarbeitung ⇒ Ausgänge (siehe Bild 16 und Anhang J);

6) Zuordnung eines Sicherheitsausgangs an nur einer Stelle im Programm;

7) Verwendung von Techniken zur Detektion und Beherrschung von Hardware-Ausfällen und zur defensiven Programmierung innerhalb von Eingangs-, Verarbeitungs- und Ausgangsbausteinen, die zum sicheren Zustand führen.

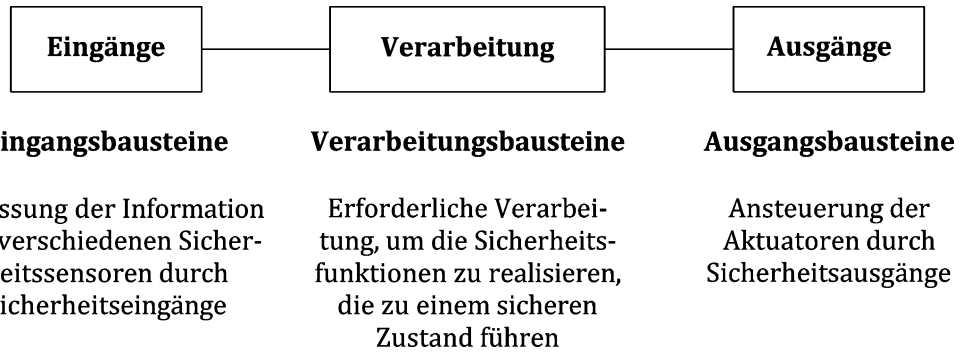


Bild 16 — Allgemeines Architekturmodell für Software

d) Wo SRASW und nicht-SRASW in einer Komponente kombiniert werden:

1) müssen SRASW und nicht-SRASW in unterschiedlichen Funktionsblöcken codiert werden, mit sorgfältig definierten Datenschnittstellen;

2) darf es keine logische Verknüpfung von nicht sicherheitsbezogenen und sicherheitsbezogenen Daten geben, die zur Herabstufung der Integrität der sicherheitsbezogenen Signale führen kann, z. B. Verknüpfen eines sicherheitsbezogenen und eines nicht sicherheitsbezogenen Signals durch ein logisches „ODER“, dessen Ausgang sicherheitsbezogene Signale steuert.

e) Softwareimplementierung/Codierung:

1) der Code muss lesbar, verständlich und testfähig sein, und aufgrund dessen sollten symbolische Variablen (anstelle expliziter Hardwareadressen) angewendet werden;

2) begründete oder akzeptierte Codierungsrichtlinien müssen verwendet werden (siehe auch Anhang J);

3) Datenintegritäts- und Plausibilitätsprüfungen (z. B. Bereichsüberprüfungen) auf Anwendungsebene (defensive Programmierung) sollten verwendet werden;

4) der Code sollte durch Simulation getestet werden;

5) die Verifizierung sollte durch Kontrollflussanalyse und Datenflussanalyse bei PL d oder PL e erfolgen.

f) Testen:

1) das angemessene Validierungsverfahren ist der Black-Box-Test des Funktionsverhaltens und der Leistungskriterien (z. B. zeitliches Leistungsverhalten);

2) für PL d oder PL e wird eine Testfallausführung auf der Basis von Grenzwertanalysen empfohlen;

3) eine Testplanung sollte Testfälle mit Abschlussbedingungen und erforderlichen Tools enthalten;

4) I/O-Tests müssen sicherstellen, dass die sicherheitsbezogenen Signale in der SRASW korrekt verwendet werden.

g) Dokumentation:

1) alle Lebenszyklus- und Änderungsaktivitäten müssen dokumentiert werden;

2) die Dokumentation muss vollständig, verfügbar, lesbar und verständlich sein;

3) die Codedokumentation innerhalb des Quelltextes muss Modulköpfe enthalten mit einer juristischen Person, Funktions- und I/O-Beschreibung, Version der verwendeten Funktionsblock-Bibliothek und ausreichender Kommentierung der Netzwerke/Anweisung und Deklarationszeilen.

h) Verifizierung:

1) Die Verifizierung muss beispielsweise durch Überprüfung, Inspektion, Walk-through oder durch andere geeignete Aktivitäten erfolgen.

ANMERKUNG Eine Verifizierung wird nur für einen anwendungsspezifischen Code angewendet und nicht für validierte Bibliotheksfunktionen.

i) Konfigurationsmanagement:

1) Die Einführung von Verfahren und Datensicherung wird besonders empfohlen, um alle Dokumente, Softwaremodule, Ergebnisse der Verifizierung/Validierung und Toolkonfiguration, die im Bezug zu einer bestimmten SRASW stehen, zu identifizieren und zu archivieren.

j) Änderungen:

1) Bevor eine Änderung der SRASW vorgenommen wird, muss eine Auswirkungsanalyse durchgeführt werden, um die Übereinstimmung mit dem Softwaredesign sicherzustellen. Nach Änderungen müssen angemessene Lebenszyklusaktivitäten stattfinden. Es müssen Maßnahmen zum Schutz vor unberechtigten Änderungen an der SRASW umgesetzt und der Änderungsverlauf muss dokumentiert werden.

8 Verifizierung des erreichten Performance Levels

Für jede einzelne Sicherheitsfunktion muss der PL des zugehörigen SRP/CS dem nach 5.3 und 6.1.1 bestimmten erforderlichen Performance Level (PL_r) entsprechen oder größer als dieser sein. Wenn das nicht der Fall ist, wird eine Wiederholung des Prozesses, wie in Bild 4 beschrieben, notwendig.

Der PL der verschiedenen Teilsysteme, die Teil einer Sicherheitsfunktion sind, muss größer oder gleich dem PL_r dieser Sicherheitsfunktion sein (siehe 5.3 und 6.1.1).

9 Ergonomische Entwurfsaspekte

Die Schnittstelle zwischen den Bedienern und dem SRP/CS muss so gestaltet und konstruiert werden, dass die Gefährdungsexposition während der bestimmungsgemäßen Verwendung und der vernünftigerweise vorhersehbaren Fehlanwendung der Maschine, die aus der Nichtbeachtung ergonomischer Grundsätze resultieren, minimiert wird.

Es gelten die in ISO 12100:2010, 6.2.8, angegebenen ergonomischen Grundsätze.

ANMERKUNG Ergonomische Grundsätze sollen die Benutzerfreundlichkeit der Steuerungen verbessern, um den Anreiz zum Umgehen oder eine unbeabsichtigte Fehlanwendung der Maschine zu vermeiden. Siehe ISO/TR 22100-3 und ISO 9241-210 für Leitlinien zur Ergonomie.

10 Validierung

10.1 Grundsätze der Validierung

10.1.1 Allgemeines

Der Zweck des Validierungsprozesses ist es, zu bestätigen, dass das SRP/CS der gesamten SRS entspricht, die nach Abschnitt 5 und Abschnitt 7 erstellt wurde.

Bild 17 zeigt eine Übersicht über den Validierungsprozess. Die Validierung besteht aus der Durchführung einer Analyse (siehe 10.3) und der Ausführung von Tests (siehe 10.4) unter vorhersehbaren Bedingungen in Übereinstimmung mit dem Validierungsplan.

ANMERKUNG 1 Durch die SRP/CS-Validierung wird sichergestellt, dass die Sicherheitsfunktionen die vorgesehene Risikominderung erzielen, und sie ist als Teil des Gesamtvalidierungsprozesses der Maschine gedacht.

Die Validierungstätigkeiten müssen die Vollständigkeit und Richtigkeit jeder im Validierungsplan gekennzeichneten Entwurfstätigkeit sicherstellen.

Die auf das SRP/CS anzuwendende Validierung umfasst die Inspektion (z. B. durch Analyse) und das Testen des SRP/CS, um sicherzustellen, dass es die in der SRS (nach Abschnitt 5) angegebenen Anforderungen erfüllt.

Die Validierung muss belegen, dass das SRP/CS den Anforderungen entspricht, insbesondere den folgenden:

a) den festgelegten funktionalen Anforderungen der Sicherheitsfunktionen, wie in der SRS festgelegt;

b) den Anforderungen des festgelegten PL nach 6.1.1:

   1) den Anforderungen der festgelegten Kategorie;

   2) den Maßnahmen zur Beherrschung und Vermeidung systematischer Ausfälle (systematische Integrität);

   3) sofern zutreffend, den Softwareanforderungen; und

   4) der Fähigkeit, eine Sicherheitsfunktion unter vorhersehbaren Umgebungsbedingungen auszuführen;

c) der ergonomischen Gestaltung von, der Interaktion mit und der Anordnung von Bedienerschnittstellen.

Der Validierungsprozess sollte von (einer) Person(en) durchgeführt werden, die vom Entwurf des SRP/CS unabhängig ist/sind.

ANMERKUNG 2 Eine unabhängige Person ist eine Person, die nicht am Entwurf des SRP/CS beteiligt war, und bedeutet nicht unbedingt, dass eine dritte Partei erforderlich ist.

Die Analyse sollte so früh wie möglich und parallel zum Entwurfsprozess gestartet werden. Es kann notwendig sein, dass einige Teile der Analyse später als geplant erfolgen, wenn der Entwurf weiterentwickelt ist.

ANMERKUNG 3 Dadurch können Probleme frühzeitig behoben werden, während sie sich noch relativ einfach beheben lassen, d. h. während der Schritte „Entwurf und technische Realisierung der Sicherheitsfunktion“ und „Bewerten des PL“.

Wenn es aufgrund der Größe des Systems, der Komplexität oder der Auswirkungen seiner Integration in die Steuerung (der Maschine) notwendig ist, sollten besondere Vorkehrungen getroffen werden für:

— die separate Validierung des Teilsystem vor der Integration, einschließlich einer Simulation von geeigneten Eingangs- und Ausgangssignalen; und

— die Validierung der Auswirkungen der Integration von SRP/CS auf die verbleibende Steuerung in Zusammenhang mit ihrer Verwendung in der Maschine.

Das Verhältnis von Analyse und den Tests hängt von der Technologie ab, die für das SRP/CS zum Einsatz kommt, sowie von dem erforderlichen Performance Level (PL_r). Für die Kategorien 2, 3 und 4 muss die Validierung der Sicherheitsfunktionen auch das Testen durch geeignete Fehlerimplementierung umfassen, um aufzuzeigen, dass die Reaktion auf einen Fehler unter anderem von der vorhandenen Diagnosefunktion ausgelöst wird.

„Änderung des Entwurfs“ in Bild 17 bezieht sich auf den Entwurfsprozess. Falls die Validierung nicht erfolgreich abgeschlossen werden kann, sind Änderungen des Entwurfs notwendig. Die Validierung der geänderten Teile des SRP/CS muss dann wiederholt werden. Dieser Prozess muss wiederholt werden, bis das SRP/CS für jede Sicherheitsfunktion erfolgreich validiert worden ist.

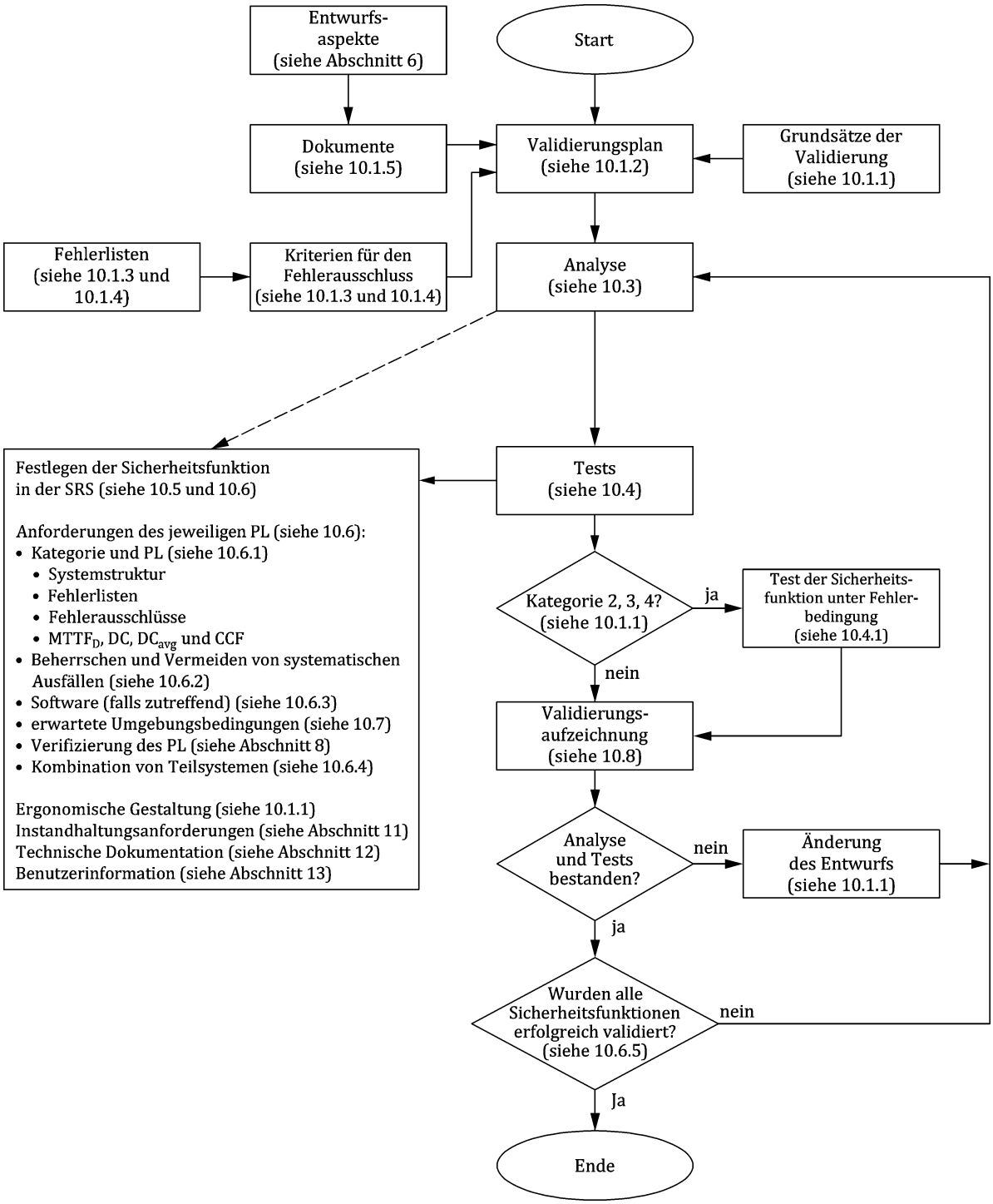


Bild 17 — Übersicht über den Validierungsprozess

10.1.2 Validierungsplan

Der Validierungsplan muss die Anforderungen an die Durchführung des Validierungsprozesses festlegen und beschreiben und muss betroffenen Personen und Parteien verfügbar gemacht werden, die am Validierungsprozess beteiligt sind. Der Validierungsplan muss auch die Maßnahmen festlegen, die umzusetzen sind, um die festgelegten Sicherheitsfunktionen zu validieren. Er muss Folgendes festlegen, soweit angemessen:

a) die Dokumente für die Spezifikationen;

b) die Betriebs- und Umgebungsbedingungen während des Tests;

c) die durchzuführenden Analysen und Tests;

d) die Verweisung auf anzuwendende Prüfnormen; und

e) für jeden Schritt im Validierungsprozess die verantwortlichen Personen oder Parteien.

10.1.3 Allgemeine Fehlerlisten

Die Validierung schließt eine Betrachtung des Verhaltens des SRP/CS bei allen anzunehmenden Fehlern ein. Eine Grundlage für die Fehlerbetrachtung ist in den Fehlerlistentabellen von ISO 13849-2:2012, Anhang A bis Anhang D, zu finden, die auf Erfahrungen basieren und Folgendes enthalten:

— die einzubeziehenden Bauteile/Elemente, z. B. Leiter/Kabel;

— die zu berücksichtigenden Fehler, z. B. Kurzschlüsse zwischen Leitern;

— die erlaubten Fehlerausschlüsse, unter Berücksichtigung von Umgebungs-, Betriebs- und Anwendungsaspekten; und

— eine Spalte für Bemerkungen, die die Begründungen für Fehlerausschlüsse enthält.

In den Fehlerlisten sind nur permanente Fehlzustände berücksichtigt.

10.1.4 Spezielle Fehlerlisten

Falls notwendig, muss eine spezielle auf das Produkt bezogene Fehlerliste als Bezugsdokument für die Validierung des Teilsystems/der Teilsysteme und/oder des Teilsystemelements/der Teilsystemelemente erstellt werden. Diese Liste kann auf der/den entsprechenden allgemeinen Liste(n) basieren, die in den Anhängen von ISO 13849-2:2012 zu finden ist/sind, oder auf (wiederkehrenden) Fehlern, die als Ergebnis einer Produktüberwachung festgestellt wurden.

Wenn diese spezielle auf das Produkt bezogene Fehlerliste auf der/den allgemeinen Liste(n) aufbaut, muss Folgendes darin angegeben sein:

a) die aus der/den allgemeinen Liste(n) einzubeziehenden Fehler;

b) alle anderen maßgeblichen aufzunehmenden Fehler, die nicht in der allgemeinen Liste aufgeführt sind (z. B. Ausfälle infolge gemeinsamer Ursache);

c) die aus der/den allgemeinen Liste(n) entnommenen Fehler, die auf der Grundlage ausgeschlossen werden dürfen, dass die in den allgemeinen Listen enthaltenen Kriterien erfüllt werden; und

d) in Ausnahmefällen alle anderen Fehler, für die eine Rechtfertigung und Begründung für einen Ausschluss vorgelegt wird.

Wenn diese Liste nicht auf der/den allgemeinen Liste(n) aufbaut, muss der Konstrukteur eine Begründung für Fehlerausschlüsse geben.

10.1.5 Angaben zur Validierung

Die für die Validierung notwendigen Angaben unterscheiden sich je nach angewendeter Technologie, der/den nachzuweisenden Kategorie(n) und dem PL, der SRS und des Beitrags des SRP/CS zur Risikominderung. Dokumente aus der nachfolgenden Liste, die ausreichende Informationen enthalten, müssen in die Validierung aufgenommen werden, um nachzuweisen, dass das SRP/CS die festgelegten Sicherheitsfunktionen mit dem erforderlichen PL und der erforderlichen Kategorie ausführt:

a) SRS einschließlich der geforderten Eigenschaften jeder Sicherheitsfunktion, z. B. Ansprechzeit (nach ISO 13855:2010), Betriebsart, PL, Schnittstellen zwischen den Teilsystemen des SRP/CS und, sofern notwendig, Eigenschaften der angewendeten Kategorie jedes Teilsystems des SRP/CS;

b) Zeichnungen und Festlegungen, z. B. für mechanische, hydraulische und pneumatische Teile, gedruckte Schaltungen, Montagepläne, interne Verdrahtung, Gehäuse, Werkstoffe, Einbau;

c) Blockdiagramm(e) und, sofern zur Verdeutlichung notwendig, eine Funktionsbeschreibung der Blöcke;

d) Schaltpläne einschließlich ihrer Verknüpfungen/Verbindungen;

e) Funktionsbeschreibung des Schaltplans/der Schaltpläne, sofern notwendig zur Verdeutlichung;

f) Ablaufdiagramm(e) für schaltende Bauteile und Signale, die sicherheitsrelevant sind;

g) Beschreibung der entsprechenden Eigenschaften von bereits zuvor validierten Bauteilen;

h) für andere als die unter g) aufgeführten SRP/CS die Bauteillisten, z. B. mit Stückbezeichnungen, Nennwerten, Grenzabmaßen, maßgeblichen Betriebsbeanspruchungen, Typbezeichnungen, Daten über Ausfallraten und Bauteilhersteller und alle weiteren Daten, die für die Sicherheit maßgebend sind;

ANMERKUNG 1 Die Daten können in Übereinstimmung mit VDMA 66413 in Bibliotheken bereitgestellt werden.

i) Bericht über die Analyse aller maßgeblichen Fehler nach 10.1.3 und 10.1.4, die z. B. in den Tabellen von ISO 13849-2:2012, Anhang A bis Anhang D, aufgeführt sind, einschließlich der Begründung aller Fehlerausschlüsse;

j) Bericht über die Analyse des Einflusses der im Verfahren verwendeten Werkstoffe;

k) Benutzerinformation, Instandhaltungsanforderungen, z. B. Anleitung für Aufbau und Betrieb/Benutzerhandbuch.

Wenn Software für die Sicherheitsfunktion(en) maßgeblich ist, muss die Software-Dokumentation Folgendes enthalten:

— eine Spezifikation, die klar und eindeutig ist;

— den Nachweis, dass die Software so entworfen ist, dass sie den erforderlichen PL erreicht (siehe 10.6.3); und

— Einzelheiten über Tests (insbesondere Testberichte), die durchgeführt wurden, um nachzuweisen, dass der erforderliche PL erreicht wurde.

Es sind Informationen darüber notwendig, wie der PL und die PFH bestimmt werden. Die Dokumentation der quantifizierbaren Aspekte muss Folgendes enthalten:

— das sicherheitsbezogene Blockdiagramm oder die vorgesehene Architektur nach 6.1.3.2;

— die Bestimmung von $MTTF_D$, DC_{avg} und CCF; und

— die Bestimmung der Kategorie.

ANMERKUNG 2 Für Leitlinien zum sicherheitsbezogenen Blockdiagramm siehe Anhang B.

In der Dokumentation sind Angaben über Maßnahmen gegen systematische Ausfälle des SRP/CS erforderlich.

Es sind Angaben darüber erforderlich, inwiefern die Kombination mehrerer Teilsysteme den erforderlichen PL erreicht.

ANMERKUNG 3 Soweit möglich, ist eine verständliche und rückverfolgbare Referenzierung auf bestehende Dokumente akzeptabel.

10.2 Validierung der Spezifikation der Sicherheitsanforderungen (SRS)

Vor der Validierung des Entwurfs des SRP/CS oder der Kombination von Teilsystemen, die die Sicherheitsfunktion ausführen, muss die Spezifikation der Anforderungen an die Sicherheitsfunktion verifiziert werden, um die Übereinstimmung und Vollständigkeit für ihren vorgesehenen Verwendungszweck sicherzustellen (siehe 5.4).

Um die Spezifikation zu validieren, sind geeignete Maßnahmen zur Erkennung systematischer Ausfälle (Fehler, Abweichungen oder Inkonsistenzen) anzuwenden.

Die Validierung kann durch Prüfungen und Inspektionen der SRS erfolgen, insbesondere unter Berücksichtigung von Folgendem:

— den vorgesehenen Anwendungsanforderungen;

— der Risikobeurteilung;

— den Betriebs- und Umgebungsbedingungen; und

— der vernünftigerweise vorhersehbaren Fehlanwendung.

10.3 Validierung durch Analyse

10.3.1 Allgemeines

Die Validierung des SRP/CS muss durch eine Analyse erfolgen. In die Analyse gehen ein:

— die nach 5.2 festgelegte(n) Sicherheitsfunktion(en), ihre Eigenschaften und die Sicherheitsintegrität;

— die Systemstruktur (z. B. vorgesehene Architekturen) nach 6.1.3.2;

— die quantifizierbaren Aspekte ($MTTF_D$, DC_{avg} und CCF) nach 6.1.4, 6.1.5 und 6.1.6 durch Validierung von Annahmen und Daten, die bei der Auswahl der in den Systemberechnungen verwendeten Werte berücksichtigt wurden;

— die nicht quantifizierbaren, qualitativen Aspekte, die das Systemverhalten beeinträchtigen (gegebenenfalls Softwareaspekte);

— deterministische Betrachtungen;

— Fehlerlisten;

— Kriterien für den Fehlerausschluss.

ANMERKUNG Ein deterministisches Argument ist ein Argument, das auf qualitativen Aspekten (z. B. Qualität bei der Herstellung, Erfahrungen bei der Anwendung) basiert. Diese Betrachtung ist abhängig von der Anwendung, welche zusammen mit anderen Faktoren die deterministischen Argumente beeinträchtigen kann. Deterministische Argumente unterscheiden sich von anderen Anhaltspunkten dadurch, dass sie zeigen, dass die geforderten Eigenschaften des Systems logisch einem Systemmodell folgen. Derartige Argumente können auf der Grundlage einfacher, gut verständlicher Konzepte entwickelt werden.

10.3.2 Analysetechniken

Die beiden folgenden Grundtechniken können zur Analyse angewendet werden:

a) (deduktive) „Top-down"-Techniken sind zur Bestimmung der auslösenden Ereignisse geeignet, die zu den festgestellten Top-Ereignissen und zur Berechnung der Wahrscheinlichkeit von Top-Ereignissen aus der Wahrscheinlichkeit der auslösenden Ereignisse führen können. Sie können auch angewendet werden bei der Untersuchung der Folgen von erkannten Mehrfachfehlern.

   BEISPIEL 1 FTA (siehe IEC 61025), ETA (siehe IEC 62502).

b) (Induktive) „Bottom-up"-Techniken sind für die Untersuchung der Auswirkungen von festgestellten Einzelfehlern geeignet.

   BEISPIEL 2 FMEA (siehe IEC 60812) und Ausfalleffekt- und Kritikalitätsanalyse (FMECA, siehe IEC 60812).

10.4 Validierung durch Prüfung

10.4.1 Allgemeines

Die Prüfung muss Teil der Validierung sein. Im Fall von Kategorie B oder 1 sind keine Prüfungen unter Fehlerbedingungen erforderlich und die Analyse mithilfe von Funktionstests kann ausreichend sein.

Die Validierungsprüfungen müssen geplant und in logischer Weise ausgeführt werden. Das heißt insbesondere:

a) vor Beginn der Prüfungen muss ein Prüfplan ausgearbeitet werden, der Folgendes enthalten muss:

   1) die Prüfspezifikationen;

   2) die für die Einhaltung erforderlichen Ergebnisse der Prüfungen; und

   3) die zeitliche Abfolge der Prüfungen, sofern zutreffend;

b) Prüfaufzeichnungen müssen erstellt werden, die folgende Angaben enthalten:

   1) den Namen der Person, die die Prüfung durchführt;

   2) die Umgebungsbedingungen;

   3) den Prüfablauf und die verwendete Ausrüstung;

   4) das Prüfdatum; und

   5) die Ergebnisse der Prüfung;

c) die Prüfaufzeichnungen müssen mit dem Prüfplan verglichen werden, um sicherzustellen, dass die festgelegten Funktions- und Leistungsziele erreicht sind.

Die Prüfung am Prüfling muss möglichst mit seiner endgültigen Betriebskonfiguration durchgeführt werden, d. h. mit allen peripheren Geräten und mit allen Abdeckungen an ihren vorgesehenen Stellen.

Die Prüfungen dürfen manuell oder automatisch, z. B. durch Computer, durchgeführt werden.

Sofern angebracht, muss die Validierung der Sicherheitsfunktionen durch Prüfung durchgeführt werden, indem Eingangssignale in verschiedenen Kombinationen in das SRP/CS eingegeben werden. Die endgültige Reaktion an den Ausgängen muss mit den spezifizierten Ausgangssignalen verglichen werden.

Die Kombination dieser Eingangssignale sollte systematisch in die Steuerung und Maschine eingegeben werden, z. B. Energie einschalten, in Betrieb setzen, Betrieb, Richtungsänderungen, Wiederanlaufen. Es sollte ein erweiterter Umfang von Eingangsdaten eingegeben werden, um anormale oder ungewöhnliche Situationen zu berücksichtigen, und um zu sehen, wie das SRP/CS reagiert. Derartige Kombinationen von Eingangsdaten sollten vorhersehbare fehlerhafte Bedienungen berücksichtigen.

Wenn die Validierung durch Analyse nicht überzeugend ist, müssen Prüfungen durchgeführt werden, um die Validierung abzuschließen. Die Prüfungen erfolgen immer in Ergänzung zur Analyse und sind oftmals notwendig.

10.4.2 Messgenauigkeit

Die Messgenauigkeit bei der Validierung durch Prüfung muss für die durchgeführte Prüfung angemessen sein. Im Allgemeinen müssen diese Messgenauigkeiten innerhalb von $\pm$5 K bei Temperaturmessungen liegen und bei $\pm$5 % für folgende Messungen:

a) Zeitmessungen;

b) Druckmessungen;

c) Kraftmessungen;

d) elektrische Messungen;

e) Messungen der relativen Luftfeuchte;

f) Längenmessungen.

Abweichungen von diesen Messgenauigkeiten müssen begründet werden.

10.4.3 Zusätzliche Prüfanforderungen

Fall die SRP/CS höhere Anforderungen erfüllen muss als in diesem Dokument angegeben, muss die Prüfung erweitert werden, um diese höheren Anforderungen ebenfalls abzudecken.

ANMERKUNG In Abhängigkeit von der Risikobeurteilung können höhere Anforderungen zugrunde gelegt werden, wenn die Steuerung besonders ungünstigen Betriebsbedingungen standhalten muss, z. B. grobe Handhabung, Einwirkungen von Luftfeuchte, Hydrolyse, Schwankungen der Umgebungstemperatur, Auswirkungen von chemischen Substanzen, Korrosion, hohe Intensität elektromagnetischer Felder, z. B. aufgrund der Nähe zu Sendern.

10.4.4 Anzahl der Prüflinge

Soweit nicht anders in der Prüfspezifikation festgelegt, müssen die Prüfungen an einem einzelnen Produktionsmuster des zu prüfenden Teilsystems durchgeführt werden.

Das/die Teilsystem(e), das/die sich in der Prüfung befindet/n, darf/dürfen während des Prüfablaufs nicht verändert werden.

Bestimmte Prüfungen können dauerhaft die Leistungsfähigkeit einiger Bauteile verändern. Wenn eine dauerhafte Veränderung in einem Bauteil dazu führt, dass das sicherheitsbezogene Teil die Anforderungen weiterer Prüfungen nicht mehr erfüllen kann, muss/müssen (ein) neue(r) Prüfling(e) für nachfolgende Prüfungen verwendet werden.

Wenn eine bestimmte Prüfung zerstörend wirkt und gleichwertige Ergebnisse durch die Prüfung eines separaten Teils des SRP/CS erhalten werden können, darf ein Prüfling dieses Teils des SRP/CS anstelle des gesamten SRP/CS benutzt werden, um die Ergebnisse der Prüfung zu erhalten. Dieses Vorgehen darf nur angewendet werden, wo durch Analyse nachgewiesen wurde, dass die Prüfung eines Teils des SRP/CS ausreichend ist, um die sicherheitstechnische Leistungsfähigkeit des gesamten SRP/CS, das die Sicherheitsfunktion ausführt, nachzuweisen.

10.4.5 Prüfverfahren

Je nach Anwendungsart sind verschiedene Prüfverfahren anzuwenden, um das SRP/CS zu validieren. Bei einigen Anwendungen kann es notwendig sein, die verbundenen SRP/CS in mehrere Funktionsgruppen aufzuteilen und diese Gruppen und ihre Verknüpfungen Fehlersimulationsprüfungen zu unterziehen. Der genaue Zeitpunkt, wann ein Fehler in ein System eingegeben wird, kann entscheidend sein. Die ungünstigste Auswirkung (en: worst case effect) einer Fehlereinspeisung ist durch Analyse und durch Einspeisung des Fehlers zu diesem geeigneten kritischen Zeitpunkt zu bestimmen. Übliche Prüfverfahren sind:

a) eine Simulation des Verhaltens der Steuerung bei Auftreten eines Fehlers, z. B. mithilfe von entweder Hardware- oder Softwaremodellen oder beidem;

b) Softwaresimulation von Fehlern;

c) Funktionsprüfung der Sicherheitsfunktionen in allen Betriebsarten der Maschine, um festzustellen, ob sie mit den festgelegten Eigenschaften übereinstimmen (siehe Abschnitt 5). Die Funktionsprüfungen müssen sicherstellen, dass alle sicherheitsbezogenen Ausgangssignale über ihren gesamten Bereich umgesetzt werden und auf sicherheitsbezogene Eingangssignale entsprechend der Spezifikation reagieren. Die Prüffälle werden üblicherweise aus den Spezifikationen abgeleitet, können jedoch auch einige Fälle enthalten, die aus der Analyse der Schaltpläne oder der Software abgeleitet sind;

d) erweiterte Funktionsprüfung, um vorhersehbare anomale Signale oder Kombinationen von Signalen aus einer beliebigen Eingangsquelle zu überprüfen, einschließlich Energieunterbrechung und -wiederkehr und Fehlbedienungen;

e) Prüfungen durch Fehlerimplementierung in den betroffenen Steuerkreis und Fehlerauslösung an tatsächlich vorhandenen Bauteilen, insbesondere in Teilen des Systems, bei denen es Zweifel hinsichtlich der bei der Fehleranalyse ermittelten Ergebnisse gibt;

f) Prüfungen durch Fehlereinspeisung in ein Produktionsmuster;

g) Prüfungen durch Fehlereinspeisung in ein Hardwaremodell;

h) Prüfungen durch Ausfall eines Teilsystems (z. B. Energieversorgung).

10.5 Validierung der Sicherheitsfunktionen

Die Validierung der Sicherheitsfunktionen muss nachweisen, dass das SRP/CS oder die Kombination der Teilsysteme die Sicherheitsfunktion(en) erfüllt, die den festgelegten Eigenschaften entspricht/entsprechen.

Die Validierung der festgelegten Eigenschaften der Sicherheitsfunktionen muss durch Anwendung geeigneter Maßnahmen durchgeführt werden, die im Folgenden aufgelistet sind:

a) funktionale Analyse der Schaltpläne, Überprüfungen der Software (siehe 10.6.3);

ANMERKUNG Wenn eine Maschine komplexe oder eine große Anzahl von Sicherheitsfunktionen aufweist, kann eine Analyse die Anzahl der erforderlichen Funktionsprüfungen verringern.

b) Simulation;

c) Überprüfung der in die Maschine eingebauten Hardwarekomponenten und Details der damit verbundenen Software, um ihre Übereinstimmung mit der Dokumentation (z. B. Hersteller, Art, Bauart) zu bestätigen;

d) Funktionstests (siehe 10.4.5);

e) Überprüfung der Bedieneroberfläche der SRP/CS auf Erfüllung ergonomischer Grundsätze.

10.6 Validierung der Sicherheitsintegrität des SRP/CS

10.6.1 Validierung von Teilsystem(en)

Die Sicherheitsintegrität jedes Teilsystems des SRP/CS muss validiert werden, indem die Anforderungen von Tabelle 10 entsprechend der verwendeten Kategorie bestätigt werden.

Tabelle 10 — Grundlegende Anforderungen an die zu validierenden Kategorien

Anforderungen	Kategorie				
	B	1	2	3	4
Grundlegende Sicherheitsprinzipien	X	X	X	X	X
Zu erwartende Betriebsbeanspruchungen	X	X	X	X	X
Einfluss der im Verfahren verwendeten Werkstoffe	X	X	X	X	X
Leistungsfähigkeit bei anderen maßgeblichen äußeren Einflüssen	X	X	X	X	X
Bewährte Bauteile	—	X	—	—	—
Bewährte Bauteile für die Bestimmung des PL ohne $MTTF_D$	—	X	X	X	X
Bewährte Sicherheitsprinzipien	—	X	X	X	X
$MTTF_D$ jedes Kanals	X	X	X	X	X
Erkennbare Fehler und zugehörige Diagnosemaßnahmen, einschließlich Fehlerreaktion	—	—	X	X	X
Prüfintervalle, sofern festgelegt	—	—	X	X	X
DC_{avg}	—	—	X	X	X
Festgestellte CCF und deren Vermeidung	—	—	X	X	X
Begründung für den Fehlerausschluss	X	X	X	X	X
Aufrechterhaltung der Sicherheitsfunktion bei jedem der Fehler	—	—	—	X	X
Aufrechterhaltung der Sicherheitsfunktion bei jeder Kombination von Fehlern	—	—	—	—	X
Maßnahmen gegen systematische Ausfälle	X	X	X	X	X
Maßnahmen gegen Softwarefehler	X	—	X	X	X

Legende
X erforderlich
— nicht erforderlich
ANMERKUNG Die Kategorien entsprechen denen, die in 6.1.3.2 angegeben sind.

Des Weiteren muss die Sicherheitsintegrität jedes Teilsystems des SRP/CS validiert werden, indem Folgendes bestätigt wird:

— die Wahrscheinlichkeit eines gefahrbringenden zufälligen Ausfalls der Hardware; und

— die systematische Integrität (siehe Anhang G, Abschnitt 7 Software, CCF).

In diesem Zusammenhang erfolgt die Validierung von $MTTF_D$ (einschließlich der Werte von B_{10D}, T_{10D} und n_{op}), DC_{avg} und CCF üblicherweise durch eine Analyse und Sichtprüfung.

Wenn die Inanspruchnahme von Fehlerausschlussen bedeutet, dass bestimmte Bauteile nicht zur $MTTF_D$ des Kanals beitragen, ist die Plausibilität des Fehlerausschlusses zu überprüfen.

ANMERKUNG Ein Fehlerausschluss setzt eine unendliche $MTTF_D$ voraus; deshalb tragen die Ausfallarten des Bauteils mit Fehlerausschluss nicht zur Berechnung der $MTTF_D$ des Kanals bei.

Die $MTTF_D$ jedes Kanals des Teilsystems, einschließlich Anwendung der Symmetrisierungsgleichung (siehe Anhang D) bei unterschiedlichen redundanten Kanälen, muss auf die richtige Berechnung überprüft werden. Die $MTTF_D$ einzelner Kanäle ist auf höchstens 100 Jahre (2 500 Jahre für Kategorie 4) zu begrenzen, bevor die Symmetrisierungsgleichung angewendet wird.

Die DC-Werte entweder von Bauteilen (Elementen des Teilsystems) oder von logischen Blöcken oder beidem müssen auf Plausibilität überprüft werden (z. B. anhand von Maßnahmen nach Anhang E). Die korrekte Durchführung (Hardware und Software) von Überprüfungen und Diagnosen einschließlich einer angemessenen Fehlerreaktion muss validiert werden, indem unter den für den Betrieb typischen Umgebungsbedingungen geprüft wird.

Die richtige Durchführung ausreichender Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache muss validiert werden (z. B. nach Anhang F). Typische Validierungsmaßnahmen sind eine statische Hardware-analyse und Funktionsprüfungen unter Umgebungsbedingungen.

Für die Festlegung der $MTTF_D$-Werte elektronischer Bauteile wird in der Regel eine Umgebungstemperatur von +40 °C als Grundlage angenommen. Während der Validierung ist es wichtig sicherzustellen, dass die als Grundlage angenommenen Umgebungs- und Funktionsbedingungen (besonders die Temperatur) für $MTTF_D$-Werte erfüllt werden. Wenn eine Baugruppe oder ein Bauteil deutlich über (z. B. > 10 K) der festgelegten Temperatur von +40 °C betrieben wird, ist es notwendig, $MTTF_D$-Werte für die erhöhte Umgebungstemperatur zu verwenden.

10.6.2 Validierung der Maßnahmen zur Vermeidung systematischer Ausfälle

Die Validierung der Maßnahmen zur Vermeidung systematischer Ausfälle kann üblicherweise durchgeführt werden durch:

a) Überprüfungen von Entwurfsdokumenten, die die Übereinstimmung mit Folgendem bestätigen:

   1) grundlegenden und bewährten Sicherheitsprinzipien (siehe ISO 13849-2:2012, Anhang A bis Anhang D);

   2) weiteren Maßnahmen zur Vermeidung systematischer Ausfälle nach Anhang G; und

   3) weiteren Maßnahmen zur Beherrschung systematischer Ausfälle wie Diversität der Hardware, Schutz vor Änderungen oder „Failure Assertion"-Programmierung (en: failure assertion programming);

b) Fehleranalyse (z. B. FMEA);

c) Prüfungen durch Fehlereingabe/Fehlerauslösung;

d) Inspektion und Prüfung von Datenkommunikation, sofern verwendet;

e) Überprüfungen, ob ein Qualitätsmanagementsystem zur Vermeidung systematischer Ausfälle im Fertigungsprozess angewendet wird.

ANMERKUNG Systematische Ausfälle können durch Fehler während des Entwurfs und der Integration verursacht worden sein (z. B. durch eine Fehlinterpretation der Eigenschaften der Sicherheitsfunktion, einen Fehler in der logischen Gestaltung, einen Fehler innerhalb des Hardwareaufbaus, einen Fehler beim Tippen des Softwarecodes). Einige dieser Fehler werden während des Entwurfsprozesses entdeckt, während andere während des Validierungsvorgangs erkannt werden oder unbemerkt bleiben. Zusätzlich ist es möglich, einen Fehler während des Validierungsprozesses zu begehen (z. B. Nicht-Überprüfung einer Eigenschaft).

10.6.3 Validierung der sicherheitsbezogenen Software

Die Validierung der Software muss Folgendes umfassen:

— das festgelegte Funktionsverhalten und die Leistungskriterien (z. B. Zeitverhalten) der Software, wenn sie auf der Zielhardware ausgeführt wird;

— eine Verifizierung, ob die Softwaremaßnahmen für den festgelegten PL_r der Sicherheitsfunktion ausreichen; und

— eine Verifizierung durch Einsichtnahme in die dokumentierten Nachweise, ob die bei der Softwareentwicklung geplanten Schutzmaßnahmen und Aktivitäten zur Vermeidung systematischer Softwarefehler angewendet wurden.

Als erster Schritt wird überprüft, ob eine Dokumentation der Spezifikation und des Entwurfs der sicherheitsbezogenen Software vorhanden ist. Diese Dokumentation ist auf ihre Vollständigkeit sowie auf die Vermeidung von fehlerhaften Auslegungen, Auslassungen und Widersprüchen zu überprüfen.

Im Allgemeinen kann die Software als „Black Box“ oder „Grey Box“ (siehe Abschnitt 7) betrachtet und entsprechend durch Black-Box- bzw. Grey-Box-Tests validiert werden.

ANMERKUNG 1 Bei kleinen Programmen kann eine Programmanalyse durch Überprüfungen oder Walk-trough des Kontrollflusses und Prozeduren mithilfe der Softwaredokumentation (Kontrollflussgraph, Quellcodes von Modulen oder Blöcken, I/O und Variablenzuweisungslisten, Querverweislisten) ausreichend sein.

ANMERKUNG 2 Ziel der Black-Box-Tests ist es, das dynamische Verhalten unter realen Funktionsbedingungen zu überprüfen und Ausfälle aufzudecken, um so die Funktionsspezifikation zu erfüllen und die Nützlichkeit und Robustheit zu beurteilen. Grey-Box-Tests ähneln den Black-Box-Tests; sie überwachen allerdings (den) relevante(n) Prüfparameter innerhalb des Softwaremoduls.

In Abhängigkeit vom PL_r sollten die Prüfungen Folgendes umfassen:

— Black-Box- oder Grey-Box-Tests des Funktionsverhaltens und der Leistungsfähigkeit (z. B. Zeitverhalten);

— zusätzliche erweiterte Prüffälle, die auf Grenzwertanalysen beruhen, empfohlen für PL d oder PL e;

— I/O-Prüfungen, um sicherzustellen, dass die sicherheitsbezogenen Eingangs- und Ausgangssignale richtig verwendet werden; und

— Prüffälle, die Fehler simulieren, die vorher analytisch bestimmt werden, zusammen mit der erwarteten Reaktion, um die Eignung der softwarebasierten Maßnahmen zur Beherrschung von Ausfällen zu bewerten.

ANMERKUNG 3 Siehe Abschnitt N.2 für ein Beispiel.

Einzelne Softwarefunktionen, die bereits validiert wurden, brauchen nicht erneut validiert zu werden. Wenn mehrere derartige Sicherheitsfunktionsblöcke für ein bestimmtes Projekt kombiniert werden, muss allerdings die sich daraus ergebende gesamte Sicherheitsfunktion validiert werden.

Die Maßnahmen zur Softwareimplementierung und -konfiguration und für das Änderungsmanagement nach Abschnitt 7, die vom zu erzielenden PL abhängig sind, müssen hinsichtlich ihrer geeigneten Umsetzung untersucht werden.

Sollte die sicherheitsbezogene Software nachträglich verändert werden, muss sie in angemessenem Umfang erneut validiert werden.

10.6.4 Validierung der Kombination von Teilsystemen

Wenn die Sicherheitsfunktion durch zwei oder mehr Teilsysteme ausgeführt wird, muss diese Kombination — durch Analyse und durch Prüfung — validiert werden, um zu bestätigen, dass diese Kombination die für den Entwurf festgelegte Sicherheitsintegrität erreicht. Vorhandene aufgezeichnete Validierungsergebnisse von Teilsystemen können dabei berücksichtigt werden. Die folgenden Validierungsschritte müssen durchgeführt werden:

— Überprüfung der Entwurfsdokumente, die die gesamte(n) Sicherheitsfunktion(en) beschreiben;

— Überprüfung, ob der Gesamt-PL der Teilsystemkombination auf der Grundlage des PL jedes einzelnen Teilsystems richtig bewertet wurde (nach 6.2);

— Berücksichtigung von Schnittstelleneigenschaften, z. B. Spannung, Strom, Druck, Datenformat der Signale, Signalpegel;

— Analyse von Ausfällen in Abhängigkeit von der Kombination/Integration, z. B. durch FMEA;

— Prüfung der Kombination von Teilsystemen;

— Prüfungen durch Fehlereinspeisung für redundante Systeme in Abhängigkeit von der Kombination/Integration.

10.6.5 Gesamtvalidierung der Sicherheitsintegrität

Die folgenden Schritte müssen durchgeführt werden:

— Überprüfung/Verifizierung der korrekten Bewertung des PL auf der Grundlage von PFH und PL/SIL der Teilsysteme (siehe 7.2);

— Überprüfung/Verifizierung der korrekten Bewertung des PL auf der Grundlage der Kategorie, von DC_{avg} und $MTTF_D$, CCF und Maßnahmen gegen systematische Ausfälle;

— Überprüfung/Verifizierung, ob der vom SRP/CS erreichte PL den PL_r erfüllt, der in der SRS für die Maschine festgelegt ist: $PL \geq PL_r$.

10.7 Validierung der Umgebungsanforderungen

Die im Entwurf des SRP/CS festgelegte Leistungsfähigkeit muss im Hinblick auf die für die Steuerung festgelegten Umgebungsbedingungen validiert werden.

Die Validierung muss durch Analyse und durch Prüfung erfolgen. Der Umfang der Analyse und der Prüfung hängt von den sicherheitsbezogenen Teilen, dem System, in das sie eingebaut werden, der verwendeten Technologie und den zu validierenden Umgebungsbedingungen ab. Durch die Verwendung von Daten zur Betriebszuverlässigkeit des Systems oder seiner Bauteile oder die Bestätigung der Übereinstimmung mit einschlägigen Umweltnormen (z. B. Abdichtung gegen Wasser, Schutz gegen Vibration) kann dieser Validierungsprozess unterstützt werden.

Soweit zutreffend, muss die Validierung Folgendes betreffen:

— zu erwartende mechanische Spannungen durch Stoß, Vibrationen, Eindringen von Verunreinigungen;

— mechanische Haltbarkeit;

— elektrische Nennwerte und Energieversorgung;

— klimatische Bedingungen (Temperatur und Luftfeuchte); und

— EMI (Störfestigkeit).

Wenn Prüfungen erforderlich sind, um die Einhaltung der Umgebungsanforderungen festzustellen, sind die in den zutreffenden Normen beschriebenen Verfahren zu befolgen, soweit dies für die Anwendung erforderlich ist.

Nach Abschluss der Validierung durch Prüfung müssen die Sicherheitsfunktionen weiterhin mit den Spezifikationen der Sicherheitsanforderungen übereinstimmen oder das SRP/CS muss (ein) Ausgangssignal(e) für einen sicheren Zustand erzeugen.

10.8 Aufzeichnung der Validierung

Die Validierung durch Analyse und Prüfung muss aufgezeichnet werden. Die Aufzeichnung muss den Validierungsprozess für jede Sicherheitsanforderung belegen. Querverweisungen auf frühere Validierungsaufzeichnungen dürfen eingefügt werden, sofern sie ordnungsgemäß gekennzeichnet werden.

Für jedes sicherheitsbezogene Teil, das einen Schritt des Validierungsprozesses nicht bestanden hat, muss in der Validierungsaufzeichnung beschrieben werden, welche Schritte der Analyse/Prüfung für die Validierung nicht bestanden wurden. Es muss sichergestellt sein, dass alle SRP/CS nach einer Änderung erfolgreich neu validiert wurden.

10.9 Validierung der Instandhaltungsanforderungen

Der Validierungsprozess muss belegen, dass die Vorkehrungen für die Instandhaltungsanforderungen umgesetzt wurden.

Die Validierung der Instandhaltungsanforderungen muss Folgendes betreffen, soweit zutreffend:

a) eine Überprüfung der Benutzerinformationen, um zu bestätigen, dass:

   1) Instandhaltungsanleitungen vollständig [einschließlich der Verfahren, der erforderlichen Werkzeuge, Inspektionshäufigkeit, Zeitabstände für das verschleißbedingte Austauschen von Bauteilen (T_{10D}) usw.] und verständlich sind;

   2) soweit zutreffend, es Bestimmungen gibt, dass die Instandhaltungsaufgaben nur von geschultem Instandhaltungspersonal durchzuführen sind;

b) eine Überprüfung, ob Maßnahmen für eine verbesserte Wartungsfreundlichkeit (z. B. Bereitstellung von Diagnoseinstrumenten zur Unterstützung der Fehlersuche und der Reparatur) umgesetzt wurden.

Außerdem müssen die folgenden Maßnahmen berücksichtigt werden, sofern sie vorhanden sind:

— Maßnahmen zur Fehlervermeidung während der Instandhaltung (z. B. Erkennen von falschen Eingangsdaten mithilfe von Plausibilitätsprüfungen);

— Maßnahmen zum Vermeiden von Änderungen (z. B. Passwort-Schutz zum Verhindern des Zugriffs auf das Programm durch unbefugte Personen).

11 Wartungsfreundlichkeit von SRP/CS

Eine vorbeugende Instandhaltung oder Instandsetzung kann notwendig sein, um das festgelegte Leistungsverhalten des SRP/CS aufrechtzuerhalten.

ANMERKUNG Eine Überschreitung der festgelegten Lebensdauer oder des Prüfintervalls kann zur Verschlechterung der Sicherheit oder zu einer Gefährdungssituation führen.

Folgende Faktoren müssen berücksichtigt werden, um die Instandhaltung des SRP/CS zu ermöglichen:

— Zugänglichkeit unter Berücksichtigung der Umgebung und der menschlichen Körpermaße, einschließlich der Maße der Arbeitsbekleidung und der verwendeten Werkzeuge;

— leichte Handhabung unter Berücksichtigung der ergonomischen Fähigkeiten;

— Begrenzung der Anzahl von besonderen Werkzeugen und Ausrüstungen, soweit möglich;

— Anzeigen, dass eine Instandhaltung notwendig ist (z. B. verstärkte Schwingungen), idealerweise mit einer automatischen Erzeugung von Warnsignalen (z. B. Aufzeichnung der Lebensdauer, Selbsttest, Überwachung von Prozessparametern);

— erforderliche Beleuchtungsstärken.

12 Technische Dokumentation

Bei der Gestaltung eines SRP/CS nach diesem Dokument müssen mindestens die folgenden Informationen für interne Zwecke dokumentiert werden, die für das sicherheitsbezogene Teil maßgebend sind:

a) SRS (siehe 5.2.1);

b) die genauen Punkte, wo das/die sicherheitsbezogene(n) Teil(e) beginnt/beginnen und endet/enden;

c) Zerlegung in Teilsysteme (siehe 5.2.2), sofern zutreffend;

d) die Umgebungsbedingungen (z. B. elektromagnetische Störfestigkeit, Temperatur, Vibration);

e) erreichter Performance Level und PFH-Wert;

f) ausgewählte Kategorie bzw. Kategorien (kann für zuvor validierte Teilsysteme nicht zutreffend sein);

g) Parameter, die für die Zuverlässigkeit ($MTTF_D$, DC, CCF und T_{10D}) sowie für die Gebrauchsdauer maßgebend sind;

h) die Maßnahmen gegen systematischen Ausfall;

i) die verwendete Technologie oder die verwendeten Technologien;

j) die berücksichtigten sicherheitsbezogenen Fehler;

k) die Begründungen für Fehlerausschlüsse (siehe 6.1.10.3 und alle Anhänge in ISO 13849-2:2012);

l) die Softwaredokumentation, sofern zutreffend;

m) Maßnahmen gegen vernünftigerweise vorhersehbare Fehlanwendung;

n) sicherheitsbezogenes Blockdiagramm;

o) sachdienliche Dokumentation des Entwurfs, der Prüfung, Verifizierung und Validierung, soweit zutreffend.

ANMERKUNG Die Entwurfsdokumentation ist im Allgemeinen für interne Zwecke des Herstellers oder für den Austausch technischer Informationen zwischen Unterauftragnehmern (z. B. externen Systementwicklern, Zertifizierungsstellen) und dem Hersteller vorgesehen. Die Entwurfsdokumentation ist auch notwendig, um die gesetzlichen Dokumentationspflichten zu erfüllen. Die Entwurfsdokumentation muss nicht an den Anwender der Maschine weitergegeben werden, aber Teile davon sind relevant, um angemessene Benutzerinformationen zu erstellen (siehe Abschnitt 13).

13 Benutzerinformation

13.1 Allgemeines

Die Benutzerinformationen des SRP/CS müssen ISO 20607:2019 oder IEC/IEEE 82079-1:2019 entsprechen und die maßgebenden Anleitungen für die entsprechenden Zielgruppen enthalten. Die Lebenszyklusphasen der Maschinen, an denen ein SRP/CS beteiligt ist, müssen in diesen Benutzerinformationen behandelt werden.

13.2 Informationen für die Integration des SRP/CS

Die Informationen, die für die sichere Integration des SRP/CS wichtig sind, müssen dem Integrator bereitgestellt werden. Dies muss Folgendes einschließen, ist aber nicht darauf begrenzt:

a) die Grenzen der ausgewählten sicherheitsbezogenen Teile eines SRP/CS (z. B. Umgebungsbedingungen wie elektromagnetische Störfestigkeit, Temperatur, Schwingungen) und geeignete Informationen, um die fortlaufende Rechtfertigung der Fehlerausschlüsse sicherzustellen, z. B. in Bezug auf Änderung, Instandhaltung und Reparatur;

b) eindeutige Beschreibungen der Schnittstellen mit dem SRP/CS und den Schutzeinrichtungen;

c) Ansprechzeit, soweit maßgebend (nach ISO 13855:2010);

d) Betriebsgrenzen (z. B. Anforderungshäufigkeit);

e) Anzeigen und Alarme;

f) Überbrückungsfunktion (en: muting) und zeitweiliges Aufheben der Sicherheitsfunktionen;

g) Steuerungsarten und Rückstellung;

h) Instandhaltung (siehe Abschnitt 11);

i) Checklisten für die Instandhaltung;

j) Zugang zu und Austausch von Teilen des SRP/CS;

k) Mittel zur leichten und sicheren Fehlersuche;

l) Prüfintervalle, soweit maßgebend;

m) Gebrauchsdauer.

ANMERKUNG Der Integrator kann ein Hersteller, ein Monteur, ein Ingenieurbüro oder der Benutzer sein.

Spezifische Informationen zu jeder Sicherheitsfunktion über die Kategorien und den Performance Level müssen wie folgt bereitgestellt werden (siehe 5.3):

— die Kategorien der Teilsysteme, die das SRP/CS bilden (möglicherweise nicht zutreffend für zuvor validierte Teilsysteme);

— der Performance Level a, b, c, d oder e;

— der PFH-Wert für das SRP/CS bezogen auf die Sicherheitsfunktion, sofern für das/die Teilsystem(e) maßgebend.

13.3 Informationen für den Benutzer

Die Informationen, die für die ordnungsgemäßen Verwendung des SRP/CS wichtig sind, müssen dem Maschinenanwender (z. B. der Bedienperson) angegeben werden.

Dazu können unter anderem die relevanten Aspekte von 13.1 und 13.2 zählen. Maßgebende Informationen über die Prüfung der Sicherheitsfunktionen müssen ebenfalls bereitgestellt werden. Der Konstrukteur des SRP/CS muss die Benutzerinformationen bereitstellen, welche die notwendigen Instandhaltungsaufgaben für das SRP/CS beschreiben.

Informationen über die Instandhaltung können beispielsweise folgende Aufgaben und Anwendungsmöglichkeiten umfassen:

a) Einrichten;

b) Einlernen (Teachen)/Programmieren;

c) Umrüsten;

d) Reinigung;

e) präventive Instandhaltung;

f) Fehler behebende Instandhaltung;

g) Fehlersuche/Fehlerbehandlung;

h) Art und Häufigkeit der Inspektionen von Sicherheitsfunktionen;

i) Anweisungen zu Instandhaltungsarbeiten, die entweder Fachwissen oder besondere Fähigkeiten oder beides erfordern und deshalb nur von qualifiziertem Personal (z. B. Instandhaltungspersonal, Spezialisten) durchgeführt werden sollten;

j) Anweisungen zu Instandhaltungsarbeiten (z. B. Auswechseln von Teilen), die keine besonderen Fähigkeiten erfordern und die demzufolge von Maschinenanwendern (z. B. Bedienpersonen) durchgeführt werden dürfen. Das Instandhaltungspersonal sollte darauf hingewiesen werden, welche Teile für die Sicherheit entscheidend sind und nur durch Originalteile oder Teile, die die gleichen Anforderungen an die Sicherheit erfüllen, ersetzt werden dürfen;

k) Beherrschung gefährlicher Energie (manuelle Maßnahmen/andere Mittel) Anleitung, Zeichen und Einrichtungen;

l) Zeichnungen/Diagramme, die dem Instandhaltungspersonal die Durchführung seiner Arbeiten ermöglichen (besonders Aufgaben zur Fehlerfindung, um Bedingungen zu beseitigen, welche den Fehler verursacht haben);

m) Informationen über den Austausch von Bauteilen bei oder vor Ablauf des T_M-[N1]Zeitraums (für pneumatische, mechanische und elektromechanische Bauteile siehe auch C.4.2).

ANMERKUNG 1 Für weitere Informationen siehe ISO 20607:2019 und IEC 60204-1:2016+AMD1:2021, 17.2 f).

Erfordert eine Instandhaltungstätigkeit die Instandsetzung oder Änderung eines SRP/CS, muss eine Neuvalidierung einschließlich eines Funktionstests durchgeführt werden.

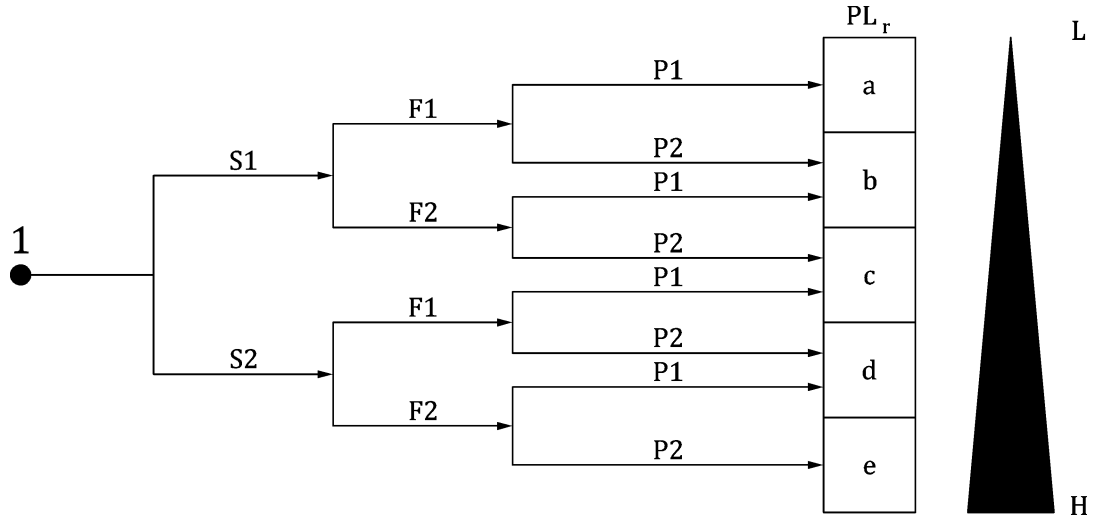
ANMERKUNG 2 Die entsprechenden Tätigkeiten bei der Neuvalidierung würden vom Ausmaß der Unterschiede zwischen dem ursprünglichen und dem ersetzenden Bauteil abhängen.

N1 Nationale Fußnote: T_M ist die korrekte Schreibweise. In der englischen Originalfassung liegt ein Schreibfehler vor.

Anhang A
(informativ)

Leitlinien für die Bestimmung des erforderlichen Performance Levels (PL_r)

A.1 Allgemeines



Legende
1 Startpunkt zur Bewertung des Beitrags der Sicherheitsfunktion zur Risikominderung
L niedriger Beitrag zur Risikominderung
H hoher Beitrag zur Risikominderung
PL_r erforderlicher Performance Level

Risikoparameter:
S Schwere der Verletzung
S1 leicht (üblicherweise reversible Verletzung)
S2 ernst (üblicherweise irreversible Verletzung oder Tod)
F Häufigkeit und/oder Dauer der Gefährdungsexposition
F1 selten bis weniger häufig und/oder die Zeit der Gefährdungsexposition ist kurz
F2 häufig bis ständig und/oder die Zeit der Gefährdungsexposition ist lang
P Möglichkeit zur Vermeidung oder Begrenzung eines Schadens
P1 möglich unter bestimmten Bedingungen
P2 kaum möglich

Bild A.1 — Diagramm für die Bestimmung des PL_r einer Sicherheitsfunktion

Bild A.1 enthält Leitlinien für die Bestimmung des sicherheitsbezogenen PL_r einer Sicherheitsfunktion. Das Diagramm sollte für jede Sicherheitsfunktion betrachtet werden.

A.2 Auswahl des erforderlichen Performance Levels (PL_r)

Anhang A beschäftigt sich mit dem Beitrag zur Risikominderung, der durch das betrachtete SRP/CS erzielt wird. Das in diesem Abschnitt beschriebene Verfahren basiert auf der Abschätzung der Risikoparameter (die naturgemäß teilweise subjektiv ist, wie bei jedem anderen Verfahren zur Risikoeinschätzung). Daher dient dieses Verfahren lediglich als eine Leitlinie für Maschinenkonstrukteure und Normungsgremien, um den PL_r für jede Sicherheitsfunktion, die von einem SRP/CS auszuführen ist, abzuschätzen.

Dieses Verfahren zur Abschätzung des PL_r ist nicht verbindlich. Es handelt sich hierbei um einen generischen Ansatz, der von einer Eintrittswahrscheinlichkeit eines Gefährdungsereignisses im ungünstigsten Fall ausgeht (die Eintrittswahrscheinlichkeit beträgt 100 %). In Fällen, in denen die Eintrittswahrscheinlichkeit als gering beurteilt werden kann (diese Entscheidung sollte begründet und dokumentiert werden), ist eine Herabstufung um einen Performance Level möglich, andernfalls beträgt die Eintrittswahrscheinlichkeit 100 %. Andere geeignete Verfahren zur Risikoeinschätzung für bestimmte Arten von Maschinen können angewendet werden und Erfahrungen im erfolgreichen Umgang mit ähnlichen Maschinen/Gefährdungen sollten bei der Abschätzung des PL_r berücksichtigt werden. Daher kann der in einer Typ-C-Norm geforderte PL von dem PL abweichen, der durch den generischen Ansatz in Bild A.1 ermittelt wird.

Das Diagramm in Bild A.1 basiert auf der Situation vor Festlegung der beabsichtigten Sicherheitsfunktion (siehe auch ISO/TR 22100-2:2013). Eine Risikominderung durch technische Maßnahmen unabhängig von der Steuerung (z. B. mechanischer Schutz) oder zusätzliche Sicherheitsfunktionen müssen bei der Bestimmung des PL_r der beabsichtigten Sicherheitsfunktion berücksichtigt werden; in diesem Fall wird der Startpunkt in Bild A.1 nach der Umsetzung dieser Maßnahmen gewählt (siehe auch Bild 3).

Die Parameter, die zur Bestimmung des PL_r verwendet werden, sind:

— Schwere der Verletzung (S);

— Häufigkeit und/oder Dauer der Gefährdungsexposition (F);

— Möglichkeit zur Vermeidung oder Begrenzung des Schadens (P).

Diese Parameter können kombiniert werden, wie in Bild A.1 gezeigt, um eine Abstufung des Beitrags zur erforderlichen Risikominderung von niedrig bis hoch zu erhalten.

A.3 Anleitung für die Auswahl der Parameter S, F und P zur Einschätzung des Risikos

A.3.1 Schwere der Verletzung S1 und S2

Bei der Einschätzung des Risikos werden nur leichte Verletzungen oder ernste Verletzungen berücksichtigt.

Um eine Entscheidung treffen zu können, sollten die üblichen Folgen der Unfälle und die üblichen Heilungsprozesse bei der Bestimmung von S1 und S2 in Betracht gezogen werden. Zum Beispiel würden Quetschungen und/oder Fleischwunden ohne Komplikationen als S1 klassifiziert, wohingegen eine Amputation oder Tod S2 sein würde.

ANMERKUNG Für Leitlinien zur Bewertung von ernsten oder leichten Verletzungen siehe auch ISO/TR 14121-2.

A.3.2 Häufigkeit und/oder Dauer der Gefährdungsexposition F1 und F2

Ein allgemeingültiger Zeitraum, wann Parameter F1 oder wann F2 auszuwählen ist, kann nicht festgelegt werden. Die folgende Erklärung kann allerdings den Entscheidungsfindungsprozess erleichtern.

F2 sollte ausgewählt werden, wenn eine Person häufig oder ständig einer Gefährdung ausgesetzt ist. Dabei ist es unerheblich, ob dieselbe oder nacheinander unterschiedliche Personen der Gefährdung ausgesetzt werden, z. B. bei der Verwendung von Aufzügen. Der Parameter der Häufigkeit sollte nach der Häufigkeit und Dauer des Zugangs zur Gefährdung ausgewählt werden.

Wo die Anforderung der Sicherheitsfunktion dem Konstrukteur bekannt ist, kann die Häufigkeit und Dauer dieser Anforderung anstelle der Häufigkeit und Dauer des Zugangs zur Gefährdung gewählt werden. In diesem Dokument wird angenommen, dass die Häufigkeit einer Anforderung der Sicherheitsfunktion mehr als einmal je Jahr beträgt.

Die Dauer der Gefährdungsexposition sollte auf der Grundlage eines Durchschnittswerts bewertet werden, der im Verhältnis zur Gesamtzeit gesehen werden kann, über die die Einrichtung verwendet wird. Ist es z. B. notwendig, im zyklischen Betrieb regelmäßig zwischen die Werkzeuge der Maschine zu greifen, um Werkstücke zuzuführen oder zu bewegen, dann sollte F2 gewählt werden.

Liegt keine andere Begründung vor, sollte F2 gewählt werden, wenn die Häufigkeit höher als einmal je 15 Minuten ist.

F1 darf gewählt werden, wenn die gesamte Expositionsdauer 1/20 der gesamten Betriebsdauer nicht überschreitet und die Häufigkeit nicht höher als einmal je 15 Minuten ist.

BEISPIEL An einer Maschine mit einer Gesamtbetriebszeit von 8 h je Tag ist eine Person einmal je Stunde für 2 min exponiert, wenn sie Werkstücke wechselt (geschätzter Durchschnittswert), so dass die kumulierte Expositionszeit 16 min im Verhältnis zu 8 min × 60 min beträgt, was 1/30 ergibt. Da die Häufigkeit 1/h beträgt, kann F1 gewählt werden.

A.3.3 Möglichkeit zur Vermeidung oder Begrenzung eines Schadens, P1 und P2

Es ist wichtig, zu wissen, ob ein Gefährdungsereignis erkannt und vermieden werden kann, bevor es einen Schaden verursachen kann. Zum Beispiel kann die Gefährdungsexposition direkt durch ihre physikalischen Eigenschaften identifiziert, oder nur durch technische Mittel erkannt werden, z. B. durch Anzeigen. Andere wichtige Aspekte, die die Auswahl des Parameters P beeinflussen, sind z. B.:

a) Geschwindigkeit, mit der die Gefährdungssituation auftritt (z. B. schnell oder langsam);

b) Möglichkeiten, um sich der Gefährdungssituation zu entziehen (z. B. Vermeidung durch Entkommen);

c) praktische Erfahrungen mit der Sicherheit in Bezug zum Prozess;

d) Betrieb durch geschulte und geeignete Bedienpersonen;

e) Betrieb mit oder ohne Beaufsichtigung.

Wenn ein Gefährdungsereignis eintritt, sollte P1 nur dann ausgewählt werden, wenn eine realistische Möglichkeit besteht, dass ein Schaden vermieden oder deutlich verringert wird. Anderenfalls sollte P2 gewählt werden.

Eine Möglichkeit zur Bestimmung von P liegt im folgenden Ansatz:

— Bestimmen des Buchstabens jedes Faktors aus Tabelle A.1, der die spezifische Anwendung widerspiegelt (nur eine Auswahl für jeden Faktor ist möglich);

— Ermitteln der Häufigkeit des gewählten Buchstabens „A“, „B“ und „C“;

— Bestimmen des zugehörigen Werts für den Parameter P in Tabelle A.2.

Tabelle A.1 — Bestimmen des Parameters P auf der Grundlage von fünf Faktoren

Faktor	C	B	A
1. Benutzung der Maschine durch		Laie[a]	Fachkraft[a]
2. Geschwindigkeit des Teils der Maschine, der ein Gefährdungsereignis erzeugen kann (je nach spezifischer Maschine und der Zeit zum Entkommen aus einer Gefährdungssituation oder zum Vermeiden einer Gefährdungssituation)	Ereignis mit hoher Geschwindigkeit z. B. > 1 000 mm/s, Zeit bis zur Gefährdung < 1 s und/oder keine oder zu wenig Zeit zum Entkommen	Ereignis mit mittlerer Geschwindigkeit z. B. 251 mm/s bis 1 000 mm/s, Zeit bis zur Gefährdung ≥ 1 s und < 3 s und/oder begrenzte Zeit zum Entkommen	Ereignis mit niedriger oder sehr niedriger Geschwindigkeit z. B. < 250 mm/s, Zeit bis zur Gefährdung ≥ 3 s und/oder ausreichend Zeit zum Entkommen
3. Räumliche Möglichkeit, sich der Gefährdung zu entziehen	nicht möglich	Gelegentlich/selten möglich möglich in < 50 % der Fälle	leicht möglich möglich in ≥ 50 % der Fälle
4. Möglichkeit der Erkennung/Wahrnehmung der Gefährdung (z. B. heiße/kalte Oberfläche, nicht-ionisierende Strahlung usw.)	nicht möglich z. B. Notwendigkeit von Geräten, Unfähigkeit die Gefährdung mit den Sinnen wahrzunehmen, Verhindern der Wahrnehmung aufgrund von Umgebungsbedingungen	gelegentliches/seltenes Erkennen der Gefährdung möglich in < 50 % der Fälle	einfaches Erkennen der Gefährdung möglich in ≥ 50 % der Fälle
5. Komplexität der Tätigkeiten (menschliche Interaktion in Bezug auf die Anzahl der Handlungen und/oder die für diese Handlungen zur Verfügung stehende Zeit)		mittlere bis hohe Komplexität z. B. Fehlersuche, Verwendung einer Steuerung mit Tippbetrieb zum Errichten eines Teils der Maschine	geringe Komplexität z. B. Einstellen der Werkstückklemmen, oder sehr geringe Komplexität/ oder keine Interaktion z. B. Einlegen eines Werkstücks in die Maschine
ANMERKUNG Alle Zahlenwerte in dieser Tabelle sind rein informativ und können in Typ-C-Normen oder in Zusammenhang mit der spezifischen Maschinenanwendung abweichen.			
[a] 3.1.55 definiert eine „Fachkraft“ als Person, die eine Ausbildung und Schulung sowie jahrelange Praxis im Sinne dieses Dokuments vereint.			

Tabelle A.2 — Auswahl von Parameter P1 bzw. P2

Gesamtbewertung		Parameter „P“
Ein oder mehr „C“		P2
Kein „C“, drei oder mehr „B“		P2
Kein „C“, zwei „B“, der Rest „A“		P1 oder P2, je nach spezifischer Situation
Kein „C“, ein oder kein „B“, der Rest „A“		P1

Der Ansatz auf der Grundlage von Tabelle A.1 und Tabelle A.2 sollte immer mit der folgenden Grundabsicht verwendet werden: P1 sollte nur dann gewählt werden, wenn eine realistische Möglichkeit besteht, den Schaden zu vermeiden oder seine Auswirkungen erheblich zu verringern; andernfalls sollte P2 gewählt werden.

A.4 Überlagerte Gefährdungen

Bei Anwendung dieses Dokuments werden alle Gefährdungen als spezifische Gefährdungen oder Gefährdungssituationen betrachtet. Jede Gefährdung kann deshalb separat bewertet werden.

Wenn es offenbar eine Kombination von direkt miteinander verbundenen Gefährdungen gibt, die immer gleichzeitig eintreten, dann sollten sie zur Risikoeinschätzung zusammengefasst werden.

Die Festlegung, ob Gefährdungen einzeln oder zusammengefasst betrachtet werden sollten, sollte während der Risikobeurteilung der Maschine getroffen werden.

BEISPIEL 1 Ein kontinuierlich arbeitender Schweißroboter kann gleichzeitig verschiedene Gefährdungssituationen erzeugen, wie z. B. Quetschen durch Bewegen und Verbrennen durch den Schweißvorgang. Diese können als eine Kombination von direkt miteinander verbundenen Gefährdungen betrachtet werden.

BEISPIEL 2 Für eine Roboterzelle, in der einzelne Roboter arbeiten, können für die Zellenbereiche, in denen nur ein Roboter gleichzeitig eine Gefährdung erzeugen kann, die Roboter getrennt betrachtet werden.

BEISPIEL 3 Infolge der Risikobeurteilung kann es ausreichend sein, für einen Rundschalttisch mit Klemmvorrichtungen jede Klemmvorrichtung einzeln zu betrachten.

Anhang B
(informativ)

Blockmethode und sicherheitsbezogenes Blockdiagramm

B.1 Blockmethode

Der vereinfachte Ansatz erfordert eine blockorientierte logische Darstellung des Teilsystems. Das Teilsystem sollte in eine kleine Anzahl von Blöcken wie folgt zerlegt werden:

a) die Blöcke sollten die logischen Einheiten des Teilsystems abbilden, die sich auf die Ausführung der Sicherheitsfunktion beziehen;

b) unterschiedliche Kanäle, die die Teilfunktion ausführen, sollten in separaten Blöcken dargestellt werden;

c) wenn ein Block nicht mehr in der Lage ist, seine Funktion zu leisten, sollte die Ausführung der Teilfunktion durch die Blöcke des anderen Kanals nicht betroffen werden;

d) jeder Kanal darf aus einem oder mehreren Blöcken bestehen — drei Blöcke je Kanal der vorgesehenen Architekturen, Eingang, Logik und Ausgang, ist keine bindende Anzahl, sondern nur ein Beispiel der logischen Aufteilung innerhalb jedes Kanals;

e) jede Hardwareeinheit des Teilsystems sollte nur einem Block zugeordnet werden; dies erlaubt die Berechnung der $MTTF_D$ des Blocks, basierend auf der $MTTF_D$ der Hardwareeinheiten, die zu diesem Block gehören (z. B. durch die FMEA oder das „Parts-Count“-Verfahren, siehe D.1).

B.2 Sicherheitsbezogenes Blockdiagramm

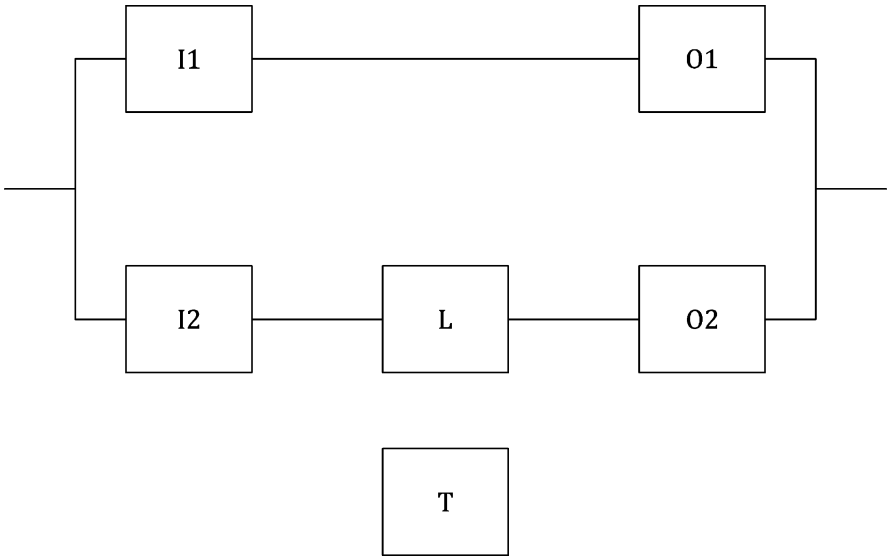
Die durch die Blockmethode definierten Blöcke dürfen verwendet werden, um die logische Struktur des Teilsystems in einem sicherheitsbezogenen Blockdiagramm graphisch darzustellen. Für eine solche graphische Darstellung können folgende Leitlinien angewendet werden:

— der Ausfall eines Blocks in einer Serienschaltung von Blöcken führt zu einem Ausfall des gesamten Kanals (z. B. wenn eine Hardwareeinheit in einem Kanal des Teilsystems gefahrbringend ausfällt, kann der gesamte Kanal seine Teilfunktion nicht weiter ausführen);

— nur der gefahrbringende Ausfall aller Kanäle in einer Parallelschaltung führt zum Verlust der Teilfunktion (z. B. eine durch mehrere Kanäle ausgeführte Teilfunktion wird so lange ausgeführt, wie mindestens ein Kanal keinen Ausfall hat); CCFs können diesen Zustand herbeiführen (siehe 6.1.6 sowie Anhang F und Anhang G);

— Blöcke, die nur zu Testzwecken für SRP/CS der Kategorie 3 oder Kategorie 4 verwendet werden und die die Ausführung der Teilfunktion nicht beeinflussen, wenn sie gefahrbringend ausfallen, dürfen von Blöcken in den verschiedenen Kanälen getrennt werden.

Siehe Bild B.1 als Beispiel.



Legende

I1, I2	Eingabegeräte, z. B. Sensor
L	Logik
O1, O2	Ausgabegeräte, z. B. Hauptschütz
T	Prüfeinrichtung
I1 und O1	bilden den ersten Kanal (Serienschaltung)
I2, L und O2	bilden den zweiten Kanal (Serienschaltung); mit beiden Kanälen wird die Teilfunktion redundant ausgeführt (Parallelschaltung)
T	nur zu Prüfzwecken verwendet

Bild B.1 — Beispiel für ein sicherheitsbezogenes Blockdiagramm

Anhang C
(informativ)

Berechnung oder Bewertung von $MTTF_D$-Werten für einzelne Bauteile

C.1 Allgemeines

Dieser Anhang gibt verschiedene Verfahren an, um $MTTF_D$-Werte für einzelne Bauteile zu berechnen oder zu bewerten: das Verfahren in C.2 basiert auf der Anwendung guter ingenieurmäßiger Praxis für unterschiedliche Arten von Bauteilen; das Verfahren in C.3 ist anwendbar auf hydraulische Bauteile; das Verfahren in C.4 liefert ein Mittel zur Berechnung der $MTTF_D$ für pneumatische, mechanische und elektromechanische Bauteile anhand von B_{10}-Werten (siehe C.4.1); C.5 führt $MTTF_D$-Werte für elektrische Bauteile auf.

C.2 Verfahren guter ingenieurmäßiger Praxis

Wenn die folgenden Merkmale erfüllt sind, kann der $MTTF_D$- oder B_{10D}-Wert für ein Bauteil nach Tabelle C.1 abgeschätzt werden.

a) Die Bauteile werden nach den grundlegenden und bewährten Sicherheitsprinzipien von ISO 13849-2:2012 und der für die Konstruktion des Bauteils zutreffenden Norm (siehe Tabelle C.1) hergestellt.

   ANMERKUNG Diese Information kann im Datenblatt des Bauteilherstellers gefunden werden.

b) Der Bauteilhersteller legt die geeigneten Anwendungs- und Betriebsbedingungen für den SRP/CS-Konstrukteur fest.

c) Der Entwurf des SRP/CS erfüllt die grundlegenden und bewährten Sicherheitsprinzipien von ISO 13849-2:2012 für die Ausführung und den Betrieb des Bauteils.

Tabelle C.1 — Internationale Normen, die sich mit $MTTF_D$ oder B_{10D} für Bauteile befassen

	Grundlegende und bewährte Sicherheitsprinzipien nach ISO 13849-2:2012	**Zutreffende Normen**	**Typische Werte: $MTTF_D$ (Jahre), B_{10D} (Zyklen)**
Mechanische Bauteile	Tabelle A.1 und Tabelle A.2	—	$MTTF_D = 150$
Hydraulische Bauteile mit $n_{op} \geq 1\,000\,000$ Zyklen je Jahr[a]	Tabelle C.1 und Tabelle C.2	ISO 4413	$MTTF_D = 150$
Hydraulische Bauteile mit 1 000 000 Zyklen je Jahr $> n_{op} \geq 500\,000$ Zyklen je Jahr[a]	Tabelle C.1 und Tabelle C.2	ISO 4413	$MTTF_D = 300$
Hydraulische Bauteile mit 500 000 Zyklen je Jahr $> n_{op} \geq 250\,000$ Zyklen je Jahr[a]	Tabelle C.1 und Tabelle C.2	ISO 4413	$MTTF_D = 600$
Hydraulische Bauteile mit $n_{op} < 250\,000$ Zyklen je Jahr[a]	Tabelle C.1 und Tabelle C.2	ISO 4413	$MTTF_D = 1\,200$
Pneumatische Bauteile	Tabelle B.1 und Tabelle B.2	ISO 4414	$B_{10D} = 20\,000\,000$[c]

	Grundlegende und bewährte Sicherheitsprinzipien nach ISO 13849-2:2012	Zutreffende Normen	Typische Werte: $MTTF_D$ (Jahre), B_{10D} (Zyklen)
Relais und Hilfsschütze mit geringer Last	Tabelle D.1 und Tabelle D.2	IEC 61810-3 Normenreihe IEC 60947	$B_{10D} = 20\,000\,000$
Relais und Hilfsschütze mit nominaler Last	Tabelle D.1 und Tabelle D.2	IEC 61810-3 Normenreihe IEC 60947	$B_{10D} = 400\,000$
Näherungsschalter mit geringer Last	Tabelle D.1 und Tabelle D.2	Normenreihe IEC 60947 ISO 14119	$B_{10D} = 20\,000\,000$
Näherungsschalter mit nominaler Last	Tabelle D.1 und Tabelle D.2	Normenreihe IEC 60947 ISO 14119	$B_{10D} = 400\,000$
Schütze mit geringer Last[d]	Tabelle D.1 und Tabelle D.2	Normenreihe IEC 60947	$B_{10D} = 20\,000\,000$
Schütze mit nominaler Last[d]	Tabelle D.1 und Tabelle D.2	Normenreihe IEC 60947	$B_{10D} = 1\,300\,000$
Positionsschalter[b]	Tabelle D.1 und Tabelle D.2	Normenreihe IEC 60947 ISO 14119	$B_{10D} = 20\,000\,000$
Positionsschalter (mit separatem Betätiger, Zuhaltung)[b]	Tabelle D.1 und Tabelle D.2	Normenreihe IEC 60947 ISO 14119	$B_{10D} = 2\,000\,000$
Not-Halt-Geräte[b]	Tabelle D.1 und Tabelle D.2	Normenreihe IEC 60947 ISO 13850	$B_{10D} = 100\,000$
Drucktaster (z. B. Zustimmungsschalter)[b]	Tabelle D.1 und Tabelle D.2	Normenreihe IEC 60947	$B_{10D} = 100\,000$

ANMERKUNG 1 Für die Definition und Verwendung von B_{10D} siehe C.4.

ANMERKUNG 2 B_{10D} wird abgeschätzt als zweimal B_{10} (50 % gefahrbringender Ausfall), wenn keine anderen Angaben vorliegen (z. B. Produktnorm).

ANMERKUNG 3 Not-Halt-Geräte nach IEC 60947-5-5 und ISO 13850 sowie Zustimmungsschalter nach IEC 60947-5-8 können als Teilsystem der Kategorie 1 oder Kategorie 3/4 abgeschätzt werden, je nach Anzahl der elektrischen Ausgangskontakte und der Fehlererkennung im nachgeordneten Teilsystem. Jedes Kontaktelement (einschließlich der mechanischen Betätigung) kann als ein Kanal mit entsprechendem B_{10D}-Wert betrachtet werden. Für Zustimmungsschalter nach IEC 60947-5-8 umfasst dies die Öffnungsfunktion durch Durchdrücken oder Loslassen. In einigen Fällen ist es möglich, dass der Maschinenhersteller einen Fehlerausschluss nach ISO 13849-2:2012, Tabelle D.8, unter Berücksichtigung der jeweiligen Anwendungs- und Umgebungsbedingungen des Geräts anwenden kann.

ANMERKUNG 4 Das Reduzieren von Schaltzyklen kann zu einer erhöhten Wahrscheinlichkeit des Festsetzens der Schaltelemente in Steuerventilen führen (siehe ISO 4413).

ANMERKUNG 5 Die $MTTF_D$ für mechanische Bauteile bezieht sich ausschließlich auf mechanisch bewegliche Bauteile/Elemente (nicht auf das Gehäuse).

[a] Die Berechnung des B_{10D}-Werts für hydraulische Bauteile ist nicht als Rückwärtsberechnung aus Standard-$MTTF_D$-Werten zulässig.

[b] Falls Fehlerausschluss für Zwangsöffnung möglich ist.

[c] In der Regel kann dieser Wert für die meisten pneumatischen Bauteile angenommen werden. In Abhängigkeit von der Anwendung und dem Typ, z. B. Absperrventil, kann dieser Wert jedoch deutlich kleiner sein.

[d] „Nominale Last“ oder „geringe Last“ sollte die Sicherheitsprinzipien berücksichtigen, die in ISO 13849-2:2012 beschrieben sind, wie Überdimensionierung des Strom-Nennwerts. „Geringe Last“ bedeutet z. B. 20 %.

C.3 Hydraulische Bauteile

Wenn die folgenden Merkmale erfüllt sind, kann der $MTTF_D$-Wert für ein einzelnes hydraulisches Bauteil, z. B. Ventil, mit 150 Jahren abgeschätzt werden. Wenn die mittlere Anzahl der jährlichen Betätigungen (n_{op}) unter 1 000 000 Zyklen je Jahr beträgt, kann der $MTTF_D$-Wert höher abgeschätzt werden als in Tabelle C.1 angegeben:

a) Die hydraulischen Bauteile werden nach den grundlegenden und bewährten Sicherheitsprinzipien von ISO 13849-2:2012, Tabelle C.1 und Tabelle C.2, und der relevanten Norm (siehe Tabelle C.1) für die Konstruktion des hydraulischen Bauteils hergestellt (Bestätigung im Datenblatt des Bauteils).

b) Der Hersteller des hydraulischen Bauteils legt die geeigneten Anwendungs- und Betriebsbedingungen für den SRP/CS-Konstrukteur fest. Der SRP/CS-Konstrukteur sollte seiner Verantwortung entsprechend Angaben darüber machen, dass er die grundlegenden und bewährten Sicherheitsprinzipien nach ISO 13849-2:2012, Tabelle C.1 und Tabelle C.2, für die Ausführung und den Betrieb des hydraulischen Bauteils erfüllt.

Wenn a) oder b) nicht erfüllt wird, sollte der $MTTF_D$-Wert für das einzelne hydraulische Bauteil durch den Hersteller angegeben werden. Anstatt einen festen Wert für $MTTF_D$ zu verwenden, wie vorstehend beschrieben, ist es zulässig, das B_{10D}-Verfahren für die $MTTF_D$-Ermittlung von pneumatischen, mechanischen und elektromechanischen Bauteilen auch für hydraulische Bauteile zu verwenden, wenn der Hersteller die Daten liefern kann, z. B. B_{10}, B_{10D}, T_{10}, T_{10D}.

C.4 $MTTF_D$ von pneumatischen, mechanischen und elektromechanischen Bauteilen

C.4.1 Allgemeines

Es kann schwierig sein, für pneumatische, mechanische und elektromechanische Bauteile (Pneumatikventile, Relais, Schütze, Positionsschalter, Nocken von Positionsschaltern) die $MTTF_D$ für Bauteile, die in Jahren angegeben und in diesem Dokument gefordert wird, zu berechnen. Meistens gibt der Hersteller solcher Art von Bauteilen nur die Schalthäufigkeit an, bis 10 % der Bauteile ausfallen (B_{10}) oder gefahrbringend ausfallen (B_{10D}). Dieser Abschnitt gibt ein Verfahren an, um die $MTTF_D$ für Bauteile zu berechnen, unter Verwendung von B_{10} oder T (Lebensdauer), die vom Hersteller angegeben werden, mit engem Bezug zur anwendungsbezogenen Schalthäufigkeit.

Wenn alle folgenden Merkmale erfüllt sind, kann der $MTTF_D$-Wert für ein einzelnes pneumatisches, elektromechanisches oder mechanisches Bauteil nach C.4.2 abgeschätzt werden.

a) Die Bauteile wurden unter Verwendung grundlegender Sicherheitsprinzipien nach ISO 13849-2:2012, Tabelle A.1, Tabelle B.1 oder Tabelle D.1, entworfen und hergestellt.

   ANMERKUNG 1 Diese Information kann im Datenblatt des Bauteilherstellers gefunden werden.

b) Die Bauteile, die in Kategorie 1, 2, 3 oder 4 verwendet werden sollen, wurden unter Verwendung bewährter Sicherheitsprinzipien nach ISO 13849-2:2012, Tabelle A.2, Tabelle B.2 oder Tabelle D.2, entworfen und hergestellt.

   ANMERKUNG 2 Diese Information kann im Datenblatt des Bauteilherstellers gefunden werden.

c) Der Bauteilhersteller legt die geeigneten Anwendungs- und Betriebsbedingungen für den SRP/CS-Konstrukteur fest. Der SRP/CS-Konstrukteur sollte seiner Verantwortung entsprechend Angaben darüber machen, dass er die grundlegenden Sicherheitsprinzipien nach ISO 13849-2:2012, Tabelle A.1, Tabelle B.1 oder Tabelle D.1, für die Ausführung und den Betrieb des Bauteils erfüllt. Für Kategorie 1, 2, 3 oder 4 sollte der Anwender über seine Verantwortung informiert werden, die bewährten Sicherheitsprinzipien nach ISO 13849-2:2012, Tabelle A.1, Tabelle B.2 oder Tabelle D.2, für die Ausführung und den Betrieb des Bauteils zu erfüllen.

C.4.2 Berechnung der $MTTF_D$ für Bauteile aus B_{10D}

Die mittlere Anzahl von Zyklen, bis 10 % der Bauteile gefahrbringend ausgefallen sind (B_{10D})[1], sollte durch den Hersteller des Bauteils in Übereinstimmung mit den entsprechenden Produktnormen für die Prüfung bestimmt werden (z. B. der Normenreihe ISO 19973, IEC 60947-4-1, IEC 60947-5-1, IEC 60947-5-5, IEC 61810-2-1). Die gefahrbringenden Ausfallarten der Bauteile sollten definiert werden, z. B. Verkleben in einer Endposition oder Änderung der Schaltzeiten. Mit B_{10D} und n_{op}, der mittleren Anzahl jährlicher Betätigungen, kann die $MTTF_D$ für Bauteile wie folgt berechnet werden:

$$MTTF_D = \frac{B_{10D}}{0{,}1 \times n_{op}} \tag{C.1}$$

Dabei ist

$$n_{op} = \frac{d_{op} \times h_{op} \times 3\,600\ \text{s/h}}{t_{Zyklus}} \tag{C.2}$$

Dabei ist

h_{op} die mittlere Betriebszeit, in Stunden je Tag;

d_{op} die mittlere Betriebszeit, in Tagen je Jahr;

t_{Zyklus} ist die mittlere Betriebszeit zwischen dem Beginn zweier aufeinanderfolgender Zyklen des Bauteils (z. B. Schalten eines Ventils), in Sekunden je Zyklus.

Die Betriebslebensdauer des Bauteils ist begrenzt auf T_{10D}, die mittlere Dauer bis 10 % der Bauteile gefahrbringend ausfallen:

$$T_{10D} = \frac{B_{10D}}{n_{op}} \tag{C.3}$$

Falls kein Wert für B_{10D} vom Bauteilhersteller angegeben ist, ist es zulässig, den B_{10D}-Wert mithilfe von Gleichung (C.4) zu ermitteln:

$$B_{10D} = \frac{B_{10}}{RDF} \tag{C.4}$$

Falls der vom Bauteilhersteller angegebene Anteil gefahrbringender Ausfälle (RDF[N2]) auf unter 50 % geschätzt wird, dann ist der T_{10D}-Wert auf $T_{10} \times 2$ begrenzt.

Wenn der T_{10D}-Wert für ein Bauteil unter der Gebrauchsdauer (20 Jahre oder kürzer) liegt, informiert der Hersteller, der für die Integration des SRP/CS verantwortlich ist, welches die Sicherheitsfunktion ausführt, den Nutzer darüber, das Bauteil bei Erreichen von T_{10D} oder vor Ablauf des T_{10D}-Zeitraums auszutauschen. Durch die Begrenzung der Verwendung des Bauteils auf T_{10D} wird die Aufrechterhaltung des erwarteten Performance Levels der Sicherheitsfunktion ermöglicht.

---

1 Wenn der Anteil gefahrbringender Ausfälle (RDF) von B_{10} nicht angegeben ist (z. B. durch den Bauteilhersteller), können 50 % von B_{10} verwendet werden; deshalb wird $B_{10D} = 2\ B_{10}$ empfohlen.

N2 Nationale Fußnote: Schreibfehler in der Originalfassung hier sowie in Gleichung (C.4), dort steht „R_{DF}“ statt „RDF“ (s. Begriff 3.1.34).

C.4.3 Erläuterung der Gleichungen

Die Verfahren der Zuverlässigkeit in diesem Dokument setzen voraus, dass die Ausfälle von Bauteilen exponentiell über die Zeit verteilt sind: $F_{\mathrm{D}}(t) = 1 - e^{-\lambda_{\mathrm{D}} t}$. Für nicht-elektronische Bauteile ist eine Weibull-Verteilung wahrscheinlicher; wenn aber die Gebrauchsdauer der Bauteile auf die mittlere Dauer bis 10 % der Bauteile gefahrbringend ausfallen ($T_{10\mathrm{D}}$) begrenzt wird, kann eine konstante gefahrbringende Ausfallrate (λ_{D}) während dieser Gebrauchsdauer wie folgt abgeschätzt werden:

$$\lambda_{\mathrm{D}} = \frac{0{,}1}{T_{10\mathrm{D}}} = \frac{0{,}1 \times n_{\mathrm{op}}}{B_{10\mathrm{D}}} \tag{C.5}$$

Gleichung (C.6) berücksichtigt, dass mit einer konstanten Ausfallrate 10 % der Bauteile in der angenommenen Anwendung nach $T_{10\mathrm{D}}$ [Jahren] ausfallen, entsprechend nach $B_{10\mathrm{D}}$ [Zyklen]. Um exakt zu sein:

$$F_{\mathrm{D}}(t) = 1 - e^{-\lambda_{\mathrm{D}} T_{10\mathrm{D}}} = 10\,\%\ \text{ d. h. }\ \lambda_{\mathrm{D}} = -\frac{\ln(0{,}9)}{T_{10\mathrm{D}}} = \frac{0{,}105\,63}{T_{10\mathrm{D}}} \approx \frac{0{,}1}{T_{10\mathrm{D}}} \tag{C.6}$$

mit $\mathrm{MTTF_D} = 1/\lambda_{\mathrm{D}}$ für eine exponentielle Verteilung ergibt Folgendes:

$$\mathrm{MTTF_D} = \frac{T_{10\mathrm{D}}}{0{,}1} = \frac{B_{10\mathrm{D}}}{0{,}1 \times n_{\mathrm{op}}} \tag{C.7}$$

ANMERKUNG Alle Variablen, die in den Gleichungen verwendet werden, sind physikalische Größen, angegeben als das Produkt aus numerischem Wert und Maßeinheit. Die ordnungsgemäße Anwendung von Gleichung (C.5), Gleichung (C.6) und $\mathrm{MTTF_D} = 1/\lambda_{\mathrm{D}}$ kann die Umwandlung von „Jahren“ in „Stunden“ erfordern, wobei für 1 Jahr = 8 760 h verwendet werden.

C.4.4 Beispiel

Für ein Pneumatikventil gibt ein Hersteller eine mittlere Anzahl von 60 Millionen Zyklen als $B_{10\mathrm{D}}$ an. Das Ventil wird an zwei Schichten je Tag an 220 Arbeitstagen je Jahr verwendet. Die mittlere Zeit zwischen dem Beginn zweier aufeinanderfolgender Zyklen der Ventile wird auf 5 s geschätzt. Damit ergeben sich die folgenden Werte:

— d_{op} von 220 d je Jahr;

— h_{op} von 16 h je Tag;

— t_{Zyklus} von 5 s je Zyklus;

— $B_{10\mathrm{D}}$ von 60 000 000 Zyklen.

Mit diesen Eingangsdaten können die folgenden Werte berechnet werden:

$$n_{\mathrm{op}} = \frac{220 \times 16 \times 3\,600}{5\mathrm{s}} = 2{,}53 \times 10^6\ \text{Zyklen/Jahr} \tag{C.8}$$

$$T_{10\mathrm{D}} = \frac{60 \times 10^6}{2{,}53 \times 10^6} = 23{,}7\ \text{Jahre} \tag{C.9}$$

$$\mathrm{MTTF_D} = \frac{23{,}7}{0{,}1} = 237\ \text{Jahre} \tag{C.10}$$

Aus dieser Berechnung ergibt sich für das Bauteil eine $\mathrm{MTTF_D}$ von „hoch“ nach Tabelle C.5. Diese Annahmen gelten nur für eine eingeschränkte Gebrauchsdauer von 23,7 Jahren für das Ventil.

C.5 $MTTF_D$-Daten für elektronische Bauteile

C.5.1 Allgemeines

Tabelle C.2 bis Tabelle C.7 zeigen einige typische Durchschnittswerte der $MTTF_D$ für elektronische Bauteile. Die Daten wurden aus der Datenbank der Reihe SN 29500 entnommen. Alle Daten sind allgemeiner Art. Verschiedene Datenbanken sind verfügbar (siehe die unvollständige Liste in den Literaturhinweisen), die $MTTF_D$-Werte für verschiedene elektronische Bauteile enthalten. Wenn der Konstrukteur eines SRP/CS andere verlässliche spezifische Daten für die verwendeten Bauteile besitzt, dann wird die Verwendung dieser spezifischen Daten anstelle der anderen Daten empfohlen.

Die in Tabelle C.2 bis Tabelle C.7 angegebenen Werte sind gültig für eine Umgebungstemperatur von 40 °C, Nennbelastung für Strom und Spannung. Für die $MTTF_D$ sollte ein Korrekturfaktor angewendet werden, wenn die elektronischen Bauteile außerhalb der angegebenen Werte für Temperatur oder Last arbeiten (siehe auch die Normenreihe SN 29500).

In der MTTF-Spalte der Tabellen sind die Werte aus der Normenreihe SN 29500 für allgemeine Bauteile für alle möglichen Ausfallarten gezeigt, die nicht notwendigerweise gefahrbringende Ausfälle sind. In der $MTTF_D$-Spalte wird üblicherweise angenommen, dass nicht alle Ausfallarten zu gefahrbringenden Ausfällen führen. Dies hängt hauptsächlich von der Anwendung ab. Ein genauer Weg der Bestimmung der „typischen“ $MTTF_D$ für Bauteile ist die Durchführung einer FMEA. Einige Bauteile, z. B. als Schalter verwendete Transistoren, können Kurzschlüsse oder Unterbrechungen als Ausfall haben. Nur eine der beiden Arten kann gefahrbringend sein; deshalb nimmt die Spalte „Bemerkungen“ nur 50 % als gefahrbringende Ausfälle an, was bedeutet, dass die $MTTF_D$ für Bauteile das Doppelte des angegebenen MTTF-Werts ist.

C.5.2 Halbleiter

Siehe Tabelle C.2 und Tabelle C.3.

Tabelle C.2 — Transistoren (als Schalter verwendet)

Transistor	**Beispiel**	**MTTF für Bauteile** Jahre	**$MTTF_D$ für Bauteile** Jahre **Typisch**	**Bemerkungen**
Bipolar	TO18, TO92, SOT23	38 052	76 104	50 % gefahrbringende Ausfälle
Bipolar, niedrige Leistung	TO5, TO39	5 708	11 416	50 % gefahrbringende Ausfälle
Bipolar, Leistung	TO3, TO220, D-Pack	1 903	3 806	50 % gefahrbringende Ausfälle
FET	J-MOS	22 831	45 662	50 % gefahrbringende Ausfälle
MOS, Leistung	TO3, TO220, D-Pack	1 903	3 806	50 % gefahrbringende Ausfälle

Tabelle C.3 — Dioden, Leistungshalbleiter und integrierte Schaltungen

Diode	Beispiel	MTTF für Bauteile Jahre	$MTTF_D$ für Bauteile Jahre **Typisch**	Bemerkungen
Allgemeine Anwendung	—	114 155	228 311	50 % gefahrbringende Ausfälle
Entstörgerät	—	16 308	32 616	50 % gefahrbringende Ausfälle
Zenerdiode $P_{tot} < 1$ W	—	114 155	228 311	50 % gefahrbringende Ausfälle
Gleichrichterdioden	—	57 078	114 155	50 % gefahrbringende Ausfälle
Gleichrichter-brücken	—	11 415	22 831	50 % gefahrbringende Ausfälle
Thyristoren	—	2 283	4 566	50 % gefahrbringende Ausfälle
Triacs, Diacs	—	1 522	3 044	50 % gefahrbringende Ausfälle
Integrierte Schaltungen (programmierbar und nicht programmierbar)	Anwendung der Herstellerdaten			50 % gefahrbringende Ausfälle

C.5.3 Passive Bauteile

Siehe Tabelle C.4 bis Tabelle C.7.

Tabelle C.4 — Kondensatoren

Kondensator	Beispiel	MTTF für Bauteile Jahre	$MTTF_D$ für Bauteile Jahre **Typisch**	Bemerkungen
Standard, keine Leistung	KS, KP, KC, KT, MKT, MKC, MKP, MKU, MP, MKV	57 078	114 155	50 % gefahrbringende Ausfälle
Keramik	—	22 831	45 662	50 % gefahrbringende Ausfälle
Aluminiumelektrolyt	flüssiger Elektrolyt	22 831	45 662	50 % gefahrbringende Ausfälle
Aluminiumelektrolyt	fester Elektrolyt	38 052	76 104	50 % gefahrbringende Ausfälle
Tantalelektrolyt	flüssiger Elektrolyt	11 415	22 831	50 % gefahrbringende Ausfälle
Tantalelektrolyt	fester Elektrolyt	114 155	228 311	50 % gefahrbringende Ausfälle

Tabelle C.5 — Widerstände

Widerstand	Beispiel	MTTF für Bauteile Jahre	$MTTF_D$ für Bauteile Jahre **Typisch**	Bemerkungen
Kohleschicht	—	114 155	228 311	50 % gefahrbringende Ausfälle
Metallfilm	—	570 776	1 141 552	50 % gefahrbringende Ausfälle
Metalloxid und gewendelt	—	22 831	45 662	50 % gefahrbringende Ausfälle
Variabel	—	3 805	7 610	50 % gefahrbringende Ausfälle

Tabelle C.6 — Induktivitäten

Induktivität	Beispiel	MTTF für Bauteile Jahre	$MTTF_D$ für Bauteile Jahre Typisch	Bemerkungen
Für MC-Anwendung	—	38 052	76 104	50 % gefahrbringende Ausfälle
Niederfrequenz-Induktivitäten und Transformatoren	—	22 831	45 662	50 % gefahrbringende Ausfälle
Leistungstransformatoren und Transformatoren für Schaltanwendungen und Netzteile	—	11 415	22 831	50 % gefahrbringende Ausfälle

Tabelle C.7 — Optokoppler

Optokoppler	Beispiel	MTTF für Bauteile Jahre	$MTTF_D$ für Bauteile Jahre Typisch	Bemerkungen
Bipolar-Ausgang	SFH 610	7 610	15 220	50 % gefahrbringende Ausfälle
FET-Ausgang	LH 1056	2 854	5 708	50 % gefahrbringende Ausfälle

Anhang D
(informativ)

Vereinfachtes Verfahren zur Abschätzung der $MTTF_D$ für jeden Kanal

D.1 Parts-Count-Verfahren

Das „Parts-Count-Verfahren“ hilft bei der getrennten Abschätzung der $MTTF_D$ für jeden Kanal. Die $MTTF_D$-Werte aller einzelnen Bauteile eines Kanals werden für diese Berechnung verwendet.

ANMERKUNG Das Parts-Count-Verfahren ist eine Näherung, deren Abweichung immer zur sicheren Seite geht.

Die allgemeine Gleichung (D.1) ist:

$$\frac{1}{\mathrm{MTTF_D}} = \sum_{i=1}^{N} \frac{1}{\mathrm{MTTF_{Di}}} = \sum_{j=1}^{\tilde{N}} \frac{n_j}{\mathrm{MTTF_{Dj}}} \tag{D.1}$$

Dabei ist

$MTTF_D$ die mittlere Dauer bis zum gefahrbringenden Ausfall des kompletten Kanals;

$MTTF_{D\,i}$, $MTTF_{D\,j}$ die $MTTF_D$ jedes Bauteils, das einen Beitrag zur Teilfunktion leistet. Die erste Summe wird über jedes Bauteil getrennt gebildet; die zweite Summe ist gleichwertig aber vereinfacht, wobei alle n_j-identischen Bauteile mit der gleichen $MTTF_{D\,j}$ zusammengefasst werden.

Das in Tabelle D.1 angegebene Beispiel ergibt eine $MTTF_D$ des Kanals von 22,4 Jahren, was „mittel“ nach 6.1.4, Tabelle 6, entspricht.

Tabelle D.1 — Beispiel für die Teileliste einer Platine

j	**Bauteil**	**Anzahl** n_j	$MTTF_{D\,j}$ Jahre	$1/MTTF_{D\,j}$ 1/Jahr	$n_j/MTTF_{D\,j}$ 1/Jahr
1	Transistoren, bipolar, Kleinleistung (siehe Tabelle C.2)	2	11 416	0,000 087 6	0,000 175 2
2	Widerstand, Kohleschicht (siehe Tabelle C.5)	5	228 311	0,000 004 4	0,000 021 9
3	Kondensator, Standard, keine Leistung (siehe Tabelle C.4)	4	114 155	0,000 008 8	0,000 035 0
4	Relais, vom Hersteller angegebener Wert (B_{10D} = 20 000 000 Zyklen, n_{op} = 633 600 Zyklen je Jahr)	4	315,7	0,003 167 6	0,012 670 3
5	Schütz, vom Hersteller angegebener Wert (B_{10D} = 2 000 000 Zyklen, n_{op} = 633 600 Zyklen je Jahr)	1	31,6	0,031 645 6	0,031 645 6
$\sum(n_j/MTTF_{D\,j})$					0,044 548 0
$MTTF_D = 1/\sum(n_j/MTTF_{D\,j})$ [Jahre]					22,4

ANMERKUNG 1 Dieses Verfahren basiert auf der Annahme, dass ein gefahrbringender Ausfall irgendeines Bauteils (Abschätzung des ungünstigsten Falls) im Kanal zu einem gefahrbringenden Ausfall des Kanals führt. Die $MTTF_D$-Berechnung nach Tabelle D.1 basiert auf dieser Annahme.

ANMERKUNG 2 In diesem Beispiel kommt der Haupteinfluss vom Schütz. Die gewählten Werte für $MTTF_D$ und B_{10D} in diesem Beispiel basieren auf Anhang C. Für das Beispiel werden $d_{op} = 220$ Tage/Jahr, $h_{op} = 8$ h/Tag und $t_{Zyklus} = 10$ s/Zyklus angenommen; das ergibt $n_{op} = 633\,600$ Zyklen/Jahr. Im Allgemeinen führt die Wahl der Herstellerdaten für $MTTF_D$ und B_{10D} zu viel besseren Ergebnissen, also zu einer höheren $MTTF_D$ des Kanals.

ANMERKUNG 3 Wenn die MTTR (mittlere Zeit bis zur Wiederherstellung, en: mean time to restoration) als vernachlässigbar angesehen werden kann, kann die MTTF gleich der MTBF angenommen werden.

ANMERKUNG 4 Liegen ausschließlich MTBF-Werte vor, kann eine Umwandlung in $MTTF_D$-Werte mithilfe von $MTTF_D \approx 2$*MTBF erfolgen.

D.2 $MTTF_D$ für unterschiedliche Kanäle, Symmetrisierung der $MTTF_D$ für jeden Kanal

Die vorgesehenen Architekturen in 6.1.3.2 gehen davon aus, dass für unterschiedliche Kanäle in einem redundanten SRP/CS die Werte für $MTTF_D$ für jeden Kanal gleich sind. Dieser Wert je Kanal sollte die Eingangsgröße für Bild 12 sein.

Wenn die $MTTF_D$ der Kanäle unterschiedlich sind, gibt es zwei Möglichkeiten:

— als eine Annahme für den ungünstigsten Fall sollte der kleinere Wert in Betracht gezogen werden;

— Gleichung (D.2) kann zur Abschätzung eines Ersatzwerts für $MTTF_D$ für jeden Kanal verwendet werden:

$$MTTF_D = \frac{2}{3}\left[MTTF_{D\,C1} + MTTF_{D\,C2} - \frac{1}{\frac{1}{MTTF_{D\,C1}} + \frac{1}{MTTF_{D\,C2}}}\right] \quad \text{(D.2)}$$

Dabei sind

$MTTF_{D\,C1}$ und $MTTF_{D\,C2}$ die Werte für zwei unterschiedliche redundante Kanäle, die jeweils auf einen Höchstwert von 100 Jahren (Kategorien B, 1, 2 und 3) oder von 2 500 Jahren (Kategorie 4) begrenzt sind.

BEISPIEL Ein Kanal hat eine $MTTF_{D\,C1} = 3$ Jahre, der andere Kanal hat eine $MTTF_{D\,C2} = 100$ Jahre, dann ist das Ergebnis $MTTF_D = 66$ Jahre für jeden Kanal. Das bedeutet, dass ein redundantes System mit einer $MTTF_D$ von 100 Jahren in einem Kanal und einer $MTTF_D$ von 3 Jahren im anderen Kanal gleichwertig ist zu einem System mit einer $MTTF_D$ von 66 Jahren in jedem Kanal.

Ein redundantes System mit zwei Kanälen und unterschiedlichen $MTTF_D$-Werten jedes Kanals kann unter Verwendung der obigen Gleichung durch ein redundantes System mit identischen $MTTF_D$-Werten für jeden Kanal ersetzt werden. Dieses Verfahren ist notwendig, um Bild 12 richtig anwenden zu können.

ANMERKUNG Dieses Verfahren setzt unabhängige, parallele Kanäle voraus.

Anhang E
(informativ)

Abschätzungen des Diagnosedeckungsgrades (DC) für Funktionen und Teilsysteme

E.1 Beispiele für den Diagnosedeckungsgrad (DC)

Siehe Tabelle E.1.

Tabelle E.1 — Abschätzungen des Diagnosedeckungsgrades (DC)

Maßnahme	DC[a b]
Eingabeeinheit	
Zyklischer Testimpuls durch dynamischen Wechsel der Eingangssignale	90 %
Plausibilitätsprüfung, z. B. Verwendung der Schließer- und Öffnerkontakte von zwangsgeführten Relais	99 %
Kreuzvergleich von Eingangssignalen ohne dynamischen Test	prozentualer Anteil, der in Abhängigkeit von der jeweiligen Anwendung festzulegen ist, z. B. abhängig davon, wie oft ein Signalwechsel durch die Anwendung erfolgt (siehe ANMERKUNG 4)
Kreuzvergleich von Eingangssignalen mit dynamischem Test, wenn Kurzschlüsse nicht bemerkt werden können (bei Mehrfach-Ein-/Ausgängen)	90 %
Kreuzvergleich von Eingangssignalen und Zwischenergebnissen in der Logik (L) und zeitliche und logische Programmlaufüberwachung und Erkennung statischer Ausfälle und Kurzschlüsse (bei Mehrfach-Ein-/Ausgängen)	99 %
Indirekte Überwachung (z. B. Überwachung durch Druckschalter, elektrische Positionsüberwachung von Aktuatoren der Maschine)	90 % bis 99 %, abhängig von der Anwendung (siehe ANMERKUNG 2)
Direkte Überwachung (z. B. elektrische Positionsüberwachung der Steuerventile, Überwachung elektromechanischer Einheiten durch Zwangsführung)	99 %
Fehlererkennung durch den Prozess	prozentualer Anteil, der in Abhängigkeit von der jeweiligen Anwendung festzulegen ist; diese Maßnahme ist allein nicht ausreichend für den erforderlichen Performance Level (PL_r) e (siehe ANMERKUNG 2, ANMERKUNG 3 und ANMERKUNG 5)
Überwachung einiger Merkmale des Sensors (Ansprechzeit, der Bereich analoger Signale, z. B. elektrischer Widerstand, Kapazität)	60 %
Logik	
Indirekte Überwachung (z. B. Überwachung durch Druckschalter, elektrische Positionsüberwachung von Aktuatoren der Maschine, Plausibilitätsprüfung von Endergebnissen)	90 % bis 99 %, abhängig von der Anwendung (siehe ANMERKUNG 2)
Direkte Überwachung (z. B. elektrische Stellungsüberwachung der Steuerventile, Überwachung elektromechanischer Einheiten durch Zwangsführung, Plausibilitätsprüfung von Zwischenergebnissen)	99 %

Maßnahme	DC[a b]
Einfache zeitliche Programmlaufüberwachung (z. B. Zeitglied als Watchdog, mit Triggersignalen im Programm der Logik)	60 %
Zeitliche und logische Programmlaufüberwachung durch den Watchdog, wobei die Testeinrichtung Plausibilitätsprüfungen des Verhaltens der Logik durchführt	90 %
Selbsttest bei Anlauf, um verborgene Fehler in Teilen der Logik zu finden (z. B. Programm- und Datenspeicher, Eingangs-/Ausgangsanschlüsse, Schnittstellen)	60 % bis 90 % (siehe ANMERKUNG 2)
Testung des Ansprechvermögens der Überwachungseinrichtung (z. B. Watchdog) durch den Hauptkanal nach Anlauf, oder wann immer die Sicherheitsfunktion angefordert wird, oder wann immer ein externes Signal dies durch eine Eingangseinrichtung anfordert	90 %
Dynamische Prinzipien (alle Bauteile der Logik erfordern eine Zustandsänderung EIN-AUS-EIN, wenn die Sicherheitsfunktion angefordert wird), z. B. Verriegelungsschaltungen in Relaistechnik	99 %
Invarianter Speicher: Signatur einfacher Wortbreite (einfache Busbreite)	90 %
Invarianter Speicher: Signatur doppelter Wortbreite (doppelte Busbreite)	99 %
Variabler Speicher: RAM-Test durch Verwendung redundanter Daten, z. B. Flags, Merker, Konstanten, Timer und Kreuzvergleich dieser Daten	60 %
Variabler Speicher: Test der Lesbarkeit und der Beschreibbarkeit der verwendeten Speicherzellen	60 %
Variabler Speicher: RAM-Selbsttest (z. B. „Galpat“ oder „Abraham“) oder Doppel-RAM mit Hardware- oder Software-Vergleich und Lese-/Schreibtest.	99 %
Verarbeitungseinheit: Selbsttest durch Software (siehe IEC 61508-7:2010, A.3)	60 % bis 90 % (siehe ANMERKUNG 2)
Verarbeitungseinheit: codierte Verarbeitung (siehe IEC 61508-7:2010, A.3)	90 % bis 99 % (siehe ANMERKUNG 2)
Fehlererkennung durch den Prozess	prozentualer Anteil, der in Abhängigkeit von der jeweiligen Anwendung festzulegen ist; diese Maßnahme ist allein nicht ausreichend für den erforderlichen Performance Level (PL_r) e (siehe ANMERKUNG 2, ANMERKUNG 3 und ANMERKUNG 5)
Ausgabeeinheit	
Überwachung der Ausgänge durch einen Kanal ohne dynamischen Test	prozentualer Anteil, der in Abhängigkeit von der jeweiligen Anwendung festzulegen ist, z. B. abhängig davon, wie oft ein Signalwechsel durch die Anwendung erfolgt (siehe ANMERKUNG 4)
Kreuzvergleich von Ausgangssignalen ohne dynamischen Test	prozentualer Anteil, der in Abhängigkeit von der jeweiligen Anwendung festzulegen ist, z. B. abhängig davon, wie oft ein Signalwechsel durch die Anwendung erfolgt (siehe ANMERKUNG 4)
Kreuzvergleich von Ausgangssignalen mit dynamischem Test, ohne Erkennung von Kurzschlüssen (bei mehreren Ein-/Ausgängen)	90 %

Maßnahme	DC[a b]
Kreuzvergleich von Ausgangssignalen und Zwischenergebnissen in der Logik (L) und zeitliche und logische Softwareüberwachung des Programmablaufs und Erkennen statischer Fehler und Kurzschlüsse (bei mehreren Ein-/Ausgängen)	99 %
Redundanter Abschaltpfad mit Überwachung der Ausgänge durch die Logik und Testeinrichtung, siehe Beispiel in ISO 13849-2:2012, Anhang E	99 %
Indirekte Überwachung (z. B. Überwachung durch Druckschalter, elektrische Positionsüberwachung von Aktuatoren der Maschine)	90 % bis 99 %, abhängig von der Anwendung (siehe ANMERKUNG 2)
Fehlererkennung durch den Prozess	prozentualer Anteil, der in Abhängigkeit von der jeweiligen Anwendung festzulegen ist; diese Maßnahme ist allein nicht ausreichend für den erforderlichen Performance Level (PL_r) e (siehe ANMERKUNG 2, ANMERKUNG 3 und ANMERKUNG 5)
Direkte Überwachung (z. B. elektrische Positionsüberwachung der Steuerventile, Überwachung elektromechanischer Einheiten durch Zwangsführung)	99 %

ANMERKUNG 1 Für weitere Abschätzungen des DC siehe z. B. IEC 61508-2:2010, Tabelle A.2 bis Tabelle A.14.

ANMERKUNG 2 Für Maßnahmen, für die ein Bereich des DC angegeben ist (z. B. Fehlererkennung durch den Prozess), kann der richtige DC-Wert durch Betrachten aller gefahrbringenden Ausfälle bestimmt werden und anschließend die Entscheidung getroffen werden, welcher von ihnen durch die DC-Maßnahme erkannt wird. Im Zweifelsfall sollte eine FMEA die Grundlage für die Abschätzung des DC darstellen.

ANMERKUNG 3 Für die DC-Maßnahme „Fehlererkennung durch den Prozess“ können die Anforderungsrate der Sicherheitsfunktion (r_d) und die Prozessdiagnoserate (Testrate) (r_t) zusammen berücksichtigt werden, mit einer Begrenzung des effektiven DC der geprüften Komponente:

a) $r_t/r_d > 1$ DC ist auf 60 % begrenzt;

b) $r_t/r_d > 10$ DC ist auf 90 % begrenzt;

c) $r_t/r_d > 100$ DC ist auf 99 % begrenzt.

ANMERKUNG 4 Für die DC-Maßnahme „Kreuzvergleich von Ein- oder Ausgängen ohne dynamischen Test“ kann der Effekt der Testrate unter Verwendung der folgenden Einschränkungen für den effektiven DC der getesteten Komponente berücksichtigt werden:

Für Kategorie 3 und Kategorie 4:

r_t < 1/Jahr DC beträgt 0 %;

r_t ≥ 1/Jahr DC ist auf 90 % begrenzt;

r_t ≥ 1/Monat DC ist auf 99 % begrenzt.

ANMERKUNG 5 Wenn die DC-Maßnahme „Fehlererkennung durch den Prozess“ mit anderen DC-Maßnahmen nach Anhang E kombiniert wird, kann diese Maßnahme immer noch in die DC-Schätzung des Blocks einbezogen werden, selbst für PL_r e.

[a] DC-Maßnahmen können kombiniert werden, um einen höheren DC zu erzielen.

[b] Wenn ein mittlerer oder hoher DC für die Logik gefordert wird, ist mindestens eine Maßnahme für jeden variablen Speicher, invarianten Speicher und jede Verarbeitungseinheit mit mindestens je 60 % zu wählen. Andere Maßnahmen als die in dieser Tabelle aufgeführten können verwendet werden.

Für die Anwendung von Tabelle E.1 gelten die folgenden hinweisenden Beispiele.

BEISPIEL 1 ISO 13849-2:2012, Anhang E, zeigt ein vollständiges (sehr detailliertes) Beispiel für die Validierung des Fehlerverhaltens und der Diagnosemaßnahmen einer automatischen Montageanlage.

ANMERKUNG ISO/TR 24119 beschreibt mithilfe von Tabellen ein anwendungsbezogenes Schritt-für-Schritt-Verfahren zur Bewertung des DC für Reihenschaltungen von Verriegelungseinrichtungen mit potenzialfreien Kontakten.

BEISPIEL 2 Die DC-Maßnahme „Fehlererkennung durch den Prozess“ kann nur angewendet werden, wenn das sicherheitsbezogene Bauteil am Fertigungsprozess beteiligt ist, z. B. wenn eine normale SPS oder normale Sensoren für die Fertigung eines Werkstücks benutzt werden, und als Teil von einem von zwei Kanälen, die die Sicherheitsfunktion ausführen, fungieren. Das geeignete DC-Level hängt von der Überschneidung der gewöhnlich verwendeten Ressourcen (Logik, Eingänge/Ausgänge) ab. Wenn beispielsweise alle Fehler eines Drehreglers in einer Druckmaschine zu stark sichtbaren Fehlern im Druckvorgang führen, kann der DC für diesen Sensor, der zur Überwachung einer sicher begrenzten Geschwindigkeit genutzt wird, zwischen 90 % und 99 % abgeschätzt werden.

E.2 Abschätzung des durchschnittlichen Diagnosedeckungsgrads

In vielen Systemen können mehrere Maßnahmen zur Fehlererkennung angewendet werden. Diese Maßnahmen können unterschiedliche Teile des SRP/CS testen und unterschiedliche DC besitzen. Zur Abschätzung des PL nach 6.1.8 und Bild 12 ist nur ein durchschnittlicher DC für das gesamte SRP/CS, das die Sicherheitsfunktion ausführt, anwendbar.

Der DC darf bestimmt werden als das Verhältnis zwischen der Ausfallrate von erkannten gefahrbringenden Ausfällen und der Ausfallrate aller gefahrbringenden Ausfälle. Nach dieser Definition wird der durchschnittliche Diagnosedeckungsgrad DC_{avg} mit Gleichung (E.1) abgeschätzt:

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \cdots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \cdots + \frac{1}{MTTF_{DN}}} \quad \text{(E.1)}$$

Alle Bauteile des SRP/CS ohne Fehlerausschluss sollten berücksichtigt und aufsummiert werden. Für jeden Block werden die $MTTF_D$ und der DC berücksichtigt. DC in dieser Gleichung bedeutet das Verhältnis der Ausfallrate erkannter gefahrbringender Ausfälle des Teils (ungeachtet der Maßnahmen, durch die die Ausfälle erkannt werden) zur Ausfallrate aller gefahrbringenden Ausfälle des Teils. Somit bezieht sich der DC auf die getesteten Teile und nicht auf die Testeinrichtung. Bauteile ohne Ausfallerkennung (z. B. die nicht getestet werden) haben einen $DC = 0$ und tragen nur zum Nenner des DC_{avg} bei.

Anhang F
(informativ)

Verfahren zur Quantifizierung von Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF)

F.1 Allgemeines

Das umfangreiche Verfahren für die Maßnahmen gegen CCF, wie in F.2 und F.3 beschrieben, sollte für jedes Teilsystem der Kategorie 2, 3 oder 4, das einen Beitrag zum SRP/CS leistet, befolgt werden.

Das vereinfachte Verfahren von 6.1.8 dieses Dokuments setzt einen β-Faktor von 2 % nach IEC 61508-6:2010, Anhang D, voraus. Dies kann durch Einhaltung des Verfahrens in F.2 erreicht werden.

Die in F.2 und F.3 beschriebenen Maßnahmen sollten dokumentiert werden, um das Erreichen einer Mindestbewertung von 65 Punkten zu unterstützen.

F.2 Abschätzung der Auswirkung der Maßnahmen gegen CCF

Jeder Teil des Teilsystems sollte hinsichtlich CCF betrachtet werden.

In Tabelle F.1 sind die Maßnahmen auf der Grundlage einer technischen Bewertung angegeben und es ist der Beitrag jeder Maßnahme zur Verringerung von CCFs aufgeführt.

In F.3 sind diese Maßnahmen ausführlicher beschrieben. Für jede aufgeführte Maßnahme kann die volle Punktzahl nur dann erzielt werden, wenn die Maßnahme vollständig umgesetzt wird. Falls eine Maßnahme nur zum Teil umgesetzt wird, sollte eine Punktzahl von null angenommen werden.

Jede Maßnahme sollte auf der Grundlage der spezifischen Anwendung und der relevanten Ursachen für CCF bewertet werden (z. B. ist für elektronische Systeme nur die „Vermeidung von elektromagnetischen Störungen“ relevant und nicht die „Verunreinigung des flüssigen Mediums“).

Falls im SRP/CS Bauteile verwendet werden, die nicht ausreichend durch interne Maßnahmen gegen Überspannung und Umgebungseinflüsse geschützt sind, sollte dieser Schutz mithilfe von externen Schutzkomponenten wie Filtern und Abschirmungen auf Systemebene erreicht werden.

Tabelle F.1 — Verfahren zur Punktevergabe und Quantifizierung für Maßnahmen gegen CCF

Nr.	Maßnahme gegen CCF	Punktzahl
1	Trennung/Abtrennung	15
2	Diversität	20
3	Gestaltung/Anwendung/Erfahrung	
3.1	Schutz gegen Überspannung, Überdruck, Überstrom, Übertemperatur	15
3.2	Verwendung bewährter Bauteile	5
4	Beurteilung/Analyse	5
5	Ausbildung	5
6	Umgebung	

Nr.	Maßnahme gegen CCF	Punktzahl
6.1	Verhindern von elektromagnetischen Störungen oder von Verunreinigungen des Fluids	25
6.2	Andere Einflüsse	10
	Gesamt	[max. erreichbar 100]

Gesamtpunktzahl	Maßnahmen zum Vermeiden von CCF
65 oder besser	Anforderungen erfüllt
Weniger als 65	Verfahren gescheitert ⇒ Anwendung zusätzlicher Maßnahmen

Die in Tabelle F.1 aufgeführten Maßnahmen sollten hinsichtlich ihrer Wirksamkeit zur Vermeidung oder Beherrschung von CCFs in redundanten Kanälen bewertet werden. Eine ingenieurmäßige Beurteilung sollte unterstützen, dass typische Ursachen für CCF weitestgehend reduziert werden.

ANMERKUNG 1 Die Berechnung von CCF erfolgt üblicherweise auf Teilsystemebene, da sich die Maßnahmen für die einzelnen Teilsysteme voneinander unterscheiden (z. B. Eingänge, Logik und Ausgänge).

ANMERKUNG 2 Redundante Kanäle bedeuten in diesem Anhang Funktionskanäle und Testkanäle in der Kategorie 2 oder redundante Funktionskanäle in den Kategorien 3 und 4.

ANMERKUNG 3 Typische Ursachen für CCFs sind Überspannung, Überdruck, Überstrom, Überhitzung, Luftfeuchte, Stoß, Vibration, EMI, Verunreinigung des Druckmediums. Das angemessene Ausmaß dieser Ursachen wird aus der bestimmungsgemäßen Verwendung des SRP/CS abgeleitet, einschließlich vorhersehbarer Fehler (z. B. Ausfall eines Lüfters) und vernünftigerweise vorhersehbarer Fehlanwendung. Die Maßnahmen können in Abhängigkeit von den Kategorien (Kategorie 2 im Vergleich zu den Kategorien 3 und 4) oder von den Eingabe-/Logik-/Ausgabe-Einheiten des SRP/CS variieren.

F.3 Beschreibung der Maßnahmen von Tabelle F.1 gegen Ausfälle infolge gemeinsamer Ursache (CCF)

F.3.1 Trennung/Abtrennung

Physische Trennung zwischen den Signalpfaden von redundanten Kanälen, z. B.:

a) Trennung der Verdrahtung (z. B. mehradriges Kabel mit geeigneter Isolierung zwischen den Leitern);

b) Trennung der Verrohrung (z. B. Vermeiden von Beschädigungen einer Hydraulikleitung durch zu hohen Druck, der von einer anderen benachbarten Leitung freigesetzt wurde);

c) Erkennen von Kurzschlüssen und Unterbrechungen in Kabeln durch dynamische Prüfung;

d) getrennte Abschirmung des Signalpfads jedes Kanals;

e) redundante Kanäle auf separaten gedruckten Schaltungen oder in separaten Gehäusen oder Schränken;

f) ausreichende Luft- und Kriechstrecken zwischen redundanten Kanälen auf gedruckten Schaltungen, auch unter Berücksichtigung von z. B. Zinn-Whiskers (siehe ISO 13849-2:2012, D.2.2).

F.3.2 Diversität

Betrachtungen der Diversität beinhalten z. B.:

a) unterschiedliche Technologien/Gestaltung oder physikalische Prinzipien werden verwendet, z. B.:

   — der erste Kanal elektronisch oder programmierbar elektronisch und der zweite Kanal elektromechanisch fest verdrahtet;

   — unterschiedliche Initiierung der Sicherheitsfunktion für jeden Kanal (z. B. Position, Druck, Temperatur);

   — das Ventil im ersten Kanal mit Gummidichtung und im zweiten Kanal mit Metalldichtung;

   — zwei Positionsschalter werden verwendet, um das Öffnen einer beweglichen trennenden Schutzeinrichtung (Schutzgitter) zu erkennen; dabei wird der erste Positionsschalter betätigt, wenn das Schutzgitter geöffnet wird, und dieser enthält einen Öffner-Kontakt mit Zwangsöffnung nach IEC 60947-5-1:2020, Anhang K; der zweite Positionsschalter wird betätigt, wenn das Schutzgitter geschlossen wird, und enthält einen Schließer-Kontakt;

b) Sensorlemente nutzen unterschiedliche Messprinzipien (z. B. digitale und analoge) oder physikalische Prinzipien (z. B. Abstand, Druck oder Temperatur);

c) verschiedene Bauteile, z. B. von unterschiedlichen Herstellern (nicht nur mit einem anderen Markenzeichen versehen);

d) unterschiedliche Lasten, z. B. Kontakt/Ventil des einen Kanals schaltet ohne Last, Kontakt/Ventil im zweiten Kanal schaltet unter Last.

F.3.3 Gestaltung/Anwendung/Erfahrung

Schutz vor oder Beherrschung von Überspannung, Überdruck, Überstrom, Überhitzung, z. B.:

a) Eingänge und Ausgänge des SRP/CS und die Energieversorgung der Logikeinheit sind vor potenziellen Überspannungs- und/oder Überstrom-Pegeln geschützt (siehe auch IEC 60204-1);

   ANMERKUNG Teile des SRP/CS können entweder potenziellen Überspannungs- oder Überstrom-Niveaus oder beidem standhalten oder sind davor geschützt. Das mögliche maximale Überspannungs-Niveau des Schaltnetzteils hängt von der angewendeten Norm ab (z. B. maximale Spannungsgrenze unter Einzelfehlerbedingung).

   Es ist wichtig, das mögliche maximale Überspannungs-Niveau durch das verwendete Standard-Schaltnetzteil sowie andere Betriebsbedingungen (z. B. Überspannungskategorie, Betriebstemperatur) zu berücksichtigen.

b) die Maßnahme gegen Überdruck kann ein einkanaliges System sein, wenn der primäre Druck bei einem Ausfall niemals über den 1,5-fachen Betriebsdruck steigen kann. In ISO 4414 ist eine Anforderung an den Schutz vor unbeabsichtigtem Druck enthalten (z. B. ein Druckentlastungsventil).

Nur bewährte Bauteile werden verwendet. Siehe 6.1.11 und ISO 13849-2.

F.3.4 Beurteilung/Analyse

Für jedes Teil von SRP/CS wurde eine Ausfalleffektanalyse oder eine FTA durchgeführt, um die möglichen Ursachen für CCF zu ermitteln, und es wurden deren Ergebnisse berücksichtigt, um CCFs im Entwurf zu vermeiden.

F.3.5 Ausbildung

Die Konstrukteure wurden ausgebildet (einschließlich eines Ausbildungsnachweises, z. B. ein Ausbildungszertifikat), damit sie die Gründe und Auswirkungen von CCFs nachvollziehen können.

F.3.6 Umgebung

F.3.6.1 Verhindern von elektromagnetischen Störungen oder Verunreinigungen des Druckmediums

Für elektrische/elektronische Systeme werden Verunreinigungen und elektromagnetische Störungen verhindert, um vor CCFs entsprechend den zutreffenden Normen (z. B. IEC 61326-3-1, IEC 61000-6-7:2014, IEC 61000-1-2:2016, IEC 61800-5-2) zu schützen.

ANMERKUNG 1 Diese EMI-Normen enthalten üblicherweise strengere Anforderungen im Vergleich zu den Anforderungen, nach denen Standard-Bauteile (z. B. SPS für allgemeine Anwendung) konstruiert sind. Siehe IEC 61800-3 für weitere Informationen.

ANMERKUNG 2 Anhang L enthält weitere Leitlinien in Bezug auf die elektromagnetische Störfestigkeit.

Für Fluidsysteme erfolgt das Filtrieren des Druckmediums, das Verhindern von Schmutzeintrag, das Entwässern von Druckluft in Übereinstimmung mit den Anforderungen des Bauteilherstellers an die Reinheit des Druckmediums (siehe ISO 8573-1 für Hinweise).

Bei kombinierten Fluid- und Elektrosystemen sollten beide Aspekte berücksichtigt werden.

F.3.6.2 Andere Einflüsse

Das SRP/CS besitzt eine Störfestigkeit gegenüber allen maßgebenden Umgebungseinflüssen wie Temperatur, Stoß, mechanische Beanspruchungen, Vibration, Luftfeuchte, wie in den zutreffenden Normen angegeben, z. B. in der Normenreihe IEC 60068, in der die strengeren Anforderungen an sicherheitsbezogene Anwendungen berücksichtigt werden.

F.4 Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF) und weitere zutreffende Normen

Für einige SRP/CS (Teilsysteme) können nicht alle in Tabelle F.1 aufgeführten Maßnahme gegen CCF eine ausreichende Minderung des CCF-Einflusses bieten, da die mögliche Risikominderung, die durch diese SRP/CS erzielt werden kann, auch durch deren systematische Fähigkeiten (z. B. Detektionsvermögen von Sensoren) begrenzt ist.

ANMERKUNG Einige zutreffende Normen (z. B. die Normenreihe IEC 62024 für die Anwendung von Schutzeinrichtungen zum Erkennen von anwesenden Personen oder ISO 14119:2013 für die Auswahl und Anwendung von Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen) können Anwendungsgrenzen in Zusammenhang mit den systematischen Fähigkeiten enthalten.

Der Konstrukteur des gesamten SRP/CS wendet die Maßnahmen an, die in diesen Normen angegeben sind, und befolgt die vom Hersteller bereitgestellte Betriebsanleitung.

Anhang G
(informativ)

Systematischer Ausfall

G.1 Allgemeines

Dieser Anhang enthält Leitlinien für die Maßnahmen zur Beherrschung und Vermeidung von systematischen Ausfällen während des Entwurfs und der Integration des SRP/CS.

G.2 Maßnahmen zur Beherrschung systematischer Ausfälle

Die folgenden Maßnahmen sollten angewendet werden:

a) Verwendung der Abschaltung: Das SRP/CS sollte so ausgelegt sein, dass die Maschine bei einem Ausfall der Stromversorgung einen sicheren Zustand erreicht oder beibehält (siehe ISO 13849-2:2012, IEC 60204-1:2016+AMD1:2021, 7.5 und ISO 62061:2021);

b) Maßnahmen zur Beherrschung der Auswirkungen von Spannungsausfall, Spannungsschwankungen, Überspannung und Unterspannung: das Verhalten des SRP/CS als Reaktion auf die Bedingungen bei Spannungsausfall, Spannungsschwankungen, Überspannung und Unterspannung sollte im Voraus bestimmt werden, sodass das SRP/CS den sicheren Zustand der Maschine erreichen oder aufrechterhalten kann (siehe auch IEC 60204-1:2016+AMD1:2021, Abschnitt 7 und IEC 61508-7:2010, A.8);

c) Maßnahmen zur Beherrschung oder Vermeidung von Einflüssen der physikalischen Umgebungsbedingungen (z. B. Temperatur, Luftfeuchte, Wasser, Vibration, Staub, korrosive Substanzen, EMI und deren Auswirkungen): das Verhalten des SRP/CS als Reaktion auf die Einflüsse der physikalischen Umgebungsbedingungen sollte im Voraus bestimmt werden, sodass das SRP/CS den sicheren Zustand der Maschine erreichen oder aufrechterhalten kann (siehe auch z. B. IEC 60529, IEC 60204-1);

d) für SRP/CS, die Software enthalten, sollte eine Überwachung des Programmablaufs verwendet werden, um fehlerhafte Programmabläufe zu erkennen: ein fehlerhafter Programmablauf liegt vor, wenn die einzelnen Elemente eines Programms (z. B. Softwaremodule, Unterprogramme oder Befehle) in der falschen Reihenfolge oder im falschen Zeitablauf bearbeitet werden oder wenn der Takt des Prozessors fehlerhaft ist (siehe IEC 61508-7:2010, A.9);

e) Maßnahmen zur Beherrschung der Auswirkungen von Abweichungen und anderen Auswirkungen, verursacht durch irgendeinen Datenkommunikationsprozess (siehe IEC 61508-2:2010, 7.4.11).

Zusätzlich sollten eine oder mehrere der folgenden Maßnahmen unter Berücksichtigung der Komplexität des SRP/CS und dessen PL angewendet werden:

— Ausfallerkennung durch automatische Tests;

— Testung durch redundante Hardware;

— diversitäre Hardware;

— Betreiben im Ruhestromprinzip;

— zwangsgeführte Kontakte;

— zwangsöffnende Kontakte;

— gerichtetes Ausfallverhalten;

— Überdimensionierung durch einen geeigneten Faktor, wenn der Hersteller nachweisen kann, dass eine Überdimensionierung die Zuverlässigkeit erhöht.

ANMERKUNG Für Beispiele für Überdimensionierung siehe ISO 13849-2:2012, Tabelle D.2.

G.3 Maßnahmen zur Vermeidung systematischer Ausfälle während des SRP/CS-Entwurfs

Die folgenden Maßnahmen sollten angewendet werden:

a) Verwenden angemessener Materialien und geeignete Herstellung;

Auswahl des Materials, Herstellungsverfahren und Behandlung in Bezug auf z. B. Belastung, Haltbarkeit, Elastizität, Reibung, Abnutzung, Korrosion, Temperatur, Leitfähigkeit, dielektrische Festigkeit.

b) richtige Dimensionierung und Formgebung;

Berücksichtigen von z. B. Belastung, Dehnung, Ermüdung, Temperatur, Oberflächenrauheit, Toleranzen, Verarbeitung.

c) richtige Auswahl, Kombination, Anordnung, Zusammenbau und Installation der Bauteile, einschließlich Verkabelung, Leitungsführung und Verbindungen;

Anwenden geeigneter Normen und Herstellerhinweise zur Anwendung, z. B. Katalogblätter, Montageanweisungen, Spezifikationen und Anwendung guter ingenieursmäßiger Praxis.

d) Kompatibilität;

Verwenden von Bauteilen mit kompatiblen Betriebskenndaten.

ANMERKUNG Bauteile, wie z. B. hydraulische oder pneumatische Ventile, können zyklisches Schalten erfordern, um Ausfälle durch Nicht-Schalten oder inakzeptablen Anstieg der Schaltzeiten zu vermeiden. In diesem Fall ist eine wiederkehrende Prüfung notwendig.

e) Beständigkeit gegen die festgelegten Umgebungsbedingungen;

Gestalten des SRP/CS in der Form, dass es in der Lage ist, unter allen erwarteten Umgebungsbedingungen und vorhersehbaren widrigen Bedingungen, z. B. Temperatur, Feuchte, Vibration und EMI, zu arbeiten (siehe ISO 13849-2:2012, D.2).

f) Verwendung von Bauteilen, die nach einer geeigneten Norm entworfen wurden und deren Ausfallarten eindeutig definiert sind.

Zur Verminderung des Risikos unerkannter Fehler durch Verwendung von Bauteilen mit speziellen Eigenschaften siehe IEC 61508-7:2010, B.3.3.

Zusätzlich sollten eine oder mehrere der folgenden Maßnahmen unter Berücksichtigung der Komplexität des SRP/CS und dessen PL angewendet werden:

— Überprüfung der Hardwaregestaltung (z. B. durch Inspektion oder Walk-through);

  Um Unstimmigkeiten zwischen der Spezifikation und der Umsetzung durch Prüfung und Analyse aufzudecken.

— rechnergestützte Entwurfswerkzeuge, die in der Lage sind, zu simulieren oder zu analysieren;

  Systematischer Entwurfsprozess und Einbeziehen geeigneter automatischer Konstruktionselemente, die bereits verfügbar und getestet sind.

— Simulation.

  Systematische und vollständige Inspektion des Entwurfs des SRP/CS im Hinblick auf sowohl die funktionale Leistung als auch die richtige Dimensionierung der Bauteile.

G.4 Maßnahmen zur Vermeidung systematischer Ausfälle während der Integration des SRP/CS

Die folgenden Maßnahmen sollten während der Integration des SRP/CS angewendet werden:

— Funktionstests;

— Projektmanagement;

— Dokumentation.

Zusätzlich sollte der Black-Box-Test unter Berücksichtigung der Komplexität des SRP/CS und dessen PL angewendet werden.

G.5 Management der funktionalen Sicherheit

Für jedes SRP/CS-Entwurfsprojekt sollte ein Plan der funktionalen Sicherheit erstellt und dokumentiert werden, der bei Bedarf aktualisiert werden sollte. Der Plan der funktionalen Sicherheit soll Maßnahmen zur Vermeidung fehlerhafter Spezifikationen, Umsetzung oder Modifikationen enthalten.

Der Plan der funktionalen Sicherheit sollte die maßgebenden Aktivitäten festlegen (siehe Bild 4) und sollte an das Projekt angepasst werden.

ANMERKUNG 1 Der Plan der funktionalen Sicherheit kann Bestandteil anderer Entwurfsunterlagen sein.

ANMERKUNG 2 Der Inhalt des Plans der funktionalen Sicherheit hängt von den jeweiligen Umständen ab, zu denen Folgende zählen können:

— Umfang des Projekts;

— Grad der Komplexität;

— Grad der Neuartigkeit des Entwurfs und der Technologie;

— Grad der Standardisierung von Gestaltungsmerkmalen;

— mögliche Folge(n) bei Ausfall.

Insbesondere sollte der Plan der funktionalen Sicherheit:

a) die maßgebenden Aktivitäten während des Entwurfsprozesses des SRP/CS festlegen (Spezifikation, Gestaltung, Integration, Analyse, Prüfung, Verifizierung, Validierung) sowie Einzelheiten darüber, wann diese aufgeführt werden sollten;

b) die Rollen und Ressourcen festlegen, die für die Durchführung und Überprüfung jeder dieser Aktivitäten notwendig sind;

c) Verfahren für die Freigabe, Konfiguration, Dokumentation und Änderung des Hardware- und Softwareentwurfs festlegen;

d) einen Validierungsplan aufstellen (siehe 10.1.2);

e) maßgebende Aktivitäten vor der Durchführung einer Änderung festlegen.

ANMERKUNG 3 Die geforderte Änderung kann beispielsweise auf Folgendes zurückzuführen sein:

— Änderung der SRS;

— die Bedingungen bei tatsächlichem Einsatz;

— Erfahrungen aus Vorfällen/Unfällen;

— Änderung des verarbeiteten Materials;

— Obsoleszenz;

— Änderungen an der Maschine oder an einer ihrer Betriebsarten.

Die Auswirkung der geforderten Änderung sollte analysiert werden, um die Auswirkung auf die Sicherheitsfunktion festzustellen.

Alle angenommenen Änderungen, die eine Auswirkung auf das SRP/CS haben, sollten eine Rückkehr zu einer entsprechenden Entwurfsphase für seine Hardware und/oder für seine Software einleiten (z. B. Spezifikation, Gestaltung, Integration, Installation, Inbetriebnahme und Validierung). Alle nachfolgenden Phasen und Managementprozesse sollten dann in Übereinstimmung mit den für die spezifischen Phasen in diesem Dokument festgelegten Verfahren durchgeführt werden. Alle maßgebenden Dokumente sollten überarbeitet, geändert und entsprechend neu ausgestellt werden.

Anhang H
(informativ)

Beispiel für eine Kombination von mehreren Teilsystemen

Bild H.1 zeigt eine schematische Darstellung der Kombination von Teilsystemen eines SRP/CS zur Bereitstellung einer der Sicherheitsfunktionen, um einen Aktuator der Maschine anzusteuern. Dies ist kein Funktionsdiagramm/Arbeitsdiagramm und dient nur dazu, das Prinzip der Zusammenschaltung der Kategorien und Technologien in dieser einen Funktion zu verdeutlichen.

Die Steuerung erfolgt durch eine elektronische Steuerlogik und ein hydraulisches Wegeventil. Das Risiko wird durch eine AOPD gemindert, die den Zugang zum Gefährdungsbereich erkennt und die Aktivierung des Fluid-Aktuators (Hydraulikzylinders) verhindert, wenn der Lichtstrahl unterbrochen ist.

Die Teilsysteme des SRP/CS, die die Sicherheitsfunktion bereitstellen, sind: AOPD, elektronische Steuerlogik, hydraulisches Wegeventil und deren Verbindungsmittel.

Diese kombinierten Teilsysteme stellen eine Stopp-Funktion als Sicherheitsfunktion bereit. Wenn die AOPD unterbrochen wird, liefern die Ausgänge ein Signal an die elektronische Steuerlogik, welche dem hydraulischen Wegeventil ein Signal übermittelt, um als Ausgang des SRP/CS den hydraulischen Durchfluss zu stoppen. An der Maschine stoppt dies die gefahrbringende Bewegung des Fluid-Aktuators (Hydraulikzylinders).

Diese Kombination von Teilsystemen bildet eine Sicherheitsfunktion und kombiniert verschiedene Kategorien und Technologien entsprechend den Anforderungen von Abschnitt 6. Unter Verwendung der Grundsätze dieses Dokuments können die Teilsysteme aus Bild H.2 wie folgt beschrieben werden.

— Kategorie 2, PL c, $PFH = 1{,}5 \times 10^{-6}/h$ für die berührungslos wirkende Schutzeinrichtung (Lichtschranke). Um die Wahrscheinlichkeit von Fehlern zu vermindern, nutzt diese Einrichtung bewährte Sicherheitsprinzipien;

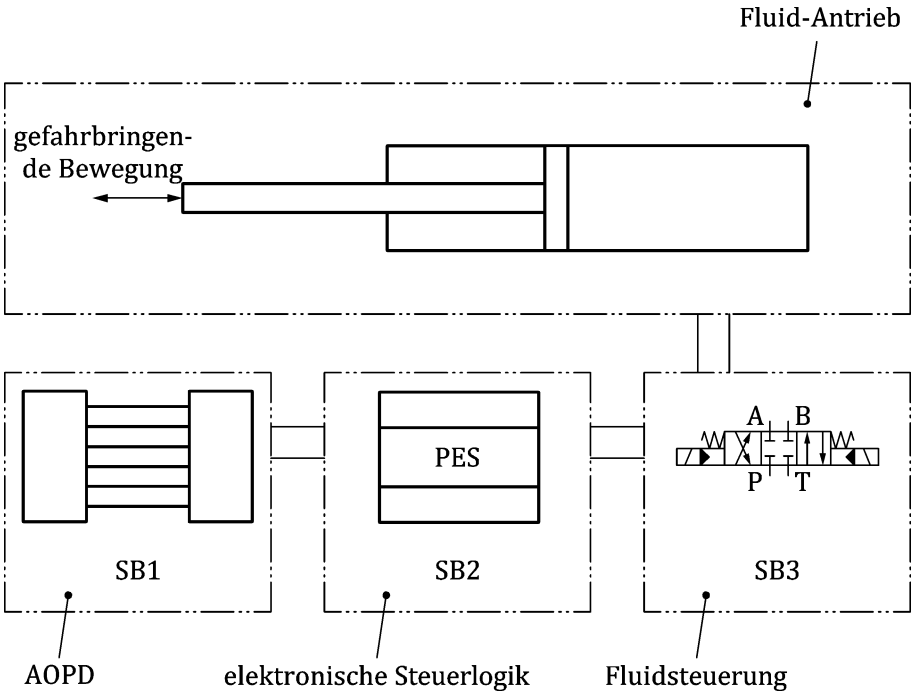
— Kategorie 3, PL d, $PFH = 2{,}0 \times 10^{-7}/h$ für die elektronische Steuerlogik. Um den Beitrag der elektronischen Steuerlogik zur sicherheitsbezogenen Leistungsfähigkeit zu erhöhen, ist die Struktur dieses Teilsystems redundant und enthält einige Fehlererkennungsmechanismen, sodass die meisten Einzelfehler erkannt werden;

— Kategorie 1, PL c, $PFH = 1{,}1 \times 10^{-6}/h$ für das hydraulische Wegeventil. Der Status als bewährtes Bauteil ist vor allem anwendungsspezifisch. In diesem Beispiel wird das Ventil als bewährt angenommen. Um die Wahrscheinlichkeit von Fehlern zu vermindern, beinhaltet dieses Gerät bewährte Bauteile und nutzt bewährte Sicherheitsprinzipien unter der Berücksichtigung aller Einsatzbedingungen (siehe 6.1.3.2.3).

ANMERKUNG 1 Die Lage, Größe und Anordnung der Verbindungsmittel wurden ebenfalls berücksichtigt.

Diese Kombination führt zu einem Summenwert von $PFH = 2{,}8 \times 10^{-6}/h$ im Bereich von PL c. Zusammen mit dem niedrigsten PL aller drei Teilsysteme, dem $PL_{niedrig}$ c, ergibt sich ein Gesamt-Performance-Level von PL c (siehe 6.2).

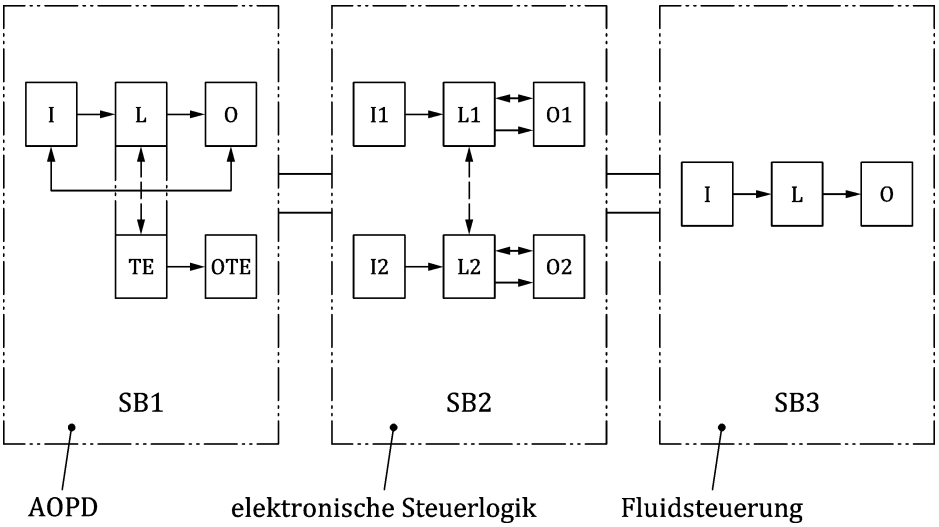
ANMERKUNG 2 Ein einzelner Fehler im Teilsystem der Kategorie 1 oder Kategorie 2 nach Bild H.2 kann zum Verlust der Sicherheitsfunktion führen.



Legende

AOPD	aktive optoelektronische Schutzeinrichtung (z. B. Lichtvorhang)
SB1	Kategorie 2 [Typ 2], PL c
SB2	Kategorie 3, PL d (elektronische Steuerlogik)
SB3	Kategorie 1, PL c (Fluidsteuerung)
PES	programmierbares elektronisches System

Bild H.1 — Beispiel — Blockdiagramm zur Erläuterung der Kombination von Teilsystemen



Legende

AOPD	aktive optoelektronische Schutzeinrichtung (z. B. Lichtvorhang)
I, I1, I2	Eingabegeräte, z. B. Sensor
L, L1, L2	Logik
O, O1, O2, OTE	Ausgabegeräte, z. B. Hauptschütz
SB1	Kategorie 2 [Typ 2], PL c
SB2	Kategorie 3, PL d (elektronische Steuerlogik)
SB3	Kategorie 1, PL c (Fluidsteuerung)
TE	Testeinrichtung

Bild H.2 — Ersatz für Bild H.1 durch vorgesehene Architekturen

Anhang I
(informativ)

Beispiele für das vereinfachte Verfahren zur Abschätzung des PL von Teilsystemen

I.1 Allgemeines

Dieser Anhang veranschaulicht die Anwendung des vereinfachten Verfahrens zur Abschätzung des PL nach 6.1.8 und den vorhergehenden Anhängen zur Ermittlung der Sicherheitsfunktionen und zur Bestimmung des PL. Es wird die Quantifizierung zweier Steuerkreise gezeigt. Für das schrittweise Vorgehen siehe Bild 4.

Die folgenden Beispiele berücksichtigen nicht die Maßnahmen, mit denen die Systemintegrität, die Softwareanforderungen sowie die ordnungsgemäße Anwendung der grundlegenden und bewährten Prinzipien sichergestellt werden. Sie dienen lediglich der Quantifizierung von $MTTF_D$, DC_{avg}, CCF, der Kategorie und des zugehörigen PL.

Es werden zwei Beispiele (A und B) für Steuerkreise von unterschiedlichen Maschinen betrachtet (siehe Bild I.1 und Bild I.3). Beide zeigen die Leistungsfähigkeit der gleichen Sicherheitsfunktion der Verriegelung einer trennenden Schutzeinrichtung in Form einer Tür, haben aber unterschiedliche PL_r aufgrund der Unterschiede bei der Anwendung. Das erste Beispiel besteht aus nur einem Kanal aus elektromechanischen Bauteilen mit mittleren und hohen $MTTF_D$-Werten, während das zweite Beispiel aus zwei Kanälen besteht, einem elektromechanischen und einem programmierbar elektronischen, mit Bauteilen mit mittleren und hohen $MTTF_D$-Werten und mit entsprechenden Diagnosemaßnahmen.

I.2 Sicherheitsfunktion und erforderlicher Performance Level (PL_r)

Für beide Beispiele können die Anforderungen an die Sicherheitsfunktion in Verbindung mit der Verriegelung der beweglich trennenden Schutzeinrichtung wie folgt festgelegt werden.

Die gefahrbringende Bewegung hält an (durch Abbremsen oder Abschalten des Elektromotors), wenn die verriegelnde trennende Schutzeinrichtung geöffnet wird.

ANMERKUNG Für das Beispiel B wurde bei der Risikobeurteilung festgestellt, dass ein Verlust des geregelten Abbremsens des Motors infolge einer Fehlfunktion (SW2, CC oder SPS) akzeptabel ist.

Der Mindestabstand zwischen der verriegelnden trennenden Schutzeinrichtung und den beweglichen Teilen der Maschine wurde nach ISO 13855:2010 ermittelt, basierend auf dem Nachlauf der Maschine.

Für Beispiel A sehen die Risikoparameter entsprechend dem Verfahren mit Risikographen (siehe Bild A.1) wie folgt aus:

— Schwere der Verletzung, S = S2, ernst;

— Häufigkeit und/oder Dauer der Gefährdungsexposition, F = F1, selten bis weniger häufig und/oder die Gefährdungsexpositionszeit ist kurz;

— Möglichkeit zur Vermeidung oder Begrenzung des Schadens, P = P1, möglich unter bestimmten Voraussetzungen.

Diese Auswahl an Risikoparametern führt zu einem PL_r von c.

Bestimmung der bevorzugten Kategorie: ein Performance Level von „c“ kann üblicherweise durch hochzuverlässige einkanalige Systeme (Kategorie 1), geprüfte einkanalige Systeme (Kategorie 2) oder durch redundante Architekturen (Kategorie 3) erreicht werden (siehe Bild 12).

Für Beispiel B sind die Risikoparameter S2 und P1 die gleichen aber bei der Häufigkeit und/oder Gefährdungsexpositionszeit ist F = F2, häufig oder ständig und/oder die Gefährdungsexpositionszeit ist von langer Dauer.

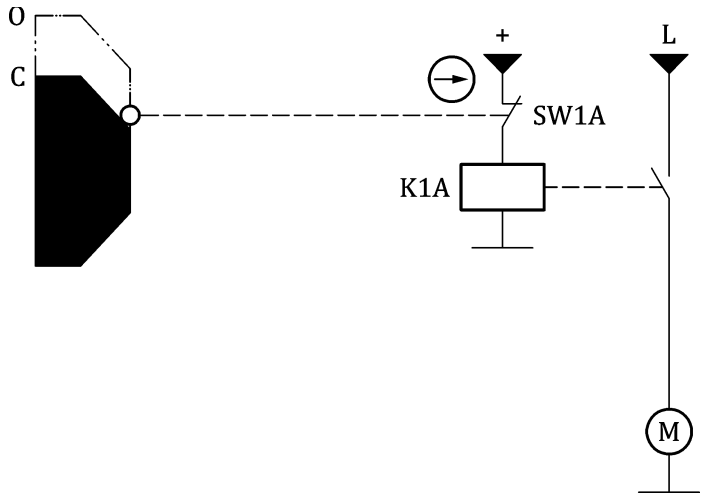
Diese Entscheidungen führen zu einem PL_r von d.

Bestimmung der bevorzugten Kategorie: ein Performance Level von „d“ kann in der Regel durch redundante Architekturen erreicht werden (Kategorie 2 oder 3) (siehe Bild 12).

I.3 Beispiel A — Einkanaliges System

I.3.1 Identifizierung der sicherheitsbezogenen Teile

Alle Bauteile, die zur Sicherheitsfunktion der Verriegelung einer trennenden Schutzeinrichtung beitragen, sind in Bild I.1 dargestellt. Andere Bauteile, die nicht zur Sicherheitsfunktion beitragen (z. B. Start- und Stopp-Schalter) sind aus Gründen der Einfachheit weggelassen worden.



Legende

O	verriegelnde trennende Schutzeinrichtung ist offen
C	verriegelnde trennende Schutzeinrichtung ist geschlossen
M	Motor
K1A	Hilfsschütz
SW1A	Positionsschalter (NC)
L	Energieversorgung
⊖	Zwangsöffnung

Bild I.1 — Steuerkreis A zur Ausführung der Sicherheitsfunktion

In diesem Beispiel wird ein Positionsschalter SW1A mit Zwangsöffnung und zwangläufiger Betätigung verwendet, jedoch kein Fehlerausschluss für die mechanischen Teile begründet. Der Positionsschalter ist mit einem Hilfsschütz K1A verbunden, der in der Lage ist, die Energiezufuhr zum Motor zu trennen. Die wesentlichen Merkmale dieses SRP/CS sind daher:

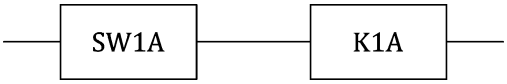
— ein Kanal aus elektromechanischen Bauteilen;

— Positionsschalter SW1A (NC) hat zwangsöffnende Kontakte und hohen B_{10D};

— Hilfsschütz K1A hat hohen B_{10D}.

Der Positionsschalter und das Hilfsschütz in diesem Beispiel gelten beide als bewährte Bauteile, wenn sie nach ISO 13849-2:2012 angewendet werden.

Das SRP/CS kann in einem sicherheitsbezogenen Blockdiagramm dargestellt werden, wie in Bild I.2 gezeigt.



Legende
SW1A Positionsschalter
K1A Hilfsschütz

Bild I.2 — Sicherheitsbezogenes Blockdiagramm, das die sicherheitsbezogenen Teile (SRPs) von Beispiel A zeigt

I.3.2 Quantifizierung von $MTTF_D$, DC_{avg}, Maßnahmen gegen CCF, Kategorie und Performance Level

Es wird angenommen, dass die Werte für $MTTF_D$, DC_{avg} und Maßnahmen gegen CCF nach Anhang C, Anhang D, Anhang E und Anhang F abgeschätzt oder durch den Hersteller angegeben werden. Die Kategorien werden nach 6.1.3 abgeschätzt.

— $MTTF_D$

Der Positionsschalter SW1A und das Hilfsschütz K1A tragen zur $MTTF_D$ des einen Kanals bei. Es wird angenommen, dass die Werte von $B_{10D,SW1A} = 20\,000\,000$ Zyklen (Positionsschalter unabhängig von der Last) und $B_{10D,K1A} = 400\,000$ Zyklen (Hilfsschütz mit maximaler Last) vom Hersteller zur Verfügung gestellt werden. Durch Anwendung des Verfahrens von C.4.2 mit 220 Arbeitstagen je Jahr, 8 Arbeitsstunden je Tag und einer Zyklusdauer von 60 Minuten ergibt sich $MTTF_{D,SW1A} = 113\,636$ Jahre und $MTTF_{D,K1A} = 2\,273$ Jahre. Anschließend wird mithilfe des Parts-Count-Verfahrens nach D.1 die $MTTF_D$ des einen Kanals mit folgender Gleichung berechnet:

$$\frac{1}{MTTF_D} = \frac{1}{MTTF_{D,SW1A}} + \frac{1}{MTTF_{D,K1A}} = \frac{1}{113\,636\ \text{Jahre}} + \frac{1}{2\,273\ \text{Jahre}} = \frac{0{,}000\,45}{\text{Jahr}} \tag{I.1}$$

woraus sich $MTTF_D = 2\,222$ Jahre (begrenzt auf 100 Jahre) für den Kanal ergibt, was „hoch“ nach 6.1.4, Tabelle 6, ist.

ANMERKUNG Wenn keine B_{10D}-Informationen zu SW1A oder K1A zur Verfügung stehen, kann eine Annahme für den ungünstigsten Fall nach C.2 oder C.4 gemacht werden.

— T_{10D}

Das in C.4.2 angegebene Verfahren ergibt $T_{10D,SW1A}$ mit 11 364 Jahren und $T_{10D,K1A}$ mit 227 Jahren, die beide die Gebrauchsdauer von 20 Jahren überschreiten und aus diesem Grund die Notwendigkeit eines vorbeugenden Austauschs ausschließen.

— DC

Da keine diagnostische Prüfung im Steuerkreis A erfolgt, ist der DC = 0 oder „keiner“; da nur ein Kanal verwendet wird, ist DC nicht relevant.

— CCF

Da nur ein Kanal verwendet wird, sind Maßnahmen gegen CCF nicht relevant.

— Kategorie

Die Eigenschaften von Kategorie 1 (grundlegende und bewährte Sicherheitsprinzipien, bewährte Bauteile) sind erfüllt, einschließlich der Anforderung, dass die $MTTF_D$ des Kanals „hoch“ sein muss.

Eingangsdaten für Bild 12: $MTTF_D$ des Kanals ist „hoch“ (100 Jahre), DC_{avg} ist „keiner“ und Kategorie ist 1.

Mithilfe von Bild 12 wird dies als Performance Level c gewertet.

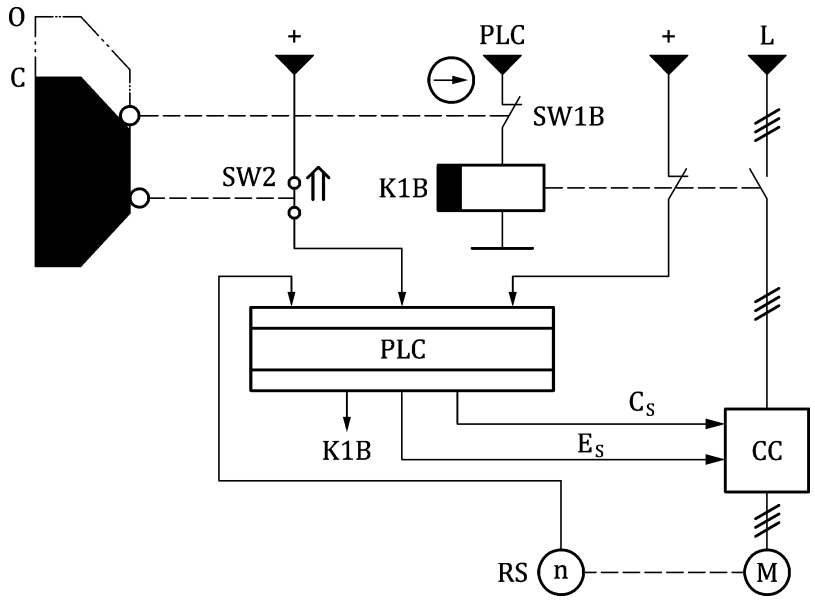
Die Anwendung von Anhang K ergibt eine PFH von $1{,}14 \times 10^{-6}$/h und PL c.

Dieses Ergebnis entspricht dem PL_r c nach Bild I.2. Die Steuerung in Beispiel A erfüllt somit die Anforderungen an die Risikominderung für das Anwendungsbeispiel A nach I.2, mit S2, F1, P1 und PL_r c.

I.4 Beispiel B — Redundantes System

I.4.1 Identifizierung der sicherheitsbezogenen Teile

Alle Bauteile, die zur Sicherheitsfunktion der Verriegelung einer trennenden Schutzeinrichtung beitragen, sind in Bild I.3 dargestellt. Andere Bauteile, die nicht zur Sicherheitsfunktion beitragen (z. B. Start- und Stopp-Schalter oder verzögertes Schalten von K1B) wurden aus Gründen der Einfachheit weggelassen.



Legende

SPS	speicherprogrammierbare Steuerung	C_s	Stopp-Signal (normal)
CC	Stromrichter (en: current converter)	E_S	Freigabe (normal)
M	Motor	K1B	Hilfsschütz
RS	Drehgeber (en: rotation sensor)	SW1B	Positionsschalter (NC)
O	verriegelnde trennende Schutzeinrichtung ist offen	SW2	Positionsschalter (NO)
C	verriegelnde trennende Schutzeinrichtung ist geschlossen	⊖	Zwangsöffnung
L	Energieversorgung	⇑	betätigte Stellung

Bild I.3 — Steuerkreis B zur Ausführung der Sicherheitsfunktion

In diesem zweiten Beispiel wird eine Architektur mit zwei Kanälen verwendet, um die Redundanz bereitzustellen. Wie in Beispiel A umfasst der erste Kanal einen Positionsschalter SW1B mit zwangsöffnenden Kontakten in zwangläufiger Betätigung. Dieser Positionsschalter ist mit einem Hilfsschütz K1B verbunden, der in der Lage ist, die Energiezufuhr zum Motor abzuschalten. Im zweiten Kanal, der (speicherprogrammierbare) elektronische Bauteile enthält, ist ein zweiter Positionsschalter SW2 an eine speicherprogrammierbare Steuerung (SPS) angeschlossen, der den Stromrichter CC ansteuern kann, um die Energiezufuhr zum Motor abzuschalten. Die wesentlichen Merkmale dieses SRP/CS sind daher:

— redundante Kanäle, ein elektromechanischer und ein programmierbar elektronischer;

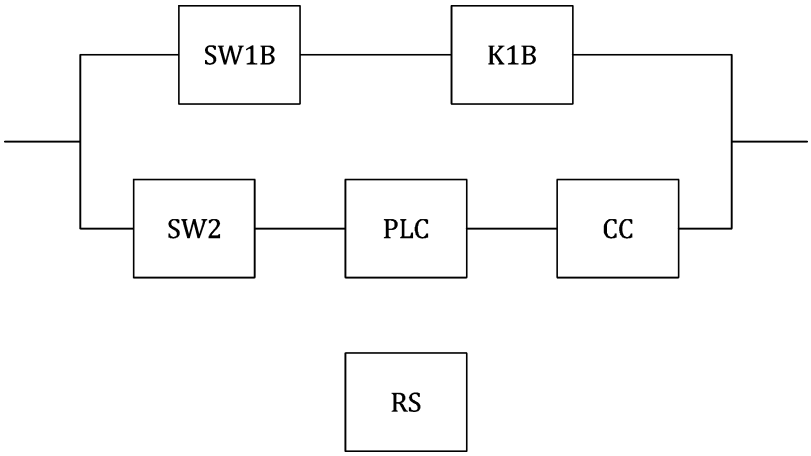
— nur der Positionsschalter SW1B (NC) verfügt über zwangsöffnende Kontakte, aber beide Positionsschalter SW1B und SW2 haben einen hohen B_{10D};

— die $MTTF_D$ des Hilfsschützes K1B ist hoch;

— die $MTTF_D$ der elektronischen Bauteile SPS und CC ist mittel;

— die SRASW der SPS, z. B. der mit der Überwachung der Eingangssignale SW2, K1B, RS und der Ausgabeanweisungen an den Stromrichter befasste Teil der Software, ist nach 7.3 mit einem PL_r von d festgelegt, entworfen und verifiziert.

Das SRP/CS und seine Aufteilung in Kanäle kann in einem sicherheitsbezogenen Blockdiagramm, wie in Bild I.4 gezeigt, dargestellt werden. Der erste Kanal besteht somit aus SW1B und K1B und der zweite Kanal besteht aus SW2, SPS und CC, während RS nur zur Prüfung des Stromrichters verwendet wird.



Legende

SW1B	Positionsschalter	SPS	speicherprogrammierbare Steuerung
K1B	Hilfsschütz	CC	Stromrichter (en: current converter)
SW2	Positionsschalter	RS	Drehgeber (en: rotation sensor)

Bild I.4 — Blockdiagramme, die die sicherheitsbezogenen Teile (SRPs) aus Beispiel B kennzeichnen

I.4.2 Quantifizierung von $MTTF_D$ für jeden Kanal, durchschnittlichem Diagnosedeckungsgrad, Maßnahmen gegen CCF, Kategorie und Performance Level

Es wird angenommen, dass die Werte für $MTTF_D$ für jeden Kanal, DC_{avg} und Maßnahmen gegen CCF nach Anhang C, Anhang D, Anhang E und Anhang F bewertet werden oder durch den Hersteller angegeben werden. Die Kategorien werden nach 6.1.3 ermittelt.

Der Positionsschalter SW1B verfügt über Zwangsöffnung mit zwangläufiger Betätigung, jedoch wird kein Fehlerausschluss für die mechanischen Teile getätigt.

— $MTTF_D$

Der Positionsschalter SW1B und das Hilfsschütz K1B tragen zur $MTTF_{D,C1}$ des ersten Kanals bei. Es wird angenommen, dass die Werte von $B_{10D,SW1B} = 20\,000\,000$ Zyklen (Positionsschalter unabhängig von der Last) und $B_{10D,K1B} = 400\,000$ Zyklen (Hilfsschütz mit maximaler Last) vom Hersteller zur Verfügung gestellt werden. Durch Anwendung des Verfahrens von C.4.2 mit 300 Arbeitstagen je Jahr, 16 Arbeitsstunden je Tag und einer Zyklusdauer von 4 Minuten ergibt sich $MTTF_{D,SW1B'} = 2\,778$ Jahre und $MTTF_{D,K1B} = 56$ Jahre. Anschließend wird mithilfe des Parts-Count-Verfahrens nach D.1 die $MTTF_{D,C1}$ des ersten Kanals mit folgender Gleichung berechnet:

$$\frac{1}{MTTF_{D,C1}} = \frac{1}{MTTF_{D,SW1B}} + \frac{1}{MTTF_{D,K1B}} = \frac{1}{2\,778\ \text{Jahre}} + \frac{1}{56\ \text{Jahre}} = \frac{0{,}018\,2}{\text{Jahr}} \tag{I.2}$$

woraus sich eine $MTTF_D = 55$ Jahre für den Kanal ergibt, was „hoch“ nach 6.1.4, Tabelle 6 ist.

Im zweiten Kanal tragen SW2, SPS und CC zur $MTTF_{D,C2}$ bei. Von $B_{10D,SW2}$ von 1 000 000 Zyklen wird angenommen, dass er vom Hersteller zur Verfügung gestellt wird. Die Anwendung des Verfahrens von C.4.2, wie für den ersten Kanal, ergibt eine $MTTF_{D,SW2}$ von 139 Jahren. Für SPS und CC wird angenommen, dass eine $MTTF_D$ von 20 Jahren vom Hersteller angegeben wird. Anschließend wird mithilfe des Parts-Count-Verfahrens nach D.1 die $MTTF_{D,C2}$ des zweiten Kanals mit folgender Gleichung berechnet:

$$\frac{1}{MTTF_{D,C2}} = \frac{1}{MTTF_{D,SW2}} + \frac{1}{MTTF_{D,PLC}} + \frac{1}{MTTF_{D,CC}} = \frac{1}{139\ \text{Jahre}} + \frac{1}{20\ \text{Jahre}} + \frac{1}{20\ \text{Jahre}} = \frac{0{,}107\ 2}{\text{Jahr}} \tag{I.3}$$

woraus sich eine $MTTF_D = 9{,}3$ Jahre für den Kanal ergibt, was „niedrig“ nach 6.1.4, Tabelle 6 ist.

ANMERKUNG Wenn keine $MTTF_D$-Informationen für SW1B, SW2 oder K1B zur Verfügung stehen, kann eine Annahme für den ungünstigsten Fall nach C.2 oder C.4 gemacht werden.

Da beide Kanäle unterschiedliche Werte für $MTTF_D$ besitzen, kann Gleichung (D.2) verwendet werden, um äquivalente identische Werte für $MTTF_D$ für ein symmetrisches Zwei-Kanal-System zu berechnen. Durch Anwendung dieser Gleichung ergibt sich $MTTF_D = 37$ Jahre für jeden Kanal, was „hoch“ nach 6.1.4, Tabelle 6 ist.

— T_{10D}

Das in C.4.2 angegebene Verfahren ergibt $T_{10D,SW1B}$ mit 278 Jahren, $T_{10D,K1B}$ mit 5,5 Jahren und $T_{10D,SW2}$ mit 13,9 Jahren, wobei die letzten beiden kürzer sind als die Gebrauchsdauer von 20 Jahren. Die Abschätzung von PL und PFH ist somit nur gültig, wenn K1B früher als nach 5,5 Jahren und SW2 früher als nach 13,9 Jahren Betriebszeit ausgetauscht werden.

— DC

Im Steuerkreis B werden fünf der SRP/CS durch die SPS geprüft. Diese Prüfung besteht aus SW1B, SW2 und K1B, die durch die SPS zurückgelesen werden, CC wird durch die SPS über RS zurückgelesen und die SPS führt Selbsttests durch. Die zugehörigen DC-Werte zu jedem dieser geprüften Teile sind:

a) $DC_{SW1B} = DC_{SW2} = 99$ %, „hoch“, aufgrund der Plausibilitätsprüfung, siehe Tabelle E.1 (zweite Zeile des Teils Eingabeeinheit);

b) $DC_{K1B} = 99$ %, „hoch“, aufgrund der zwangsgeführten Öffner-/Schließer-Kombination, siehe Tabelle E.1 (zweite Zeile des Teils Eingabeeinheit);

c) $DC_{SPS} = 30$ %, „keiner“, aufgrund der geringen Wirksamkeit der Selbsttests (dieser Wert ergibt sich aus der spezifischen Anwendung); und

d) $DC_{CC} = 90$ %, „mittel“, aufgrund indirekter Überwachung des Aktuators der Maschine durch die Steuerlogik, siehe Tabelle E.1 (sechste Zeile des Teils Ausgabeeinheit) — wenn die SPS einen Ausfall des CC bemerkt, ist es möglich, die Bewegung mit dem Freigabe-Signal (normal) anzuhalten und das Hilfsschütz K1B abzuschalten (zusätzlicher Abschaltpfad).

Für eine Abschätzung des PL wird als Eingabe für Bild 12 ein durchschnittlicher DC-Wert benötigt:

$$DC_{avg} = \frac{\frac{DC_{SW1B}}{MTTF_{D,SW1B}} + \frac{DC_{K1B}}{MTTF_{D,K1B}} + \frac{DC_{SW2}}{MTTF_{D,SW2}} + \frac{DC_{SPS}}{MTTF_{D,SPS}} + \frac{DC_{CC}}{MTTF_{D,CC}}}{\frac{1}{MTTF_{D,SW1B}} + \frac{1}{MTTF_{D,K1B}} + \frac{1}{MTTF_{D,SW2}} + \frac{1}{MTTF_{D,SPS}} + \frac{1}{MTTF_{D,CC}}} = \frac{\frac{0,99}{2\,778} + \frac{0,99}{56} + \frac{0,99}{139} + \frac{0,3}{20} + \frac{0,9}{20}}{\frac{1}{2\,778} + \frac{1}{56} + \frac{1}{139} + \frac{1}{20} + \frac{1}{20}} = \frac{0,09}{0,13} = 67,9\ \% \quad \text{(I.4)}$$

Demnach ist der sich daraus ergebende DC_{avg} „niedrig“.

— CCF

Für eine Abschätzung der Maßnahmen gegen CCF nach F.2 sind die Ergebnisse für Steuerkreis B in Tabelle I.1 angegeben.

Tabelle I.1 — Abschätzung der Maßnahmen gegen CCF für das Beispiel B

Nr.	Betrachtungseinheit	Angewendete Maßnahmen	Punktzahl für den Steuerkreis	Maximal mögliche Punktzahl
1	**Trennung/Abtrennung**			
	Physische Trennung zwischen den Signalpfaden	— getrennte Verdrahtung zur SPS zwischen SW1B und SW2 (Signalkabel getrennt verlegt) — Trennung der beiden Funktionskanäle im Gehäuse, z. B. zwischen K1B und CC (getrennte Bauteile) — Querverbindung beider Kanäle auf Diagnosetests beschränkt	15	15
2	**Diversität**			
	Unterschiedliche Technologien/Gestaltung oder physikalische Prinzipien werden verwendet	— der Positionsschalter SW1B wird betätigt, wenn das Schutzgitter geöffnet wird und ein Öffner mit Zwangsöffnung zum Einsatz kommt, während der Positionsschalter SW2 betätigt wird, wenn das Schutzgitter geschlossen ist und ein Schließer zum Einsatz kommt. — ein Funktionskanal nutzt elektromechanische Bauteile, die anderen nutzen speicherprogrammierbare elektronische Bauteile	20	20
3	**Gestaltung/Anwendung/Erfahrung**			
3.1	Schutz gegen Überspannung, Überdruck, Überstrom, Übertemperatur	— zusätzlicher Schutz gegen Überspannung und Überstrom auf Systemebene durch externe Schutzkomponenten, soweit erforderlich, d. h. Dioden, Sicherungen an den Ein- und Ausgängen und eine Freilaufdiode am Relais K1B — Überspannungs- und Unterspannungserkennung in der SPS	15	15

Nr.	Betrachtungseinheit	Angewendete Maßnahmen	Punktzahl für den Steuerkreis	Maximal mögliche Punktzahl
3.2	Verwendung bewährter Bauteile	Nur Schalter SW1B und Relais K1B sind bewährte Bauteile	keine (nur teilweise erfüllt, siehe F.2)	5
4	**Beurteilung/Analyse**			
	Für jedes Teil von SRP/CS wurde eine Ausfalleffektanalyse durchgeführt und deren Ergebnisse berücksichtigt, um Ausfälle infolge gemeinsamer Ursache im Entwurf zu vermeiden.	nicht vollständig umgesetzt (FMEA mit Schwerkpunkt auf CCF wurde durchgeführt, aber nicht auf formale und vollständig dokumentierte Weise)	keine	5
5	**Ausbildung**			
	Ausbildung der Konstrukteure, um die Gründe und Auswirkungen von CCFs zu verstehen.	nicht vollständig umgesetzt	keine	5
6	**Umgebung**			
6.1	Für elektrische/elektronische Systeme, Verhindern von Verunreinigungen und elektromagnetischen Störungen zum Schutz vor CCFs entsprechend den zutreffenden Normen (z. B. IEC 61326-3-1)	— zusätzlicher Schutz gegen elektromagnetische Störungen auf Systemebene durch externe Schutzkomponenten wie Dioden, Sicherungen, Filter und Abschirmungen an allen Ein- und Ausgängen (Umsetzung geeigneter Maßnahmen aus Tabelle L.1 mit Schwerpunkt auf CCF) — Signal- und Stromkabel sind getrennt verlegt	25	25
6.2	Andere Einflüsse Berücksichtigung der Anforderungen hinsichtlich Unempfindlichkeit gegenüber allen relevanten Umgebungsbedingungen wie Temperatur, Schock, Vibration, Luftfeuchte (z. B. wie in den zutreffenden Normen festgelegt).	— Auswahl beider Positionsschalter, um allen zu erwartenden Umwelteinflüssen mit ausreichender Überdimensionierung und Berücksichtigung möglicher CCF-Ursachen standzuhalten. — K1B, SPS und CC installiert im Gehäuse mit Temperaturregelung	10	10
	Gesamt		85	Höchstens 100

Ausreichende Maßnahmen gegen CCF erfordern eine Mindestpunktzahl von 65; somit ist die Punktzahl von 85 im Beispiel B ausreichend, um die Anforderungen gegen CCF zu erfüllen.

Die Eigenschaften von Kategorie 3 sind erfüllt, da ein einzelner Fehler in keinem dieser Teile zum Verlust der Sicherheitsfunktion führt. Wenn immer vernünftigerweise durchführbar, wird der einzelne Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt; der durchschnittliche Diagnosedeckungsgrad (DC_{avg}) ist im Bereich 60 % bis 90 %; die Maßnahmen gegen CCF sind ausreichend und die äquivalente $MTTF_D$ für jeden Kanal ist „hoch“.

Eingangsdaten für Bild 12: $MTTF_D$ des Kanals ist „hoch“ (37 Jahre), DC_{avg} ist „niedrig“ und Kategorie ist 3.

Durch Anwendung von Bild 12 kann dies als Performance Level d gewertet werden.

Die Anwendung von Anhang K (Anwendung von 36 Jahren) ergibt eine PFH von $5{,}16 \times 10^{-7}$/h und PL d.

Dieses Ergebnis entspricht dem erforderlichen PL_r d nach I.2. Somit erfüllt der Steuerkreis B die Anforderungen zur Risikominderung der Beispielanwendung B von I.2 mit S2, F2, P1 und PL_r d.

Anhang J
(informativ)

Beispiel für die Ausführung einer SRESW

J.1 Beschreibung des Beispiels

In diesem Anhang werden die Prozessschritte dargelegt, um die SRESW eines SRP/CS für einen PL_r d umzusetzen. Das SRP/CS ist mit der Maschinenausrüstung verbunden. Dies stellt Folgendes sicher:

— die Erfassung der von den verschiedenen Sensoren übermittelten Informationen;

— die notwendige Verarbeitung für den Betrieb der Leistungssteuerungselemente unter Berücksichtigung der Sicherheitsanforderungen; und

— das Ansteuern der Leistungssteuerungselemente.

Das Funktionsdiagramm der SRESW bei dieser Anwendung entspricht Bild J.1.

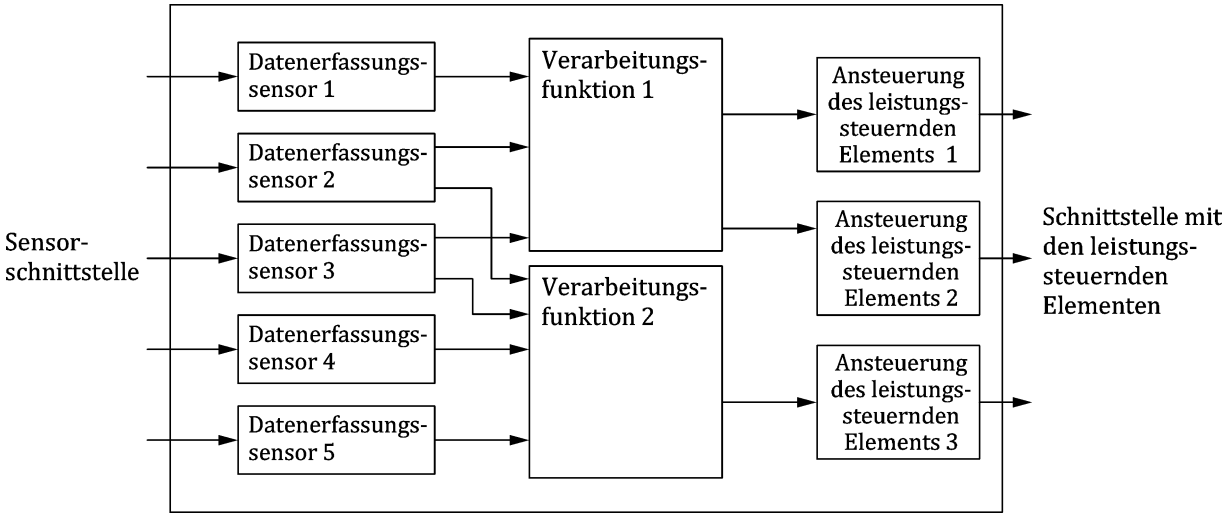


Bild J.1 — Entwurf eines Softwarebeispiels mit Funktionsbausteinsprache

J.2 Anwendung des V-Modells des Software-Sicherheitslebenszyklus

Tabelle J.1 führt die Entwicklungsaktivitäten auf, deren Verifizierungsschritte und die zugehörige Dokumentation. Diese Aktivitäten entsprechen dem V-Modell des Software-Sicherheitslebenszyklus nach Bild 14 a).

Tabelle J.1 — Aktivitäten und Dokumente innerhalb des Software-Sicherheitslebenszyklus

Entwicklungsaktivität	Lebenszyklusaktivität	Zugehörige Dokumentation
Maschinenaspekt (Hardware und Software): Identifizierung der mit dem SRP/CS verbundenen Funktionen	— Identifizierung der Sicherheitsfunktionen	Ausgang: — Spezifikation der Sicherheitsanforderungen (SRS)
Architekturaspekt (Hardware und Software): Definition der Steuerungsarchitektur mit Sensoren und Leistungssteuerungselementen	— Erläuterungen zu den Sicherheitsmerkmalen der gewählten Bauteile — Planung des Tests der SRS	Ausgang: — Definition der Steuerungsarchitektur — Testplan für die SRS
Aspekt der Softwarespezifikation: — Spezifikation der Anforderungen der sicherheitsbezogenen Software (SRSS), einschließlich: — Umsetzen der Maschinenfunktionen in Softwarefunktionen	— Überprüfen der Beschreibungen der SRSS anhand der SRS (siehe Abschnitt J.3) — Planung des Tests der SRSS anhand der SRS	Eingang: — Spezifikation der Sicherheitsanforderungen (SRS) Ausgang: — Software-Design-Spezifikation (SDS) einschließlich Softwarebeschreibungen — Testplan für die SDS — Dokumentation der Überprüfungsaktivitäten
Aspekt der Softwarearchitektur: — Software-System-Design, einschließlich der einzelnen Aufführung der Funktionen nach Funktionsblöcken	— Überprüfung des System-Designs anhand der SDS, einschließlich der Definition von kritischen Blöcken, die eine ausführlichere Überprüfung und Validierung benötigen — Planung des Tests des Software-System-Designs	Eingang: — SDS Ausgang: — Spezifikation des Software-System-Designs (SSDS), einschließlich eines Funktionsblockmodells — Testplan für die SSDS — Dokumentation der Überprüfungsaktivitäten
Design der Software-Module	— Überprüfung des Software-Modul-Designs anhand der SSDS — Planung des Tests der Software-Module	Eingang: — SSDS Ausgang: — Modul-Design-Spezifikation (MDS) — Testplan für die MDS — Dokumentation der Überprüfungsaktivitäten

Entwicklungsaktivität	Lebenszyklusaktivität	Zugehörige Dokumentation
Aspekt der Codierung: Codierung von nicht vorhandenen Software-Modulen entsprechend den Programmierregeln (siehe Abschnitt J.4)	— Überprüfung des Codes anhand der MDS — Verifizierung der Funktionen und der Übereinstimmung mit den Regeln	Eingang: — MDS Ausgang: — überprüfter Code einschließlich Codierungskommentaren im Code — Dokumentation der Überprüfungsaktivitäten
Validierungsaspekt: — Modul-Test	Test der Software-Module anhand der MDS entsprechend dem Testplan für die MDS, einschließlich: — Verifizierung der Testabdeckung — Verifizierung der Testergebnisse	Eingang: — überprüfter Code — MDS — Testplan für die MDS Ausgang: — getestete Software-Module — Dokumentation der Testaktivitäten
Validierungsaspekt: — Software-Integrations-Tests	Test der integrierten Software anhand der SSDS entsprechend dem Testplan für die SSDS, einschließlich: — Verifizierung der Testabdeckung — Verifizierung der Testergebnisse Der Test darf die endgültige Hardware umfassen (soweit möglich).	Eingang: — getestete Software-Module — SSDS — Testplan für die MDS Ausgang: — getestete Integration — Dokumentation der Testaktivitäten
Validierungsaspekt: — Validierung des SRP/CS Aufstellen von Testszenarien: — Betriebsaspekt der Funktionen — Aspekt des Verhaltens bei Ausfällen	Test der integrierten Software und Hardware (des SRP/CS) anhand der SDS entsprechend dem Testplan für die SDS, einschließlich: — Verifizierung der Testabdeckung — Verifizierung der Testergebnisse Der Test darf die endgültige Hardware umfassen (soweit möglich).	Eingang: — SDS — Testplan für die SDS Ausgang: — validierte Software (des SRP/CS) — Dokumentation der Testaktivitäten
ANMERKUNG Jeder Testplan umfasst: — eine Übereinstimmungsmatrix mit Querverweisen zu Absätzen der Spezifikation und zu Tests; — Testblätter, bestehend aus Testszenarien und Kommentaren zu erreichten Ergebnissen.		

J.3 Verifizierung der Softwarespezifikation auf verschiedenen Ebenen (d. h. SDS, SSDS, MDS)

Als Teil des Software-Sicherheitslebenszyklus nach Bild 14 a) bestehen die Verifizierungsaktivitäten in jeder Ebene der Softwarespezifikationen im Lesen der Spezifikationen, um nachzuweisen, dass alle sensiblen Punkte korrekt beschrieben sind. Folgendes sollte bei der Verifizierung jeder Softwarefunktion betrachtet werden:

a) Begrenzen der Fälle fehlerhafter Interpretation der Softwarespezifikation;

b) Vermeiden von Lücken in den Spezifikationen, die zu einem unbekannten Verhalten des SRP/CS führen;

c) genaue Definition der Bedingungen zur Aktivierung und Deaktivierung von Funktionen;

d) genaues Sicherstellen, dass alle möglichen Fälle behandelt sind;

e) Konsistenzprüfungen;

f) unterschiedliche Fälle der Parametrierung;

g) die Reaktion nach einem Ausfall.

J.4 Beispiel für Programmierregeln

Im Allgemeinen sollte es möglich sein, die Softwareversion zu identifizieren. Änderungen sollten unter Angabe von Autor, Datum und Art der Änderung dokumentiert werden. Hinsichtlich der Programmierregeln kann zwischen den folgenden Regeln unterschieden werden.

a) Programmierregeln auf Ebene der Programmstruktur

Die Programmierung sollte strukturiert werden, so dass sie ein konsistentes und verständliches allgemeines Gerüst dargestellt, in dem die verschiedenen Abläufe leicht lokalisiert werden können. Dies umfasst:

1) Verwenden von Vorlagen für typische Programm- und Funktionsblöcke;

2) Aufteilen des Programms in Teilabschnitte, um die wichtigen entsprechenden Teile zu kennzeichnen, die zu „Eingaben“, „Verarbeitungen“ und „Ausgaben“ gehören;

3) Kommentare, die in jedem Programmabschnitt des Quellcodes angezeigt werden sollten, um eine Aktualisierung der Kommentierung im Fall einer Änderung zu erleichtern;

4) die Beschreibung, welche Aufgabe ein Funktionsblock bei einem Aufruf hat;

5) dass die Verwendung eines Speicherbereichs nur durch einen einzelnen Datentyp mit eindeutigen Kennzeichnungen erfolgen sollte; und

6) dass der Programmablauf nicht abhängig sein sollte von Variablen wie Sprungadressen, die während der Laufzeit berechnet werden. Bedingungsabhängige Sprünge sind erlaubt.

b) Programmierregeln bezüglich der Verwendung von Variablen

1) Die Ansteuerung oder Absteuerung jedes Ausgangs sollte nur einmalig erfolgen (zentralisierte Bedingungen).

2) Das Programm sollte so strukturiert sein, dass die Gleichungen zum Aktualisieren einer Variablen zentralisiert sind.

3) Jede globale Variable, Eingabe oder Ausgabe sollte einen eindeutigen mnemonischen Namen erhalten und eine Beschreibung im Kommentar des Quelltextes.

c) Programmierregeln auf Funktionsblockebene

1) Es sollten Funktionsblöcke verwendet werden, die vom Lieferanten des SRP/CS validiert worden sind. Es sollte überprüft werden, ob die angenommenen Betriebsbedingungen für diese validierten Blöcke den Bedingungen des Programms entsprechen.

2) Die Größe des codierten Blocks sollte nach folgenden Richtwerten begrenzt werden:

— Parameter: höchstens acht digitale und zwei Integer-Eingänge, vier Ausgänge;

— im funktionalen Code: höchstens 10 lokale Variablen, höchstens 20 Boolesche Gleichungen.

3) Die Funktionsblöcke sollten die globalen Variablen nicht verändern.

4) Jeder Wert sollte mit den erwarteten voreingestellten Bezugswerten verglichen werden, um seine Gültigkeit sicherzustellen.

5) Die Eingabeparameter eines Funktionsblocks sollten auf Widersprüche überprüft werden.

6) Jeder Fehlercode sollte zugänglich sein und eine eindeutige Identifizierung des ursprünglichen Fehlers ermöglichen.

7) Die Fehlercodes und der Zustand des Blocks nach Bemerken eines Fehlers sollten durch Kommentare beschrieben sein.

8) Das Rücksetzen des Blocks oder die Wiederherstellung des normalen Zustands sollte durch Kommentare beschrieben sein.

Anhang K
(informativ)

Numerische Darstellung von Bild 12

Tabelle K.1 — Numerische Darstellung von Bild 12

$MTTF_D$ für jeden Kanal	Mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde (PFH) (1/h) und der zugehörige Performance Level													
	Kat. B		**Kat. 1**	**Kat. 2**		**Kat. 2**		**Kat. 3**		**Kat. 3**		**Kat. 4**		
Jahre	DC_{avg} = keiner		DC_{avg} = keiner	DC_{avg} = niedrig		DC_{avg} = mittel		DC_{avg} = niedrig		DC_{avg} = mittel		DC_{avg} = hoch		
3	$3{,}80 \times 10^{-5}$	a		$2{,}58 \times 10^{-5}$	a	$1{,}99 \times 10^{-5}$	a	$1{,}26 \times 10^{-5}$	a	$6{,}09 \times 10^{-6}$	b			
3,3	$3{,}46 \times 10^{-5}$	a		$2{,}33 \times 10^{-5}$	a	$1{,}79 \times 10^{-5}$	a	$1{,}13 \times 10^{-5}$	a	$5{,}41 \times 10^{-6}$	b			
3,6	$3{,}17 \times 10^{-5}$	a		$2{,}13 \times 10^{-5}$	a	$1{,}62 \times 10^{-5}$	a	$1{,}03 \times 10^{-5}$	a	$4{,}86 \times 10^{-6}$	b			
3,9	$2{,}93 \times 10^{-5}$	a		$1{,}95 \times 10^{-5}$	a	$1{,}48 \times 10^{-5}$	a	$9{,}37 \times 10^{-6}$	b	$4{,}40 \times 10^{-6}$	b			
4,3	$2{,}65 \times 10^{-5}$	a		$1{,}76 \times 10^{-5}$	a	$1{,}33 \times 10^{-5}$	a	$8{,}39 \times 10^{-6}$	b	$3{,}89 \times 10^{-6}$	b			
4,7	$2{,}43 \times 10^{-5}$	a		$1{,}60 \times 10^{-5}$	a	$1{,}20 \times 10^{-5}$	a	$7{,}58 \times 10^{-6}$	b	$3{,}48 \times 10^{-6}$	b			
5,1	$2{,}24 \times 10^{-5}$	a		$1{,}47 \times 10^{-5}$	a	$1{,}10 \times 10^{-5}$	a	$6{,}91 \times 10^{-6}$	b	$3{,}15 \times 10^{-6}$	b			
5,6	$2{,}04 \times 10^{-5}$	a		$1{,}33 \times 10^{-5}$	a	$9{,}87 \times 10^{-6}$	b	$6{,}21 \times 10^{-6}$	b	$2{,}80 \times 10^{-6}$	c			
6,2	$1{,}84 \times 10^{-5}$	a		$1{,}19 \times 10^{-5}$	a	$8{,}80 \times 10^{-6}$	b	$5{,}53 \times 10^{-6}$	b	$2{,}47 \times 10^{-6}$	c			
6,8	$1{,}68 \times 10^{-5}$	a		$1{,}08 \times 10^{-5}$	a	$7{,}93 \times 10^{-6}$	b	$4{,}98 \times 10^{-6}$	b	$2{,}20 \times 10^{-6}$	c			
7,5	$1{,}52 \times 10^{-5}$	a		$9{,}75 \times 10^{-6}$	b	$7{,}10 \times 10^{-6}$	b	$4{,}45 \times 10^{-6}$	b	$1{,}95 \times 10^{-6}$	c			
8,2	$1{,}39 \times 10^{-5}$	a		$8{,}87 \times 10^{-6}$	b	$6{,}43 \times 10^{-6}$	b	$4{,}02 \times 10^{-6}$	b	$1{,}74 \times 10^{-6}$	c			
9,1	$1{,}25 \times 10^{-5}$	a		$7{,}94 \times 10^{-6}$	b	$5{,}71 \times 10^{-6}$	b	$3{,}57 \times 10^{-6}$	b	$1{,}53 \times 10^{-6}$	c			
10	$1{,}14 \times 10^{-5}$	a		$7{,}18 \times 10^{-6}$	b	$5{,}14 \times 10^{-6}$	b	$3{,}21 \times 10^{-6}$	b	$1{,}36 \times 10^{-6}$	c			
11	$1{,}04 \times 10^{-5}$	a		$6{,}44 \times 10^{-6}$	b	$4{,}53 \times 10^{-6}$	b	$2{,}81 \times 10^{-6}$	c	$1{,}18 \times 10^{-6}$	c			
12	$9{,}51 \times 10^{-6}$	b		$5{,}84 \times 10^{-6}$	b	$4{,}04 \times 10^{-6}$	b	$2{,}49 \times 10^{-6}$	c	$1{,}04 \times 10^{-6}$	c			
13	$8{,}78 \times 10^{-6}$	b		$5{,}33 \times 10^{-6}$	b	$3{,}64 \times 10^{-6}$	b	$2{,}23 \times 10^{-6}$	c	$9{,}21 \times 10^{-7}$	d			

$MTTF_D$ für jeden Kanal	Mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde (PFH) (1/h) und der zugehörige Performance Level															
	Kat. B		**Kat. 1**		**Kat. 2**		**Kat. 2**		**Kat. 3**		**Kat. 3**		**Kat. 4**			
Jahre	DC_{avg} = keiner		DC_{avg} = keiner		DC_{avg} = niedrig		DC_{avg} = mittel		DC_{avg} = niedrig		DC_{avg} = mittel		DC_{avg} = hoch			
15	$7{,}61 \times 10^{-6}$	b			$4{,}53 \times 10^{-6}$	b	$3{,}01 \times 10^{-6}$	b	$1{,}82 \times 10^{-6}$	c	$7{,}44 \times 10^{-7}$	d				
16	$7{,}13 \times 10^{-6}$	b			$4{,}21 \times 10^{-6}$	b	$2{,}77 \times 10^{-6}$	c	$1{,}67 \times 10^{-6}$	c	$6{,}76 \times 10^{-7}$	d				
18	$6{,}34 \times 10^{-6}$	b			$3{,}68 \times 10^{-6}$	b	$2{,}37 \times 10^{-6}$	c	$1{,}41 \times 10^{-6}$	c	$5{,}67 \times 10^{-7}$	d				
20	$5{,}71 \times 10^{-6}$	b			$3{,}26 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}22 \times 10^{-6}$	c	$4{,}85 \times 10^{-7}$	d				
22	$5{,}19 \times 10^{-6}$	b			$2{,}93 \times 10^{-6}$	c	$1{,}82 \times 10^{-6}$	c	$1{,}07 \times 10^{-6}$	c	$4{,}21 \times 10^{-7}$	d				
24	$4{,}76 \times 10^{-6}$	b			$2{,}65 \times 10^{-6}$	c	$1{,}62 \times 10^{-6}$	c	$9{,}47 \times 10^{-7}$	d	$3{,}70 \times 10^{-7}$	d				
27	$4{,}23 \times 10^{-6}$	b			$2{,}32 \times 10^{-6}$	c	$1{,}39 \times 10^{-6}$	c	$8{,}04 \times 10^{-7}$	d	$3{,}10 \times 10^{-7}$	d				
30			$3{,}80 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}21 \times 10^{-6}$	c	$6{,}94 \times 10^{-7}$	d	$2{,}65 \times 10^{-7}$	d	$9{,}54 \times 10^{-8}$	e		
33			$3{,}46 \times 10^{-6}$	b	$1{,}85 \times 10^{-6}$	c	$1{,}06 \times 10^{-6}$	c	$5{,}94 \times 10^{-7}$	d	$2{,}30 \times 10^{-7}$	d	$8{,}57 \times 10^{-8}$	e		
36			$3{,}17 \times 10^{-6}$	b	$1{,}67 \times 10^{-6}$	c	$9{,}39 \times 10^{-7}$	d	$5{,}16 \times 10^{-7}$	d	$2{,}01 \times 10^{-7}$	d	$7{,}77 \times 10^{-8}$	e		
39			$2{,}93 \times 10^{-6}$	c	$1{,}53 \times 10^{-6}$	c	$8{,}40 \times 10^{-7}$	d	$4{,}53 \times 10^{-7}$	d	$1{,}78 \times 10^{-7}$	d	$7{,}11 \times 10^{-8}$	e		
43			$2{,}65 \times 10^{-6}$	c	$1{,}37 \times 10^{-6}$	c	$7{,}34 \times 10^{-7}$	d	$3{,}87 \times 10^{-7}$	d	$1{,}54 \times 10^{-7}$	d	$6{,}37 \times 10^{-8}$	e		
47			$2{,}43 \times 10^{-6}$	c	$1{,}24 \times 10^{-6}$	c	$6{,}49 \times 10^{-7}$	d	$3{,}35 \times 10^{-7}$	d	$1{,}34 \times 10^{-7}$	d	$5{,}76 \times 10^{-8}$	e		
51			$2{,}24 \times 10^{-6}$	c	$1{,}13 \times 10^{-6}$	c	$5{,}80 \times 10^{-7}$	d	$2{,}93 \times 10^{-7}$	d	$1{,}19 \times 10^{-7}$	d	$5{,}26 \times 10^{-8}$	e		
56			$2{,}04 \times 10^{-6}$	c	$1{,}02 \times 10^{-6}$	c	$5{,}10 \times 10^{-7}$	d	$2{,}52 \times 10^{-7}$	d	$1{,}03 \times 10^{-7}$	d	$4{,}73 \times 10^{-8}$	e		
62			$1{,}84 \times 10^{-6}$	c	$9{,}06 \times 10^{-7}$	d	$4{,}43 \times 10^{-7}$	d	$2{,}13 \times 10^{-7}$	d	$8{,}84 \times 10^{-8}$	e	$4{,}22 \times 10^{-8}$	e		
68			$1{,}68 \times 10^{-6}$	c	$8{,}17 \times 10^{-7}$	d	$3{,}90 \times 10^{-7}$	d	$1{,}84 \times 10^{-7}$	d	$7{,}68 \times 10^{-8}$	e	$3{,}80 \times 10^{-8}$	e		
75			$1{,}52 \times 10^{-6}$	c	$7{,}31 \times 10^{-7}$	d	$3{,}40 \times 10^{-7}$	d	$1{,}57 \times 10^{-7}$	d	$6{,}62 \times 10^{-8}$	e	$3{,}41 \times 10^{-8}$	e		
82			$1{,}39 \times 10^{-6}$	c	$6{,}61 \times 10^{-7}$	d	$3{,}01 \times 10^{-7}$	d	$1{,}35 \times 10^{-7}$	d	$5{,}79 \times 10^{-8}$	e	$3{,}08 \times 10^{-8}$	e		
91			$1{,}25 \times 10^{-6}$	c	$5{,}88 \times 10^{-7}$	d	$2{,}61 \times 10^{-7}$	d	$1{,}14 \times 10^{-7}$	d	$4{,}94 \times 10^{-8}$	e	$2{,}74 \times 10^{-8}$	e		
100			$1{,}14 \times 10^{-6}$	c	$5{,}28 \times 10^{-7}$	d	$2{,}29 \times 10^{-7}$	d	$1{,}01 \times 10^{-7}$	d	$4{,}29 \times 10^{-8}$	e	$2{,}47 \times 10^{-8}$	e		
110													$2{,}23 \times 10^{-8}$	e		
120													$2{,}03 \times 10^{-8}$	e		
130													$1{,}87 \times 10^{-8}$	e		
150													$1{,}61 \times 10^{-8}$	e		
160													$1{,}50 \times 10^{-8}$	e		

$MTTF_D$ für jeden Kanal	**Mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde (PFH) (1/h) und der zugehörige Performance Level**						
	Kat. B	**Kat. 1**	**Kat. 2**	**Kat. 2**	**Kat. 3**	**Kat. 3**	**Kat. 4**
Jahre	DC_{avg} = keiner	DC_{avg} = keiner	DC_{avg} = niedrig	DC_{avg} = mittel	DC_{avg} = niedrig	DC_{avg} = mittel	DC_{avg} = hoch
180							$1{,}33 \times 10^{-8}$ e
200							$1{,}19 \times 10^{-8}$ e
220							$1{,}08 \times 10^{-8}$ e
240							$9{,}81 \times 10^{-9}$ e
270							$8{,}67 \times 10^{-9}$ e
300							$7{,}76 \times 10^{-9}$ e
330							$7{,}04 \times 10^{-9}$ e
360							$6{,}44 \times 10^{-9}$ e
390							$5{,}94 \times 10^{-9}$ e
430							$5{,}38 \times 10^{-9}$ e
470							$4{,}91 \times 10^{-9}$ e
510							$4{,}52 \times 10^{-9}$ e
560							$4{,}11 \times 10^{-9}$ e
620							$3{,}70 \times 10^{-9}$ e
680							$3{,}37 \times 10^{-9}$ e
750							$3{,}05 \times 10^{-9}$ e
820							$2{,}79 \times 10^{-9}$ e
910							$2{,}51 \times 10^{-9}$ e
1 000							$2{,}28 \times 10^{-9}$ e
1 100							$2{,}07 \times 10^{-9}$ e
1 200							$1{,}90 \times 10^{-9}$ e
1 300							$1{,}75 \times 10^{-9}$ e
1 500							$1{,}51 \times 10^{-9}$ e

$MTTF_D$ für jeden Kanal Jahre	**Mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde (PFH) (1/h) und der zugehörige Performance Level**						
	Kat. B DC_{avg} = keiner	**Kat. 1** DC_{avg} = keiner	**Kat. 2** DC_{avg} = niedrig	**Kat. 2** DC_{avg} = mittel	**Kat. 3** DC_{avg} = niedrig	**Kat. 3** DC_{avg} = mittel	**Kat. 4** DC_{avg} = hoch
1 600							$1{,}42 \times 10^{-9}$ e
1 800							$1{,}26 \times 10^{-9}$ e
2 000							$1{,}13 \times 10^{-9}$ e
2 200							$1{,}03 \times 10^{-9}$ e
2 300							$9{,}85 \times 10^{-10}$ e
2 400							$9{,}44 \times 10^{-10}$ e
2 500							$9{,}06 \times 10^{-10}$ e

ANMERKUNG 1 Wenn für Kategorie 2 die Anforderungsrate geringer oder gleich 1/25 der Testrate ist (siehe 6.1.3.2.4), dann können die PFH–Werte, angegeben in dieser Tabelle für Kategorie 2 und multipliziert mit einem Faktor von 1,1, für die Abschätzung des ungünstigsten Falles benutzt werden.

ANMERKUNG 2 Die Berechnung der PFH–Werte basierte auf dem folgenden DC_{avg}:

— DC_{avg} = niedrig, berechnet mit 60 %;

— DC_{avg} = mittel, berechnet mit 90 %;

— DC_{avg} = hoch, berechnet mit 99 %.

Anhang L
(informativ)

Elektromagnetische Störfestigkeit (EMI)

Die folgenden Pfade (siehe Bild L.1) enthalten Leitlinien zur Umsetzung der Maßnahmen für die elektromagnetische Störfestigkeit (EMI) eines SRP/CS oder von Teilsystemen.

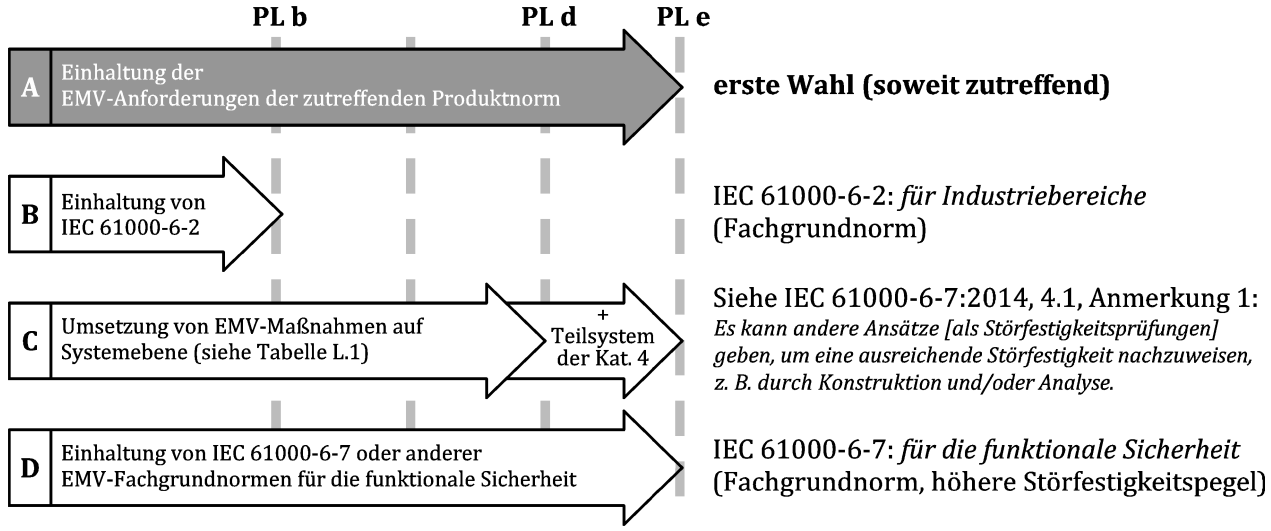


Bild L.1 — Pfade zum Erfüllen der EMI-Maßnahmen

Es sollte mindestens einer der Pfade ausgewählt und vollständig angewendet werden:

— Pfad A: Einhaltung der EMI-Anforderungen der zutreffenden Produktnorm (siehe IEC 61000-6-7:2014, 4.1, erster Satz). Ein Beispiel für eine Produktnorm ist IEC 61800-5-2;

— Pfad B: für PL_r a und b, Einhaltung der EMI-Anforderungen nach IEC 61000-6-2;

— Pfad C: für alle PL_r werden EMI-Maßnahmen durchgeführt, um eine Punktzahl von mindestens 280 (von möglichen 390 Punkten) für zweikanalige Teilsysteme (Kat. 2, Kat. 3 und Kat. 4) und 230 für einkanalige Teilsysteme (Kat. B und Kat. 1) nach Tabelle L.1 (siehe IEC 61000-6-7:2014, 4.1, Anmerkung 1) zu erreichen; für PL_r e kann dieser Pfad nur angewendet werden, wenn die Anforderungen der Kategorie 4 zusätzlich erfüllt werden;

— Pfad D: Einhaltung EMI-Fachgrundnormen bezüglich der funktionalen Sicherheit wie IEC 61000-6-7 oder IEC 61326-3-1.

Für elektromechanische Bauteile mit integrierter aktiver Elektronik sollte die Auswirkung von elektromagnetischen Störungen auf die Ausführung der Sicherheitsfunktionen analysiert werden und die relevanten Maßnahmen zum Erreichen der elektromagnetischen Störfestigkeit sollten umgesetzt werden. Falls Pfad C ausgewählt wird, sollten die in Tabelle L.1 aufgeführten Maßnahmen nach ihrer Wirksamkeit zur Vermeidung oder Beherrschung der Auswirkungen von elektromagnetischen Störungen bewertet werden. Eine ingenieurmäßige Beurteilung sollte belegen (z. B. mithilfe von FMEA-Techniken), dass diese typischen Ursachen für elektromagnetische Störungen soweit wie vernünftigerweise möglich reduziert worden sind. Die ausgewählten Pfade/Maßnahmen sollten eindeutig dokumentiert und mit einem entsprechenden Nachweis der Übereinstimmung mit dem gewählten Pfad belegt werden.

Werden für die Validierung Tests durchgeführt, sollten sie sicherstellen, dass die Sicherheitsfunktion ausgeführt wird und über eine angemessene Dauer eine elektromagnetische Störfestigkeit aufweist, um zu belegen, dass keine Störanfälligkeiten vorhanden sind.

Tabelle L.1 — Maßnahmen zum Erreichen der elektromagnetischen Störfestigkeit für ein SRP/CS oder Teilsystem(e)

Maßnahmen zum Erreichen der elektromagnetischen Störfestigkeit	Punktzahl[a]
Sicherheitsbezogene Sensoren und deren Kabelbaum	
Anwendung der in IEC 60204-1:2016+AMD1:2021, Anhang H und/oder IEC 61800-3 beschriebenen Maßnahmen (hr)	10
Analoge Spannungssignale, Winkelcodierer Abgeschirmte und entweder geerdete oder verdrillte Leitungen oder beides, für Sensoren und sicherheitsbezogene Eingangs-/Ausgangs-Signale (Leitungsabschirmungen sind rundum angeschlossen und in der Nähe der Komponenten niederohmig flach angeschlossen) (hr)	20
Verkabelung der Niederspannungs-Gleichstromversorgung zu den Bauteilen mit verdrilltem Leitungspaar	10
Sicherheitsbezogenes I/O-System (zentral oder dezentral oder in die SPS integriert)	
Eingebaut in einem abgeschirmten und geerdeten Gehäuse oder Bauteile in einem abgeschirmten und geerdeten Gehäuse (hr)	20
Steuerung und/oder spezifische Bauteile sind in Zonen[b] eingeteilt, z. B. a) Netzstromversorgung und Stromverteilung; b) starke Störer wie z. B. Netzsperre, Netzdrosseln, Heizungskomponenten, Hochleistungsversorgungen und Motorleitungen; c) empfindliche Bauteile wie z. B. Niederspannungsversorgung, SPS, Datenbusse, Sensoren und Niederspannungsstellteile. (hr)	20
SPS als Teil des SRP/CS	
Eingebaut in einem abgeschirmten und geerdeten Gehäuse oder Bauteile in einem abgeschirmten und geerdeten Gehäuse	10
Kategorie 3/4 für PL_r d/e mit verschiedenen SPS im selben Gehäuse, getrennt durch einen ausreichenden Abstand zueinander in Übereinstimmung mit den Einbauanleitungen des Herstellers	10[c,d]
Kategorie 3/4 für PL_r d/e mit redundanter SPS in unterschiedlichen Gehäusen	20[c,d]
Kategorie 3/4 für PL_r d/e mit diversen Kanälen (z. B. SPS und diskrete Logik) oder mit Sicherheits-SPS	20[c,d]
Sicherheitsbezogene Aktuatoren und deren Kabelbaum	
Anwendung der in IEC 60204-1:2016+AMD1:2021, Anhang H, beschriebenen Maßnahmen und/oder Anwendung von IEC 61800-3 (hr)	10
Sonstige Bauteile und Verdrahtungen mit maßgebendem Störpegel	
abgeschirmte und ummantelte Kabel für Motoren oder Sinusfilter zwischen Motor und Umrichter oder gleichwertige Maßnahmen in Übereinstimmung mit der Einbauanleitung des Herstellers, sofern zutreffend (hr)	20
RF-Filter, Überspannungs- und Transientenschutz (z. B. Filter, Überspannungs-Suppressordiode, Optokoppler, Ferrite) für sicherheitsbezogene Signale in Übereinstimmung mit der Einbauanleitung des Herstellers, soweit zutreffend (hr)	20
EMI-Filter (entsprechend der Einbauanleitung des Herstellers oder speziell für die Anwendung vorgesehen) für das Stromnetz (z. B. Überspannungs- und Transientenschutz)	20
Anwendung der in IEC 60204-1:2016+AMD1:2021, Anhang H, beschriebenen Maßnahmen und/oder Anwendung von IEC 61800-3	10

Maßnahmen zum Erreichen der elektromagnetischen Störfestigkeit	Punktzahl[a]
Konstruktion, Programmierung, Ausbildung, Beobachtungen während des Einsatzes	
alle Bauteile erfüllen mindestens die Anforderungen der Fachgrundnormen bezüglich der elektromagnetischen Störfestigkeit wie IEC 61000-6-2 (angegeben in der Dokumentation des Herstellers) (hr)	30
Risikoanalyse hinsichtlich elektromagnetischer Störfestigkeit (siehe Beispiel in Tabelle L.2) und Risikobeurteilung mit einem Abschlussbericht	20
Diversitär-redundante Kanäle (siehe ANMERKUNG)	20[c]
Trennung von elektromagnetischen Störquellen und empfindlichen Bauteilen, z. B.: — getrennte Verlegung und Anordnung von Stromleitungen und Signalleitungen; — getrennte Metall-Gehäuse für Hochleistungselektronik und Niederleistungselektronik; — Einhaltung der Anleitungen durch den Hersteller; falls keine Anleitungen vorhanden sind, wird ein Abstand ≥ 20 cm zwischen Leistungsbauteilen und empfindlichen Bauteilen verwendet, oder alternativ werden abgeschirmte und ummantelte Bauteile mit kürzerem Abstand verwendet, von denen erfahrungsgemäß geringe elektromagnetische Störungen ausgehen	30
Software/Firmware mit Diagnosefunktion auf Bauteil- oder Systemebene, z. B. durch Plausibilitätsprüfungen, Daten-Kreuzvergleich im Fall von Redundanz, Selbsttests	20
Konstrukteure besitzen die Erfahrung oder wurden ausgebildet (einschließlich eines Ausbildungsnachweises, z. B. ein Ausbildungszertifikat), damit sie die Ursachen für und die Folgen durch elektromagnetische Störungen nachvollziehen können	20
Wiederverwendung eines spezifischen Entwurfs eines funktionalen Sicherheitssystems, der zuvor in einer ähnlichen elektromagnetischen Umgebung eingesetzt wurde und sich als sehr zuverlässig ohne bekannte EMI-Probleme erwiesen hat	30
Stromversorgung des SRP/CS	
Stromversorgungen mit Niederspannungs-Wechselstrom oder -Gleichstrom mit isolierten Transformatoren nach IEC 61558-2-16, und/oder SELV-Versorgungen nach IEC 60950-1, IEC 62368-1 und/oder SELV- oder PELV-Versorgungen nach EN 50178	20
Redundante SPS mit separatem Schaltnetzteil für das SRP/CS mit Kanal 1/2	10[c]

Gesamtpunktzahl 390 (320 für einkanalige Teilsysteme)	Maßnahmen für die elektromagnetische Störfestigkeit[a]
280 (230 oder besser für einkanalige Teilsysteme)	Anforderungen erfüllt
Unter 280 (230 für einkanalige Teilsysteme)	Verfahren gescheitert ⇒ Auswahl zusätzlicher Maßnahmen oder Auswahl einer oder mehrerer der oben genannten Pfade

ANMERKUNG Duale Kanäle bedeuten in Tabelle L.1 Funktionskanäle und Testkanäle der Kategorie 2 oder redundante Funktionskanäle der Kategorien 3 und 4.
(hr) Diese Maßnahme wird dringend empfohlen. Ist diese Maßnahme anwendbar, wird aber nicht umgesetzt, muss eine ausführliche Begründung gegeben werden, wie die elektromagnetische Störfestigkeit auf gleichwertige Weise erreicht wird.

[a] Wenn technische Maßnahmen nicht relevant sind, können die Punktzahlen in dieser Spalte bei der ausführlichen Berechnung berücksichtigt werden.
[b] Die Zonen können sich innerhalb eines Gehäuses befinden oder auf mehrere Gehäuse aufgeteilt sein.
[c] Die Anforderungen sind nicht maßgebend für einkanalige Teilsysteme.
[d] Die Punktzahl der SPS als Teil des SRP/CS kann nur einmal je SRP/CS erteilt werden.

Tabelle L.2 — Beispiel einer Risikoanalyse für EMI

Störungs-quelle	Phänomen der elektromagnetischen Störung	Abstand Quelle/ Senke	Empfindliches Bauteil	Folge des Risikos	Problemlösung
Energie-versorgung	induktive Kopplung kapazitive Kopplung	< 20 cm	Signalleitungen Sensorleitungen	falsche Messwerte Fehlfunktion	größerer Abstand Abschirmung Filtern geschirmtes Kabel
Wechsel-richter	kapazitive Kopplung	< 40 cm	alle Leitungen alle Sensoren Speicher-programmierbare Logik Analog-Digital-Wandler	sporadischer Ausfall Fehlfunktion Funktionsverlust	größerer Abstand Filtern Sinusfilter geschirmtes Kabel Ferritklemmen
Stromnetz	leitungsgeführte Kopplung kapazitive Kopplung Hochleistungs-transienten	—	Sensor Speicher-programmierbare Logik Motorantrieb	Störung Fehlfunktion Schaden undefinierter Zustand	Netzfilter Spannungsstoßfilter verdrillte Leitung Filtern Transientenschutz
Induktive Lasten	induktive Kopplung leitungsgeführte Kopplung kapazitive Kopplung Hochleistungs-transienten	—	alle Leitungen alle Sensoren Speicher-programmierbare Logik Analog-Digital-Wandler Motorantrieb	Störung Fehlfunktion Schaden undefinierter Zustand	Filtern verdrillte Leitung Transientenschutz
Alle elektro-magnetischen Störungen	alle Kopplungen	—	alle aktiven elektronischen	—	Diagnosesystem führt zu einem sicheren Zustand

Anhang M
(informativ)

Ergänzende Informationen zur Spezifikation der Sicherheitsanforderungen (SRS)

Tabelle M.1 und Tabelle M.2 führen typische Sicherheitsfunktionen und ihre Eigenschaften und sicherheitsbezogenen Parameter auf, indem sie auf andere Internationale Normen verweisen, deren Anforderungen sich auf die Sicherheitsfunktion, die Eigenschaft oder den Parameter beziehen.

Da sich die meisten der in Tabelle M.1 und Tabelle M.2 aufgeführten Sicherheitsfunktionen auf Normen der Elektrotechnik beziehen, müssen die zutreffenden Anforderungen angepasst werden, wenn andere Technologien oder Energiequellen (z. B. hydraulische, pneumatische) verwendet werden.

Tabelle M.1 — Beispiele für Internationale Normen, die auf typische Sicherheitsfunktionen der Maschine und einige ihrer Eigenschaften anwendbar sind

Sicherheitsfunktion/ Eigenschaft	Anforderung(en)		Für ergänzende Informationen siehe
	Dieses Dokument (ISO 13849-1)	ISO 12100:2010	
Sicherheitsbezogene Stopp-Funktion	5.2.2.2	3.26, 6.2.11.3	IEC 60204-1:2016+AMD1:2021, 9.2.2, 9.2.3.3, 9.2.3.6 ISO 14119:2013 ISO 13855:2010 IEC 62046:2018 IEC 61800-5-2:2016
Manuelle Rückstellfunktion	5.2.2.3	—	IEC 62046:2018
Start-/Wiederanlauffunktion	5.2.2.4	6.2.11.3, 6.2.11.4	IEC 60204-1:2016+AMD1:2021, 9.2.3.2, 9.2.3.3, 9.2.3.10 IEC 62046:2018
Lokale Steuerungsfunktion	5.2.2.5	6.2.11.8, 6.2.11.10	IEC 60204-1:2016+AMD1:2021, 10.1.5
Überbrückungsfunktion (en: muting)	5.2.2.6	—	IEC 62046:2018, 5.7
Einrichtung mit Tippbetrieb		6.2.11.8 b)	IEC 60204-1:2016+AMD1:2021, 9.2.3.7
Zustimmfunktion		—	IEC 60204-1:2016+AMD1:2021, 9.2.3.9, 10.9
Verhindern des unerwarteten Anlaufs	—	6.2.11.4	ISO 14118:2017 IEC 60204-1:2016+AMD1:2021, 5.4 IEC 61800-5-2:2016
Befreiung und Rettung eingeschlossener Personen	—	6.3.5.3	ISO 14119:2013, 5.7.5.2
Abtrenn- und Energieableitungsfunktion	—	6.3.5.4	ISO 14118:2017 IEC 60204-1:2016+AMD1:2021, 5.3, 6.3.1
Betriebsartenwahl	5.2.2.9	6.2.11.8, 6.2.11.10	IEC 60204-1:2016+AMD1:2021, 9.2.3.5

Sicherheitsfunktion/ Eigenschaft	Anforderung(en)		Für ergänzende Informationen siehe
	Dieses Dokument (ISO 13849-1)	ISO 12100:2010	
Interaktion zwischen verschiedenen SRP/CS	—	6.2.11.1 (letzter Satz)	IEC 60204-1:2016+AMD1:2021 ISO 11161:2007 ISO 13850:2015
Überwachung der Parametrierung der sicherheitsbezogenen Eingangswerte	7.3	—	—
Funktion zum Stillsetzen im Notfall[a]	—	6.3.5.2	ISO 13850:2015 IEC 60204-1:2016+AMD1:2021, 9.2.3.4.2 IEC 61800-5-2:2016
Überwachung oder Begrenzung der Geschwindigkeit, des Drehmoments, der Leistung, der Position (z. B. Positionsbegrenzungseinrichtung), der Bewegung, des Moments, des Drucks, der Anhaltezeit, des Anhaltewegs	—	—	ISO 10218-1:2011 IEC 61800-5-2:2016 ISO/TS 15066:2016
Sichere Bremsenansteuerung	—	—	IEC 61800-5-2:2016

[a] Für ergänzende Schutzmaßnahme siehe ISO 12100:2010.

Tabelle M.2 — Beispiele für Internationale Normen, die Anforderungen für bestimmte Sicherheitsfunktionen und sicherheitsbezogene Parameter enthalten

Sicherheitsfunktion/ sicherheitsbezogener Parameter	Anforderung		Für ergänzende Informationen siehe
	Dieses Dokument (ISO 13849-1)	ISO 12100:2010	
Ansprechzeit	5.2 13.2	—	ISO 13855:2010, 3.2, A.3, A.4 IEC 62046:2018, 4.4.2.2 ISO 10218-1:2011, Anhang B
Sicherheitsbezogener Parameter, z. B. Geschwindigkeit, Temperatur, Druck, Position oder Moment	5.2	6.2.11.7.3	IEC 60204-1:2016+AMD1:2021, 7.1, 9.3.2 IEC 61800-5-2:2016
Schwankungen, Verlust und Wiederkehr der Energieversorgung	5.2.2.8	6.2.11.4 6.2.11.5	IEC 60204-1:2016+AMD1:2021, 4.3, 7.1, 7.5 ISO 4413:2010 ISO 4414:2010
Anzeigen und Alarme	—	6.2.11.6	ISO 7731:2003 ISO 11428:1996 ISO 11429:1996 IEC 61310-1:2007 IEC 60204-1:2016+AMD1:2021, 10.3, 10.4 IEC 61131-3:2013 IEC 62061:2021

Anhang N
(informativ)

Vermeiden eines systematischen Ausfalls durch den Entwurf von Software

N.1 Auswahl von Maßnahmen zur Fehlervermeidung für den Entwurf von sicherheitsbezogener Software

Die folgenden Tabellen enthalten Leitlinien für die Auswahl von Maßnahmen zur Fehlervermeidung für SRESW oder SRASW. Tabelle N.1 gibt einen Überblick über die Gruppierung zur Auswahl von Maßnahmen. Tabelle N.2 sollte für SRASW in LVL angewendet werden, und Tabelle N.3 sollte für SRESW und SRASW in FVL angewendet werden.

Tabelle N.1 — Gruppierung von Fällen für die Auswahl von Maßnahmen

PL_r	Kategorie	Software verwendet in	Fall
a und b	B	Funktionskanal	Fall 1
a, b und c	2	Testkanal	
a und b	2	Funktionskanal	
a und b	3	bereits bewertete Plattform	
a und b	3	Kanal 1 UND 2	
a, b und c	3	Kanal 1 ODER 2	
c	2	Funktionskanal	Fall 2
c	3	bereits bewertete Plattform	
c	3	Kanal 1 UND 2	
d	2	Testkanal	
d	3 und 4	Kanal 1 ODER 2	
d	2	Funktionskanal	Fall 3
d	3 und 4	bereits bewertete Plattform	
d	3 und 4	Kanal 1 UND 2	
e	3 und 4	Kanal 1 ODER 2	
e	3 und 4	bereits bewertete Plattform	Fall 4[a]
e	3 und 4	Kanal 1 UND 2	

[a] Der einzige Unterschied in den beiden Zeilen von Fall 4 besteht in den Anforderungen an die Toolauswahl.

Legende

— Kanal 1 UND 2: SRESW oder SRASW wird in beiden Funktionskanälen der Kategorie 3 oder 4 ohne Diversität verwendet;

— Kanal 1 ODER 2: SRESW oder SRASW wird nur in einem der beiden Funktionskanäle der Kategorie 3 oder 4 verwendet oder Diversität wird in beiden Funktionskanälen verwendet;

— bereits bewertete Plattform: die Hardware und die interne Software (SRESW) wurden für die Sicherheitsanwendungen entworfen und bereits beurteilt, so dass sie diesem Dokument oder der Normenreihe IEC 61508 oder IEC 62061:2021 für den erforderlichen Performance Level (PL_r) entsprechen.

BEISPIEL Für ein Teilsystem mit PL_r c und Kategorie 2 wird Fall 2 für den Funktionskanal und Fall 1 für den Testkanal ausgewählt.

Die Maßnahmen zur Fehlervermeidung für SRESW und SRASW in Tabelle N.2 und Tabelle N.3 sind nach der Kategorie und dem PL eingeteilt:

a) PL a und PL b werden üblicherweise mithilfe einer Kategorie-B-Struktur und mit Software im Logikblock des Funktionskanals erreicht.

b) PL c und PL d dürfen mithilfe einer Kategorie-2-Struktur mit Software im Logikblock des Funktionskanals oder im Block Testeinrichtung im Testkanal erreicht werden. Für den Testkanal werden die Anforderungen um einen Performance Level reduziert.

c) PL d und PL e dürfen mithilfe einer Kategorie-3-Struktur mit Software im Logikblock des Funktionskanals erreicht werden. „Kanal 1 und Kanal 2“ bedeutet, dass Software in beiden Funktionskanälen verwendet wird. „Kanal 1 oder Kanal 2“ bedeutet, dass Software nur in einem der beiden Funktionskanäle verwendet wird.

d) SRASW in PL d und PL e darf außerdem mithilfe einer bereits bewerteten Plattform erreicht werden (sicherheitsbezogene Hardware in Kombination mit dem Betriebssystem und Programmierungstool). In diesem Fall wird nur eine Anwendungssoftware für beide Funktionskanäle verwendet.

Tabelle N.2 — Auswahl von Maßnahmen für SRASW in LVL

	Fall	Fall 1	Fall 2	Fall 3	Fall 4
1	Diese grundlegenden Maßnahmen sollten angewendet werden:				
a)	Entwicklungslebenszyklus mit Verifizierungs- und Validierungstätigkeiten, siehe Bild 14 a) und Bild 14 b);	m	m	m	m
b)	Dokumentation der Spezifikation und des Entwurfs;				
c)	Modulare und strukturierte Programmierung;				
d)	Funktionstests (z. B. Black-Box-Tests);				
e)	Geeignete Entwicklungsaktivitäten nach Änderungen.				
2	Die Spezifikation der sicherheitsbezogenen Software sollte überprüft werden (siehe auch Anhang J) und jeder Person zur Verfügung stehen, die am Lebenszyklus des V-Modells beteiligt ist, und sollte die Beschreibung enthalten von:				
a)	Sicherheitsfunktionen mit erforderlichem PL und zugehörigen Betriebsarten;	—	m	m	m
b)	Leistungskriterien, z. B. Reaktionszeiten;				
c)	Hardwarearchitektur mit externen Signalschnittstellen; und				
d)	Erkennung und Beherrschung von Hardware-Ausfällen.				
3	Auswahl der Tools, Bibliotheken, Sprachen:				
a)	Tools sollten für die jeweilige Anwendung geeignet sein.	—	m	m	m
b)	Bei einem PL e, der mit einer Komponente und dessen Tool erreicht wird, sollte das Tool der entsprechenden Bauteilnorm entsprechen.	—	—	—	m[a]
c)	Technische Fähigkeiten, um Bedingungen zu erkennen, die zu systematischen Fehlern führen können (wie z. B. Datentyp-Unverträglichkeit, mehrdeutige dynamische Speicherzuordnung, unvollständiger Aufruf von Schnittstellen, Rekursion, Zeigerarithmetik), sollten verwendet werden.	—	m	m	m
d)	Prüfungen sollten hauptsächlich während der Kompilierung durchgeführt werden und nicht nur während der Laufzeit. Tools sollten Sprachenteilmengen und Programmierrichtlinien erzwingen oder mindestens den Entwickler leiten oder führen.				

	Fall	Fall 1	Fall 2	Fall 3	Fall 4
e)	Wann immer angemessen durchführbar, sollten validierte Funktionsblock-Bibliotheken (FB) verwendet werden — entweder vom Werkzeughersteller gelieferte sicherheitsbezogene FB-Bibliotheken oder validierte anwendungsspezifische FB-Bibliotheken in Übereinstimmung mit ISO 13849-1 (dieses Dokument).	—	r	r	r
f)	Eine begründete LVL-Teilmenge, geeignet für ein modulares Verfahren, sollte verwendet werden, z. B. eine anerkannte Teilmenge der IEC 61131-3-Sprachen.				
4	Das Software-Design sollte folgende Merkmale aufweisen:				
a)	semiformale Verfahren zum Beschreiben des Daten- und Steuerungs-signalflusses, z. B. Zustandsdiagramm oder Programmablaufdiagramm;	—	m	m	m
b)	modulare und strukturierte Programmierung, überwiegend realisiert durch die Bereitstellung validierter sicherheitsbezogener Funktionsbaustein-Bibliotheken oder anderer Modulstrukturen zum Erreichen einer einfachen Code-Lesbarkeit und -testfähigkeit;				
c)	Funktionsblöcke mit begrenzter Codelänge;				
d)	innerhalb des Funktionsblocks sollte die Ausführung des Codes mit einem Eingangssprung und einem Ausgangssprung erfolgen;				
e)	dreistufiges Architektur-Modell: Eingänge ⇒ Verarbeitung ⇒ Ausgänge (siehe Bild 10 und Anhang J);				
f)	Zuordnung eines Sicherheitsausgangs an nur einer Stelle im Programm; und				
g)	Verwendung von Techniken zur Detektion von Hardware-Ausfällen und zur defensiven Programmierung innerhalb von Eingangs-, Verarbeitungs- und Ausgangsbausteinen, die zum sicheren Zustand führen.				
5	Wo SRASW und nicht-SRASW in einer Komponente kombiniert werden:				
a)	SRASW und nicht-SRASW sollten in unterschiedlichen Funktionsblöcken codiert werden, mit sorgfältig definierten Datenschnittstellen;	—	m	m	m
b)	es sollte keine logische Verknüpfung von nicht sicherheitsbezogenen und sicherheitsbezogenen Daten geben, die zur Herabstufung der Integrität der sicherheitsbezogenen Signale führen kann, z. B. Verknüpfen eines sicherheits-bezogenen und eines nicht sicherheitsbezogenen Signals durch ein logisches „ODER“, dessen Ausgang sicherheitsbezogene Signale steuert.				
6	Softwareimplementierung/Codierung:				
a)	der Code sollte lesbar, verständlich und testfähig sein, und aufgrund dessen sollten symbolische Variablen (anstelle expliziter Hardwareadressen) angewendet werden;	—	m	m	m
b)	begründete oder akzeptierte Programmierrichtlinien sollten verwendet werden (siehe auch Anhang J);				
c)	Datenintegritäts- und Plausibilitätsprüfungen (z. B. Bereichsüberprüfungen) auf Anwendungsebene (defensive Programmierung) sollten verwendet werden;	—	r	r	r
d)	der Code sollte durch Simulation getestet werden;				
e)	die Verifizierung sollte durch Steuerungssignal- und Datenflussanalyse bei PL d oder e erfolgen.	—	—	r	r
7	Prüfung:				
a)	das angemessene Validierungsverfahren ist der Black-Box-Test des Funktions-verhaltens und der Leistungskriterien (z. B. zeitliches Leistungsverhalten);	—	m	m	m
b)	I/O-Tests sollten sicherstellen, dass die sicherheitsbezogenen Signale in der SRASW korrekt verwendet werden;				

	Fall	Fall 1	Fall 2	Fall 3	Fall 4
c)	eine Testplanung sollte Testfälle mit Abschlussbedingungen und erforderlichen Tools enthalten;	—	r	r	r
d)	für PL d oder e wird eine Testfallausführung auf der Basis von Grenzwertanalysen empfohlen.	—	—	r	r
8	Dokumentation:				
a)	alle Lebenszyklus- und Änderungsaktivitäten sollten dokumentiert werden;	—	m	m	m
b)	die Dokumentation sollte vollständig, verfügbar, lesbar und verständlich sein;				
c)	die Codedokumentation innerhalb des Quelltextes sollte Modulköpfe enthalten mit einer juristischen Person, Funktions- und I/O-Beschreibung, Version der verwendeten Funktionsblock-Bibliothek und ausreichende Kommentierung der Netzwerke/Anweisung und Deklarationszeilen.				
9	Validierung (nur für einen anwendungsspezifischen Code notwendig und nicht für validierte Bibliotheksfunktionen):				
	Die Validierung sollte beispielsweise durch Überprüfung, Inspektion, Walkthrough oder durch andere geeignete Aktivitäten erfolgen.	—	m	m	m
10	Konfigurationsmanagement:				
	Die Einführung von Verfahren und Datensicherung wird besonders empfohlen, um alle Dokumente, Softwaremodule, Ergebnisse der Verifizierung/Validierung und Toolkonfiguration, die im Bezug zu einer bestimmten SRASW stehen, zu identifizieren und zu archivieren.	—	r[b]	r[b]	r[b]
11	Änderungen:				
	Nach Änderungen einer SRASW sollte eine Einflussanalyse zur Sicherstellung der Spezifikation durchgeführt werden. Nach Änderungen sollten angemessene Lebenszyklusaktivitäten stattfinden. Zugriffsrechte auf die Änderungen sollten geprüft und die Änderungshistorie sollte dokumentiert werden. ANMERKUNG 1 Die Änderung betrifft keine Systeme, die bereits in Betrieb sind.	—	m	m	m

[a] Falls zwei verschiedene Komponenten mit unterschiedlichen Tools verwendet werden, darf Betriebsbewährung als ausreichend angenommen werden (für PL e).

[b] Dringend empfohlen.

Legende

— r = empfohlen (en: recommended): die Maßnahme sollte durchgeführt werden, um die Qualität der Software zu verbessern; ihre Durchführung ist nicht verpflichtend, wird sie aber nicht durchgeführt, sollte dies begründet werden;

— m = verpflichtend (en: mandatory) (mit niedriger, mittlerer oder hoher Wirksamkeit, siehe 7.4): diese Maßnahme sollte immer durchgeführt werden;

— „—“: diese Maßnahme ist nicht erforderlich.

Tabelle N.3 — Auswahl von Maßnahmen für SRESW und/oder SRASW in FVL

	Fall	Fall 1	Fall 2	Fall 3	Fall 4
1	Diese grundlegenden Maßnahmen sollten angewendet werden:				
a)	Software-Sicherheitslebenszyklus mit Verifizierung- und Validierungstätigkeiten, siehe Bild 14 a);	m	m	m	m[a]
b)	Dokumentation der Spezifikation und des Designs, z. B. Software-Design-Spezifikation, SSDS, MDS, Codelisten einschließlich Bemerkungen;				

	Fall	Fall 1	Fall 2	Fall 3	Fall 4
c)	modulares und strukturiertes Design und Codierung, z. B. Hierarchie und Einschränkung der Funktionalität, klare Programmstruktur, Definition von Schnittstellen, gut strukturierter Aufrufgraph, Vermeidung von Interrupts, Verwendung von Codierungsrichtlinien;				
d)	Beherrschung systematischer Ausfälle, z. B. Programmablaufüberwachung, Beherrschung von Fehlern im Datenkommunikationsprozess (siehe G.2);				
e)	wenn softwarebasierte Maßnahmen zur Beherrschung zufälliger Hardwareausfälle verwendet werden, wird die korrekte Umsetzung überprüft, z. B. korrekte Umsetzung von Diagnosemaßnahmen, RAM/ROM/CPU-Tests, Hardwaretests, Plausibilitätsprüfungen;				
f)	Funktionstests, z. B. Black-Box-Tests, Verifizierung von korrekten Ausgabedaten basierend auf den Eingabedaten (gültig, ungültig und Grenzwerte), Kompatibilität von Schnittstellen, Zeitvorgaben;				
g)	geeignete Aktivitäten für den Software-Sicherheitslebenszyklus nach Änderungen, z. B. auf der Grundlage einer Einfluss-Analyse.				
2	Diese ergänzenden Maßnahmen sollten angewendet werden:				
a)	Projektmanagement- und Qualitätsmanagementsystem vergleichbar mit beispielsweise der Normenreihe IEC 61508, Definition des Arbeitsablaufs, der Verantwortlichkeiten, Konfigurationsmanagement, Tooleinsatz;	—	m (siehe ANMERKUNG)	m (siehe ANMERKUNG)	m[a]
b)	Dokumentation aller maßgebenden Tätigkeiten während des Software-Sicherheitslebenszyklus, z. B. Dokumentation von Überprüfungen, Tests, Validierung und Verifizierung;				
c)	Konfigurationsmanagement zur Identifizierung aller Konfigurationselemente und Dokumente in Zusammenhang mit einer SRESW-Version, z. B. Versionskontrolle von Codelisten, Modulen, Entwurfsdokumenten, Testplänen, Freigabekontrolle, Archivierung;				
d)	strukturierte Spezifikation der Sicherheitsanforderungen und des Designs;				
e)	Anwendung geeigneter Programmiersprachen und rechnergestützter Werkzeuge mit Betriebsbewährung, z. B. werden Programmierer dahingehend geschult, diese Tools zu verwenden;				
f)	modulare und strukturierte Programmierung, Abgrenzung von der nicht sicherheitsbezogenen Software, beschränkte Modulgrößen mit vollständig definierten Schnittstellen, Verwendung von Design- und Codierungsrichtlinien;				
g)	Verifizierung der Codierung durch Walk-through/Überprüfen mit Kontrollflussanalyse (zur Überprüfung auf Fehler, Qualität der Kommentare, Einhaltung der Codierungsrichtlinien, Klarheit, Lesbarkeit, Vollständigkeit);				
h)	erweiterte Funktionstests, z. B. Grey-Box-Tests, Leistungstests oder Simulationen, z. B. Verwendung von nicht spezifizierten Eingabedaten, extremen Umgebungsbedingungen, Volllast, Tests basierend auf Kenntnissen der internen Codierung;				
i)	Einflussanalyse und angemessene Software-Sicherheitslebenszyklus-Aktivitäten nach Änderungen;				

	Fall	Fall 1	Fall 2	Fall 3	Fall 4
j)	die SRESW für Komponenten mit PL_r e sollte mit den Anforderungen von IEC 61508-3:2010, Abschnitt 7, geeignet für SIL 3, übereinstimmen.	—	—	—	m[a]

[a] Wenn Diversität in Spezifikation, Design und Codierung verwendet wird, kann für die beiden Kanäle des SRP/CS in Kategorie 3 oder 4 mit den oben erwähnten grundlegenden und ergänzenden Maßnahmen für PLr c oder d ein PLr e erreicht werden.

ANMERKUNG Für SRESW mit Diversität im Design und in der Codierung kann für die Komponenten des SRP/CS in Kategorie 3 oder 4 oder in Testkanälen der Kategorie 2 der Aufwand in Verbindung mit den zu treffenden Maßnahmen zur Vermeidung systematischer Ausfälle vermindert werden durch z. B. Überprüfung von Teilen der Software nur durch Berücksichtigung der strukturellen Aspekte, statt durch Prüfen jeder Zeile.

Legende

— m = verpflichtend (en: mandatory) (mit niedriger, mittlerer oder hoher Wirksamkeit, siehe 7.4): diese Maßnahme sollte immer durchgeführt werden;

— „—“: diese Maßnahme ist nicht erforderlich.

N.2 Beispiel für eine Software-Validierung

N.2.1 Allgemeines

Der Zweck der Validierung ist es, zu bestätigen, dass die Software allen Softwareanforderungen entspricht (siehe V-Modell, Bild 14). Die Validierung erfolgt durch eine Kombination aus Inspektion (z. B. Analyse) und Prüfung und sollte in einem frühen Stadium des Lebenszyklus geplant werden.

Die in diesem Beispiel dargestellte Validierung basiert auf zuvor beurteilten Softwaremodulen. Die Validierung erfolgt durch Testfälle an den Eingängen der zuvor beurteilten Softwaremodule, um deren Anwendung im Kontext der gesamten Anwendungssoftware zu überprüfen. Es werden nur grundlegende Testfälle als Beispiele dargestellt. Die Anzahl der Testfälle für reale Anwendungen ist möglicherweise zu erhöhen.

Die Prüfung erfordert eine Planung einschließlich einer Prüfspezifikation, die das Prüfverfahren und die zu verwendende Ausrüstung umfasst. Die tatsächlichen Prüfergebnisse sind mit dem Prüfplan abzugleichen.

N.2.2 Codierungsrichtlinien

Die Codierung sollte entsprechend den Codierungsrichtlinien erfolgen, die der Hersteller der Softwareplattform vorschreibt, soweit zutreffend. Alternativ sollte die Codierung nach einer „hausinternen Richtlinie“ erfolgen, ohne jedoch den vom Hersteller der verwendeten Softwareplattform vorgeschriebenen Richtlinien zu widersprechen.

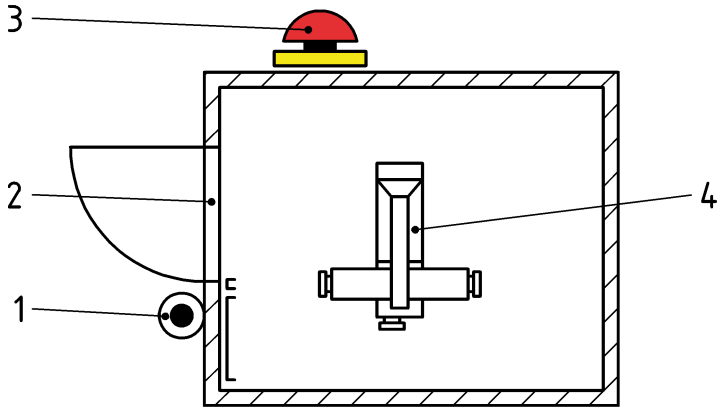
N.2.3 Spezifikation der Sicherheitsfunktionen

Die Sicherheitsfunktion und Ergänzungen arbeiten wie folgt (siehe Bild N.1):

— Wenn Tür 1 der verriegelnden trennenden Schutzeinrichtung (GD1) geöffnet wird (zugänglicher Bereich), dann wird M1 abgeschaltet (PL_r = PL d). Der Status von GD1 wird durch Quittierung mit der Taste ACK1 zurückgesetzt. Das Rücksetzen mit der Quittiertaste ACK1 ist nur möglich, wenn GD1 geschlossen ist.

— Das Betätigen des Not-Halt-Tasters (ES1) löst ein STO von Motor M1 aus (PL_r = PL d). ES1 wird mit dem Taster ACK1 quittiert. Eine Quittierung ist nur möglich, wenn ES1 entriegelt ist.

ANMERKUNG Für Anforderungen an die Rückstellfunktion siehe 5.2.2.3 Manuelle Rückstellfunktion.



Legende
1 ACK1 — Quittiertaste für Tür 1 der verriegelnden trennenden Schutzeinrichtung (zugänglicher Bereich) und Not-Halt 1
2 GD1 — Tür 1 der verriegelnden trennenden Schutzeinrichtung
3 ES1 — Not-Halt-Taster 1
4 M1 — Motor 1 mit STO (sicher abgeschaltetes Drehmoment) angehalten

Bild N.1 — Beispielanwendung

N.2.4 Eingangsinformationen aus der Spezifikation des Hardware-Entwurfs

Die entsprechenden Bauteile für den Hardware-Entwurf der Steuerung sind (siehe Bild N.2):

— Tür der verriegelnden trennenden Schutzeinrichtung GD1;

— Not-Halt-Taster ES1;

— Quittiertaste ACK1;

— sicherheitsbezogene CPU von K1;

— sicherheitsbezogene I/O-Karte(n) von K1;

— Feldbus, der eine funktionale sicherheitsbezogene Kommunikation nach der Normenreihe IEC 61784 ermöglicht;

— sicherheitsbezogener Umrichter T1 (nach IEC 61800-5-2) für Motor M1.

Wenn alle sicherheitsbezogenen Anforderungen des Herstellers der Sicherheits-SPS (K1) umgesetzt wurden, reicht das vereinfachte V-Modell aus, siehe Bild 14 b).

Diese Bauteile bilden bereits entworfene Teilsysteme, die vom Bauteilhersteller bereitgestellt werden.

Der Umrichter (Antrieb T1) liefert die integrierte sicherheitsbezogene Teilfunktion STO (sicher abgeschaltetes Drehmoment) nach IEC 61800-5-2.

ANMERKUNG Die Parametrierung des Umrichters ist im Allgemeinen auch Gegenstand dieses Dokuments und des Validierungsprozesses, wird aber in diesem Beispiel nicht gezeigt.

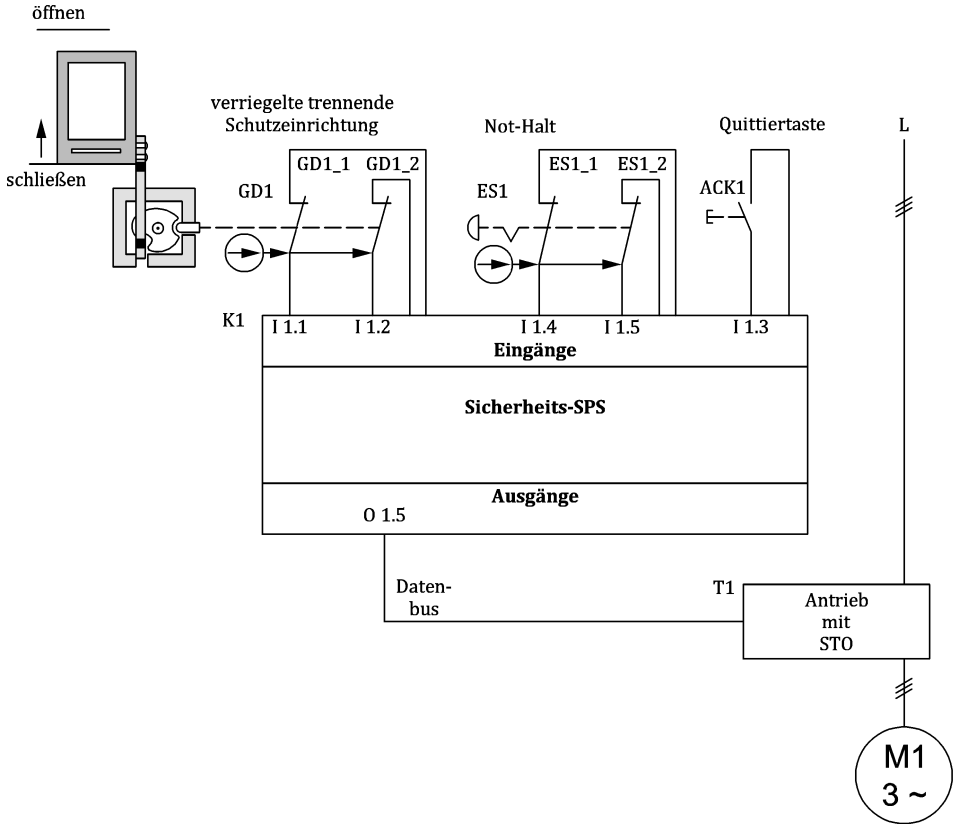
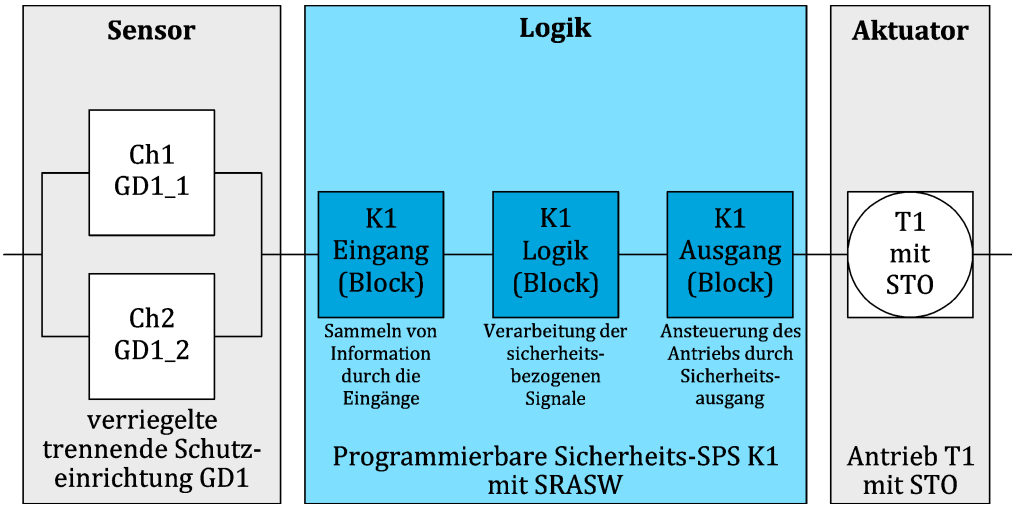


Bild N.2 — Hardware-Übersicht

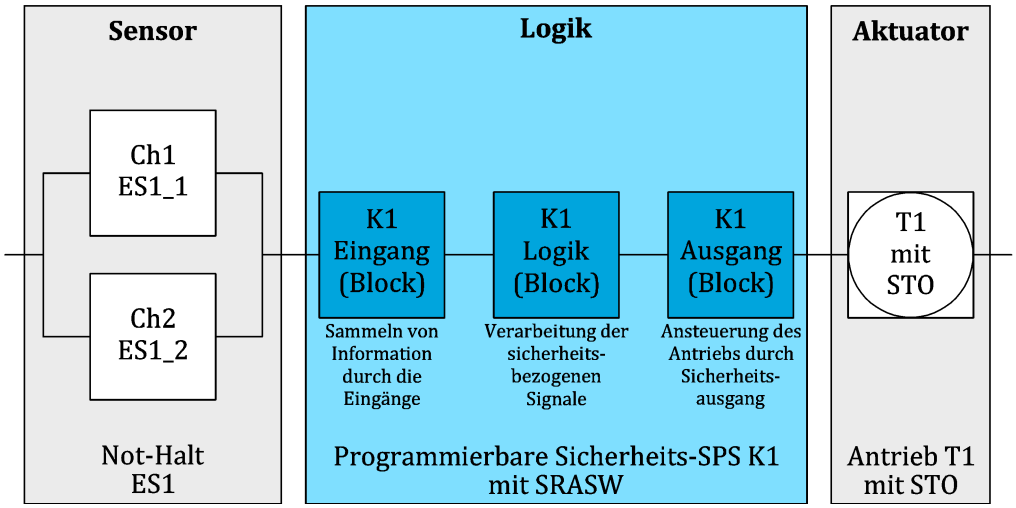
Tabelle N.4 zeigt die maßgebenden Signale zur Ausführung der Sicherheitsfunktion und der ergänzenden Funktion, die je nach Hardware-Verdrahtung und Software-Implementierung gesteuert und geprüft werden sollten.

In Bild N.3, Bild N.4 und Bild N.5 sind die sicherheitsbezogenen Blockdiagramme dargestellt.



SF1: Wenn Tür 1 der verriegelnden trennenden Schutzeinrichtung geöffnet wird, dann wird M1 vom Umrichter (Antrieb T1) in STO geschaltet.

Bild N.3 — SF1 (Verriegelung)



SF2: Not-Halt 1 löst ein STO von Motor M1 durch den Umrichter (Antrieb T1) aus.

Bild N.4 — SF2 (Not-Halt)

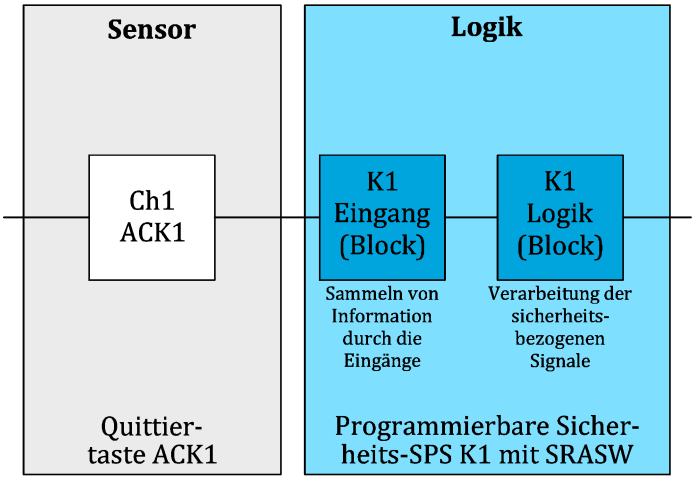


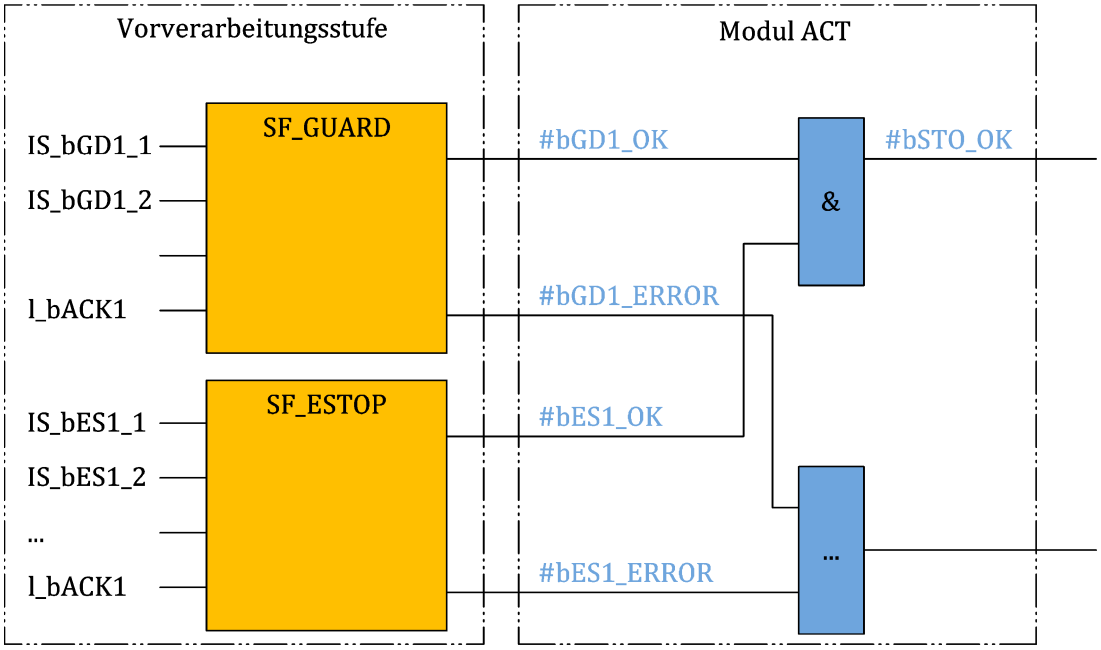
Bild N.5 — Rückstellfunktion

Tabelle N.4 — Validierung der Verdrahtung und Hardware von Eingangs-/Ausgangssignalen

Liste der Eingangssignale			
Beschreibung (Funktion, Signal)	**Variable (Bezeichnung)**	**Adresse (Bezeichnung)**	**Sind Verdrahtung und Hardware-Adresse korrekt?**
GD1_1, Kontakt 1 (NC)	IS_bGD1_1	I1.1	□ Ja □ Nein
GD1_2, Kontakt 2 (NC)	IS_bGD1_2	I1.2	□ Ja □ Nein
ES1_1, Kontakt 1 (NC)	IS_bES1_1	I1.4	□ Ja □ Nein
ES1_2, Kontakt 2 (NC)	IS_bES1_2	I1.5	□ Ja □ Nein
ACK1, Quittierkontakt (NO)	I_bACK1	I1.3	□ Ja □ Nein
Liste der Ausgangssignale			
M1, STO	QS_bM1_STO	O1.5	□ Ja □ Nein

N.2.5 Anwendungsprogramm

Bild N.6 zeigt das Anwendungsprogramm (SRASW), das in der Sicherheits-SRS K1 eingesetzt wurde, basierend auf zuvor bewerteten Softwaremodulen (Funktionsblöcken).



ANMERKUNG 1 #bSTO_OK wird vom Feldbus mithilfe eines Sicherheitsprotokolls zum Umrichter (Antrieb 1) übertragen.

ANMERKUNG 2 Die Anzeige und Fehlerbehandlung ist anwendungsspezifisch und wird in diesem Beispiel nicht berücksichtigt.

Bild N.6 — Anwendungsprogramm (SRASW), das in der Sicherheits-SRS K1 eingesetzt wurde, basierend auf zuvor bewerteten Softwaremodulen (Funktionsblöcken)

N.2.6 Validierung der eingesetzten SRASW

N.2.6.1 Allgemeines

Die auf zuvor bewerteten Softwaremodulen basierende Validierung kann wie folgt unterteilt werden:

a) Bewertung der verriegelnden trennenden Schutzeinrichtung;

b) Bewertung des Not-Halts;

c) Bewertung der Freigabe/der Abschaltung von Motor M1;

d) Dokumentation.

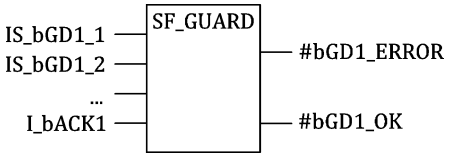
Eine Validierung der zuvor bewerteten Softwaremodule ist nicht erforderlich. Die hier dargestellte Validierung sollte belegen, dass das Anwendungsprogramm als Ganzes seine Softwarespezifikation erfüllt, einschließlich der Parametrierung und Konfiguration der zuvor bewerteten Softwaremodule.

N.2.6.2 Bewertung der verriegelnden trennenden Schutzeinrichtung

In Tabelle N.5 sind Testfälle zur Durchführung einer FMEA und Tests der verriegelnden trennenden Schutzeinrichtung aufgeführt. Test 1 in Tabelle N.5 ist ein Funktionstest ohne Fehlereinspeisung. Test 2 und Test 3 simulieren ständige HIGH-Signale an einem der Kontakte, die mit der verriegelnden trennenden Schutzeinrichtung verbunden sind. Test 4 und Test 5 simulieren ständige LOW-Signale an einem dieser Kontakte. Test 6 und Test 7 simulieren Signalwechsel beider Kontakte außerhalb der festgelegten Zeitdifferenz. Test 8 simuliert ein Festhängen des Quittierungskontakts bei einem Fehler (permanent HIGH). Für alle acht Testfälle werden die korrekten Antworten von #bGD1_OK und #bGD1_ERROR validiert.

Tabelle N.5 — FMEA und Tests der verriegelnden trennenden Schutzeinrichtung

Relevante Eingänge				
Signal	I/O	Typ	Information	Bemerkungen
GD1 Ch1: IS_bGD1_1 (Türsicherheitsschalter)	I1.1	logisch	Zeitdifferenz zwischen Kanal 1 und Kanal 2 0,5 s	Verriegelnde trennende Schutzeinrichtung NC (Zwangsöffnung)
GD1 Ch2: IS_bGD1_2 (Türsicherheitsschalter)	I1.2	logisch	Zeitdifferenz zwischen Kanal 1 und Kanal 2 0,5 s	Verriegelnde trennende Schutzeinrichtung NC (Zwangsöffnung)
ACK1: I_bACK1 (Rücksetzen)	I1.3	logisch	NO	Gemeinsames Quittierungssignal in Verbindung mit der verriegelnden trennenden Schutzeinrichtung GD1
Maßgebende Merker				
Signal		Typ	Information	Bemerkungen
Interne Kennzeichnung #bGD1_OK		logisch	NO	Dieser Freigabemerker wird für die nachfolgende Verarbeitung verwendet.
Interne Kennzeichnung #bGD1_ERROR		logisch	NO	Dieser Fehlermerker wird für die nachfolgende Verarbeitung verwendet.
Verwendete Software-Blöcke				
Name		Zuvor beurteilter Block der Software-Plattform	Beschreibung	Software-Block-Darstellung

SF_GUARD	ja	Zuvor beurteilter Software-Block für die Überwachung der verriegelnden trennenden Schutzeinrichtung. Vergleich der beiden GD1-Signale. Der beurteilte GD1-Status wird über #bGD1_OK signalisiert. Wird ein Fehler erkannt, ändert sich der #bGD1_ERROR-Merker in HIGH.	

Testfälle (Ausfalleffektanalyse)

Nr.	Test oder Fehlereinspeisung	Erwartetes Ergebnis Sicherer Zustand und Reaktion auf einen Fehler	Testergebnis
1	Funktionstest ohne Fehlereinspeisung und ohne zu erwartende Reaktion auf einen Fehler: Wenn die Sicherheitsfunktion angefordert wird (durch Öffnen der Tür der verriegelnden trennenden Schutzeinrichtung), dann ist IS_bGD1_1 = LOW und IS_bGD1_2 = LOW.	#bGD1_OK = LOW und #bGD1_ERROR = LOW. Das HIGH-Signal von #bGD1_OK wird erst nach Schließen von GD1 und Drücken von ACK1 wiederhergestellt.	□ Ja □ Nein
ANMERKUNG 1 Fehlerfreier Zustand (Ausgangssituation/Normalzustand vor Durchführung der Tests, die Tür der verriegelnden trennenden Schutzeinrichtung ist geschlossen).			
2	Dauerhaftes HIGH-Signal auf IS_bGD1_1 (I.1.1) Wenn die Sicherheitsfunktion angefordert wird (durch Öffnen der verriegelnden trennenden Schutzeinrichtung), dann ändert sich nur IS_bGD1_2 zu LOW	Sicherer Zustand mit #bGD1_OK = LOW und eingeleitete Reaktion auf einen Fehler #bGD1_ERROR = LOW ändert sich zu #bGD1_ERROR = HIGH Block SF_GUARD kann nicht quittiert werden Nachdem GD1 geschlossen wurde, kann Block SF_GUARD immer noch nicht quittiert werden. SF_GUARD kann nur durch einen Signalwechsel von ACK1 nach Reparatur und „HIGH – LOW – HIGH“-Signalwechsel für IS_bGD1_1 und IS_bGD1_2 quittiert werden.	□ Ja □ Nein
ANMERKUNG 2 Übertragungsfehler I1.1.			

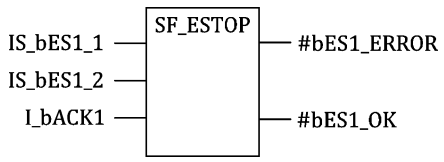
3	Dauerhaftes HIGH-Signal auf IS_bGD1_2 (I1.2). Wenn die Sicherheitsfunktion angefordert wird (durch Öffnen der verriegelnden trennenden Schutzeinrichtung), dann ändert sich nur IS_bGD1_1 zu LOW	Sicherer Zustand mit #bGD1_OK = LOW und eingeleitete Reaktion auf einen Fehler #bGD1_ERROR = LOW ändert sich zu #bGD1_ERROR = HIGH Block SF_GUARD kann nicht quittiert werden Nachdem GD1 geschlossen wurde, kann Block SF_GUARD immer noch nicht quittiert werden. SF_GUARD kann nur durch einen Signalwechsel von ACK1 nach Reparatur und „HIGH – LOW – HIGH“-Signalwechsel für IS_bGD1_1 und IS_bGD1_2 quittiert werden.	□ Ja □ Nein
ANMERKUNG 3 Übertragungsfehler I1.2.			
4	LOW-Signal an IS_bGD1_1 (I1.1) GD1 ist geschlossen, so dass IS_bGD1_2 HIGH ist	Sicherer Zustand mit #bGD1_OK = LOW und eingeleitete Reaktion auf einen Fehler #bGD1_ERROR = LOW ändert sich zu #bGD1_ERROR = HIGH Der Block SF_GUARD kann nicht quittiert werden, auch wenn GD1 geöffnet und wieder geschlossen wird.	□ Ja □ Nein
ANMERKUNG 4 Übertragungsfehler I1.1.			
5	LOW-Signal an IS_bGD1_2 (I1.2) GD1 ist geschlossen, so dass IS_bGD1_1 HIGH ist	Sicherer Zustand mit #bGD1_OK = LOW und eingeleitete Reaktion auf einen Fehler #bGD1_ERROR = LOW ändert sich zu #bGD1_ERROR = HIGH Der Block SF_GUARD kann nicht quittiert werden, auch wenn GD1 geöffnet und wieder geschlossen wird.	□ Ja □ Nein
ANMERKUNG 5 Übertragungsfehler I1.2.			

6	IS_bGD1_1 (I1.1) ändert den Signalstatus außerhalb der eingestellten Zeitdifferenz in IS_bGD1_2	Sicherer Zustand mit #bGD1_OK = LOW und eingeleitete Reaktion auf einen Fehler #bGD1_ERROR = LOW ändert sich zu #bGD1_ERROR = HIGH Block SF_GUARD kann nicht quittiert werden Nachdem GD1 geschlossen wurde, kann Block SF_GUARD immer noch nicht quittiert werden. SF_GUARD kann nur durch einen Signalwechsel von ACK1 nach Reparatur und „HIGH – LOW – HIGH“-Signalwechsel für IS_bGD1_1 und IS_bGD1_2 quittiert werden.	□ Ja □ Nein
ANMERKUNG 6 Diese Diagnosefunktion dient zum Schutz vor Manipulation.			
7	IS_bGD1_2 (I1.2) ändert den Signalstatus außerhalb der eingestellten Zeitdifferenz in IS_bGD1_1	Sicherer Zustand mit #bGD1_OK = LOW und eingeleitete Reaktion auf einen Fehler #bGD1_ERROR = LOW ändert sich zu #bGD1_ERROR = HIGH Block SF_GUARD kann nicht quittiert werden Nachdem GD1 geschlossen wurde, kann Block SF_GUARD immer noch nicht quittiert werden. SF_GUARD kann nur durch einen Signalwechsel von ACK1 nach Reparatur und „HIGH – LOW – HIGH“-Signalwechsel für IS_bGD1_1 und IS_bGD1_2 quittiert werden.	□ Ja □ Nein
ANMERKUNG 7 Diese Diagnosefunktion dient zum Schutz vor Manipulation.			
8	Dauerhaftes HIGH-Signal auf ACK1 (I1.3)	Sicherer Zustand mit #bGD1_OK = LOW Keine Quittierung möglich.	□ Ja □ Nein
ANMERKUNG 8 Eine Quittierung ist flankengesteuert und nicht pegelgesteuert. Diese Diagnosefunktion ist eine Vorbeugungsmaßnahme zum Schutz vor Manipulation.			

N.2.6.3 Bewertung des Not-Halts

In Tabelle N.6 sind Testfälle zur Durchführung einer FMEA und Tests der Not-Halt-Funktion aufgeführt. Test 1 in Tabelle N.6 ist ein Funktionstest ohne Fehlereinspeisung. Test 2 und Test 3 simulieren ständige HIGH-Signale an einem der Kontakte, die mit der Not-Halt-Funktion verbunden sind. Test 4 und Test 5 simulieren ständige LOW-Signale an einem dieser Kontakte. Test 6 und Test 7 simulieren Signalwechsel beider Kontakte außerhalb der festgelegten Zeitdifferenz. Test 8 simuliert ein Festhängen des Quittierungskontakts bei einem Fehler (permanent HIGH). Für alle acht Testfälle werden die korrekten Antworten von #bES1_OK und #bES1_ERROR validiert.

Tabelle N.6 — FMEA und Tests der Not-Halt-Funktion

Relevante Eingänge				
Signal	I/O	Typ	Information	Bemerkungen
ES1 Channel1: IS_bES1_1 Not-Halt	I1.4	logisch	Zeitdifferenz zwischen Kanal 1 und Kanal 2 0,5 s	Not-Halt NC (Zwangsöffnung)
ES1 Channel2: IS_bES1_2 Not-Halt	I1.5	logisch	Zeitdifferenz zwischen Kanal 1 und Kanal 2 0,5 s	Not-Halt NC (Zwangsöffnung)
ACK1: I_bACK1 Rücksetzen	I1.3	logisch	NO	Gemeinsames Quittierungssignal für Not-Halt ES1
Relevante Ausgänge/Merker				
Signal		Typ	Information	Bemerkungen
#bES1_OK		logisch	NO	Dieser Freigabemerker wird für die nachfolgende Verarbeitung verwendet.
#bES1_ERROR		logisch	NO	Dieser Fehlermerker wird für die nachfolgende Verarbeitung verwendet.
Verwendete Software-Blöcke				
Name		Zuvor beurteilter Block der Software-Plattform	Beschreibung	Information
SF_ESTOP		ja	Zuvor beurteilter Software-Block für die Überwachung eines Zweikanalsignals Vergleich der beiden ES1-Signale. Der beurteilte ES1-Status wird über #bES1_OK signalisiert. Im Fall eines Fehlers wird #bES1_ERROR auf HIGH gesetzt	

Testfälle (Ausfalleffektanalyse)			
Nr.	Test oder Fehlereinspeisung	Erwartetes Ergebnis Sicherer Zustand und Reaktion auf einen Fehler	Testergebnis
1	Funktionstest ohne Fehler-einspeisung und ohne zu erwartende Reaktion auf einen Fehler: wenn der Not-Halt ausgelöst wird, ist IS_bES1_1 = LOW und IS_bES1_2 = LOW.	#bES1_OK = LOW und #bES1_ERROR = LOW Das HIGH-Signal von #bES1_OK wird erst nach Entriegeln von ES1 und Drücken von I_bACK1 wiederhergestellt.	□ Ja □ Nein
ANMERKUNG 1 Fehlerfreier Zustand (Ausgangssituation/Normalzustand vor Durchführung der Prüfungen, Not-Halt wird nicht angefordert).			
2	Dauerhaftes HIGH-Signal auf IS_bES1_1 (I1.4) wenn der Not-Halt ausgelöst wird, ändert sich nur IS_bES1_2 zu LOW	Sicherer Zustand mit #bES1_OK = LOW und eingeleitete Reaktion auf einen Fehler #bES1_ERROR = LOW ändert sich zu #bES1_ERROR = HIGH Der Block SF_ESTOP kann nicht quittiert werden Nachdem ES1 entriegelt wurde, kann Block SF_ESTOP immer noch nicht quittiert werden. SF_ESTOP kann nur durch einen Signalwechsel von ACK1 nach Reparatur und „HIGH – LOW – HIGH"-Signalwechsel für IS_bES1_1 and IS_bES1_2 quittiert werden.	□ Ja □ Nein
ANMERKUNG 2 Übertragungsfehler I1.4.			
3	Dauerhaftes HIGH-Signal auf IS_bES1_2 (I1.5). Wenn der Not-Halt ausgelöst wird, ändert sich nur IS_bES1_1 zu LOW	Sicherer Zustand mit #bES1_OK = LOW und eingeleitete Reaktion auf einen Fehler #bES1_ERROR = LOW ändert sich zu #bES1_ERROR = HIGH Der Block SF_ESTOP kann nicht quittiert werden Nachdem ES1 entriegelt wurde, kann Block SF_ESTOP immer noch nicht quittiert werden. SF_ESTOP kann nur durch einen Signalwechsel von ACK1 nach Reparatur und „HIGH – LOW – HIGH"-Signalwechsel für IS_bES1_1 and IS_bES1_2 quittiert werden.	□ Ja □ Nein
ANMERKUNG 3 Übertragungsfehler I1.5.			

4	LOW-Signal an IS_bES1_1 (I1.4). ES1 ist entriegelt, so dass IS_bES1_2 HIGH ist	Sicherer Zustand mit #bES1_OK = LOW und eingeleitete Reaktion auf einen Fehler #bES1_ERROR = LOW ändert sich zu #bES1_ERROR = HIGH Der Block SF_ESTOP kann nicht quittiert werden, auch nicht, wenn ES1 betätigt und wieder entriegelt wird.	□ Ja □ Nein
ANMERKUNG 4 Übertragungsfehler I1.4.			
5	LOW-Signal an IS_bES1_2 (I1.5). ES1 ist entriegelt, so dass IS_bES1_1 HIGH ist	Sicherer Zustand mit #bES1_OK = LOW und eingeleitete Reaktion auf einen Fehler #bES1_ERROR = LOW ändert sich zu #bES1_ERROR = HIGH Der Block SF_ESTOP kann nicht quittiert werden, auch nicht, wenn ES1 betätigt und wieder entriegelt wird.	□ Ja □ Nein
ANMERKUNG 5 Übertragungsfehler I1.5.			
6	IS_bES1_1 (I1.4) ändert den Signalstatus außerhalb der eingestellten Zeitdifferenz in IS_bES1_2	Sicherer Zustand mit #bES1_OK = LOW und eingeleitete Reaktion auf einen Fehler #bES1_ERROR = LOW ändert sich zu #bES1_ERROR = HIGH Der Block SF_ESTOP kann nicht quittiert werden Nachdem ES1 entriegelt wurde, kann Block SF_ESTOP immer noch nicht quittiert werden. SF_ESTOP kann nur durch einen Signalwechsel von ACK1 nach Reparatur und „HIGH – LOW – HIGH“-Signalwechsel für IS_bES1_1 and IS_bES1_2 quittiert werden.	□ Ja □ Nein
ANMERKUNG 6 Diese Diagnosefunktion wird angewendet, um das Betätigungselement für den Not-Halt zu überprüfen.			

7	IS_bES1_2 (I1.5) ändert den Signalstatus außerhalb der eingestellten Zeitdifferenz in IS_bES1_1	Sicherer Zustand mit #bES1_OK = LOW und eingeleitete Reaktion auf einen Fehler #bES1_ERROR = LOW ändert sich zu #bES1_ERROR = HIGH Der Block SF_ESTOP kann nicht quittiert werden Nachdem ES1 entriegelt wurde, kann Block SF_ESTOP immer noch nicht quittiert werden. SF_ESTOP kann nur durch einen Signalwechsel von ACK1 nach Reparatur und „HIGH – LOW – HIGH"-Signalwechsel für IS_bES1_1 and IS_bES1_2 quittiert werden.	□ Ja □ Nein
ANMERKUNG 7 Diese Diagnosefunktion wird angewendet, um das Betätigungselement für den Not-Halt zu überprüfen.			
8	Dauerhaftes HIGH-Signal auf ACK1 (I1.3)	Sicherer Zustand mit #bES1_OK = LOW Keine Quittierung möglich.	□ Ja □ Nein
ANMERKUNG 8 Eine Quittierung ist flankengesteuert und nicht pegelgesteuert. Diese Diagnosefunktion ist eine Vorbeugungsmaßnahme zum Schutz vor Manipulation.			

N.2.6.4 Bewertung der verriegelnden trennenden Schutzeinrichtung und des Not-Halts mit Motor M1

Tabelle N.7 — FMEA und Tests der Freigabe/Abschaltung von Motor M1

Relevante Eingänge/relevante Merker			
Signal	Typ	Information	Bemerkungen
#bGD1_OK (Variable)	logisch	NO	Dieser Freigabemerker wird für die nachfolgende Verarbeitung verwendet.
#bES1_OK (Variable)	logisch	NO	Dieser Freigabemerker wird für die nachfolgende Verarbeitung verwendet.

Verwendete Software-Blöcke			
Name	zuvor beurteilter Block der Software-Plattform	Beschreibung	Information
Modul ACT	nein	Verwendung von UND wie in Bild N.6 gezeigt	Siehe Modul ACT in Bild N.6

Relevante Ausgänge/Merker				
Beschreibung	O	Typ	Information	Beschreibung
#bSTO_OK	Q1.5	BUS	zuvor beurteilt nach PL d	über Sicherheitsbus zum Umrichter (Antrieb 1), aktiviert STO

Testfälle (Ausfalleffektanalyse)			
Nr.	Test oder Fehlereinspeisung	Erwartetes Ergebnis	Testergebnis
1	Einspeisen eines Fehlers, der zu #bGD1_ERROR = HIGH führt	anwendungsspezifische Fehlerbehandlung	□ Ja □ Nein
ANMERKUNG 1 Falls ein Fehler #bGD1_ERROR vorliegt, dann sollte der Umrichter (Antrieb 1) ebenfalls abschalten.			
2	Einspeisen eines Fehlers, der zu #bES1_ERROR = HIGH führt	anwendungsspezifische Fehlerbehandlung	□ Ja □ Nein
ANMERKUNG 2 Falls ein Fehler #bES1_ERROR vorliegt, dann sollte der Umrichter (Antrieb) ebenfalls abschalten.			
3	Funktionstest. #bGD1_OK = HIGH und #bES1_OK = HIGH	#bSTO_OK = HIGH	□ Ja □ Nein
ANMERKUNG 3 Dies ist ein fehlerfreier Zustand.			
4	Funktionstest durch Betätigung von ES1, während GD1 geschlossen ist. #bGD1_OK = HIGH und #bES1_OK = LOW	#bSTO_OK = LOW	□ Ja □ Nein
ANMERKUNG 4 Dies ist ein fehlerfreier Zustand.			
5	Funktionstest durch Öffnen von GD1, während ES1 entriegelt ist. #bGD1_OK = LOW und #bES1_OK = HIGH	#bSTO_OK = LOW	□ Ja □ Nein
ANMERKUNG 5 Dies ist ein fehlerfreier Zustand.			
6	Funktionstest durch Öffnen von GD1 und Betätigen von ES1. #bGD1_OK = LOW und #bES1_OK = LOW	#bSTO_OK = LOW	□ Ja □ Nein
ANMERKUNG 6 Dies ist ein fehlerfreier Zustand.			
7	Fehler in der Feldbus-Kommunikation zwischen PLC K1 und Umrichter (Antrieb 1). Ernster Fehler (z. B. sollte im Fall eines ernsten Fehlers die Steuerung neu gestartet werden). Falls ein Fehler in der Feldbus-Kommunikation vorliegt, dann sollte der Umrichter (Antrieb) ebenfalls abschalten.	anwendungsspezifische Fehlerbehandlung	□ Ja □ Nein

N.2.6.5 Dokumentation

Dieses Dokument legt zusätzliche Anforderungen für die Validierung fest, z. B. Softwarespezifikation(en), Softwarerichtlinien, Nachweise, dass die Software so entworfen ist, dass sie den erforderlichen PL erreicht, Nachweise, dass die Software den geforderten DC unterstützt, und Dokumentation über Maßnahmen gegen systematische Ausfälle im Zusammenhang mit der Software. Die Validierung umfasst außerdem die Analyse dieser Aspekte. Tabelle N.8 enthält keine Einzelheiten für alle diese Aspekte, weshalb eine weiterführende Dokumentation notwendig ist.

Tabelle N.8 — Dokumentation der Überprüfung des Softwarecodes

	Verweisung	Korrekt
Entspricht die Software den sicherheitstechnischen Programmierregeln?	Siehe …	□ Ja □ Nein
Entspricht der Entwurf der Steuerung der Software?	Siehe …	□ Ja □ Nein
Korrekte Parametrierung der Funktionsblöcke?	Siehe …	□ Ja □ Nein
Korrekte Parametrierung der Eingangssignale?	Siehe …	□ Ja □ Nein
Korrekte Parametrierung der Ausgangssignale?	Siehe …	□ Ja □ Nein
Entspricht die Architektur des Sicherheitsprogramms der Spezifikation?	Siehe …	□ Ja □ Nein
Entspricht die Spezifikation der Sicherheitssoftware der Spezifikation der Sicherheitsfunktion?	Siehe …	□ Ja □ Nein
Defensiven Programmierung?	Siehe …	□ Ja □ Nein
Kein negativer Einfluss durch ODER-Funktionen?	Siehe …	□ Ja □ Nein
Kein negativer Einfluss durch Negierungen?	Siehe …	□ Ja □ Nein
…		□ Ja □ Nein
Datum:		
Name:		
Software-signatur:		
Hardware-signatur:		

Anhang O
(informativ)

Sicherheitsbezogene Werte von Bauteilen oder Komponenten der Steuerungen

O.1 Definition der Gerätetypen

O.1.1 Allgemeines

Die Geräte unterscheiden sich in Bezug auf Technologie, Anwendung, Verfügbarkeit und Einsatz von Diagnosemechanismen und Diagnoseinformationen. Deshalb werden an dieser Stelle verschiedene Gerätetypen definiert.

ANMERKUNG 1 Für weitere Informationen siehe VDMA 66413.

Die Geräte können im Allgemeinen anhand folgender Merkmale unterschieden werden:

— ein Gerät, das direkt als ein SRP/CS oder Teilsystemelement in einer Sicherheitsfunktion verwendet werden kann, da der Hersteller das Gerät bereits für diese spezifische Anwendung entwickelt hat (Gerätetyp 1 und Gerätetyp 4);

— ein Gerät, das durch den Gestaltungsprozess des Benutzers als ein SRP/CS oder Teilsystemelement definiert und beurteilt wird (Gerätetyp 2 und Gerätetyp 3).

ANMERKUNG 2 Eine Sicherheitsfunktion nutzt üblicherweise verschiedene Gerätetypen. Gerätetypen sind nicht zu verwechseln mit Typen nach z. B. ISO 14119 und der Normenreihe IEC 61496.

Tabelle O.1 — Charakteristische Werte der Gerätetypen

<table>
<tr><th>Charakteristischer Wert</th><th colspan="4">Gerätetyp</th><th>Bemerkung</th></tr>
<tr><th></th><th>1</th><th>2</th><th>3</th><th>4</th><th></th></tr>
<tr><td>PL</td><td rowspan="2">X</td><td></td><td></td><td></td><td>ISO 13849-1 (dieses Dokument)</td></tr>
<tr><td>SIL</td><td></td><td></td><td></td><td>IEC 62061:2021</td></tr>
<tr><td>PFH</td><td>X</td><td></td><td></td><td></td><td>ISO 13849-1 (dieses Dokument) und IEC 62061:2021</td></tr>
<tr><td>Kategorie</td><td>X</td><td>X</td><td>X</td><td></td><td>ISO 13849-1 (dieses Dokument)</td></tr>
<tr><td>HFT</td><td>X</td><td>X</td><td>X</td><td></td><td>IEC 62061:2021</td></tr>
<tr><td>$MTTF_D$</td><td></td><td rowspan="4">X</td><td></td><td></td><td rowspan="4">ISO 13849-1 (dieses Dokument) und IEC 62061:2021
Einer der charakteristischen Werte ist erforderlich.</td></tr>
<tr><td>λ_D</td><td></td><td></td><td></td></tr>
<tr><td>MTTF</td><td></td><td></td><td></td></tr>
<tr><td>MTBF</td><td></td><td></td><td></td></tr>
<tr><td>B_{10D}</td><td></td><td></td><td rowspan="2">X</td><td></td><td rowspan="2">ISO 13849-1 (dieses Dokument) und IEC 62061:2021
Einer der charakteristischen Werte ist erforderlich.</td></tr>
<tr><td>B_{10}</td><td></td><td></td><td></td></tr>
</table>

Charakteristischer Wert	Gerätetyp				Bemerkung
	1	2	3	4	
RDF		O[b]	O[b]		ISO 13849-1 (dieses Dokument)
SFF					IEC 62061:2021[a]
T_{10D}		X		X	ISO 13849-1 (dieses Dokument) und IEC 62061:2021
T_M	X				

[a] SFF (Anteil sicherer Ausfälle, en: safe failure fraction) wird in IEC 62061:2021, 3.2.54, definiert als der Anteil an der Gesamtausfallrate eines Teilsystems, der nicht zu einem gefahrbringenden Ausfall führt.

[b] Wenn der Hersteller keine Werte für $MTTF_D$ oder B_{10D} bereitstellt.

Legende
X obligatorisch
O optional

O.1.2 Gerätetyp 1

Gerätetyp 1 besitzt den höchsten Integrationsgrad. Typisch sind bereits entworfene Sicherheitssysteme mit integrierter Diagnosefunktion. Der SIL oder PL dieses Typs wird je nach Verwendungszweck eingestuft. Die Einstufung wird vom Gerätehersteller vorgenommen.

Geräte dieses Typs werden in Übereinstimmung mit Sicherheitsnormen (z. B. der Normenreihe IEC 61508) entwickelt.

ANMERKUNG 1 Beispiele für Gerätetyp 1: Sicherheitslichtschranke, Sicherheitslichtgitter, Bauteile von sicherheitsbezogenen Steuerungen, Antriebe mit integrierten Sicherheitsfunktionen, Sicherheitsrelais.

ANMERKUNG 2 Die Parameter können von anderen anwendungsspezifischen Daten abhängig sein (z. B. Begrenzung der maximalen Schalthäufigkeit).

O.1.3 Gerätetyp 2

Ergänzende Anwendungsdaten (Struktur des Schaltkreises, DC und Betrachtung von CCF) werden vom Benutzer benötigt, um eine Sicherheitsfunktion zu beurteilen.

Geräte dieses Typs werden nicht zwingend in Übereinstimmung mit Sicherheitsnormen entwickelt; dadurch wird jedoch die Anwendung nach diesem Dokument nicht ausgeschlossen.

BEISPIEL Für Gerätetyp 2: Operationsverstärker, Näherungsschalter, Drucksensor, Hydraulikventil.

ANMERKUNG Einige Geräte können Bauteile enthalten, deren Ausfallarten von den Betriebszyklen abhängen, und andere Bauteile, die von den Betriebszyklen nahezu unabhängig sind. Es liegt im Ermessen des Herstellers, ob er ein solches Gerät als Typ 1, 2 oder 3 definiert und welche Kennwerte und Anwendungsgrenzen er dem Anwender vorgibt. Beispiele sind die Kombination eines $MTTF_D$-Wertes mit einer Begrenzung auf eine maximale Anzahl von Betriebszyklen oder die Kombination eines B_{10D}-Wertes mit einer Begrenzung eines minimalen n_{op}-Wertes, der für die Anwendung von Gleichung (C.1) verwendet werden muss.

O.1.4 Gerätetyp 3

Geräte vom Typ 3 sind Bauteile mit einer Ausfallart, die von den Betriebszyklen abhängig ist.

Ergänzende Anwendungsdaten (Anzahl der Bedienungen, Anzahl der Aktivierungen, Schaltungsstruktur, DC und Betrachtung von CCF) werden vom Benutzer benötigt, um eine Sicherheitsfunktion zu beurteilen.

Geräte dieses Typs werden nicht zwingend in Übereinstimmung mit Sicherheitsnormen entwickelt; dadurch wird jedoch die Anwendung nach diesem Dokument nicht ausgeschlossen.

BEISPIEL Für Gerätetyp 3: elektromechanische Bauteile, die Verschleiß unterliegen, z. B. Leistungsschütze, Schalter, Pneumatikventile, Verriegelungseinrichtungen, Steuerungseinrichtungen.

O.1.5 Gerätetyp 4

Gerätetyp 4 ist ein Sonderfall von Gerätetyp 1. Dieser Typ hat nicht-zufällige Ausfälle, die zu einem gefährlichen Fehler führen, d. h. die Wahrscheinlichkeit, dass ein gefährlicher Fehler nahe PFH auftritt, ist 0. Für Bauteiles dieses Typs gilt einer der folgenden Punkte für jeden potenziellen Fehler:

— der Fehlerausschluss erfolgt in Übereinstimmung mit diesem Dokument; oder

— ein Fehler führt immer zu einem sicheren Zustand.

Wenn Architekturanforderungen oder andere Überlegungen eine Beschränkung zur alleinigen (einkanaligen) Verwendung auferlegen, muss ein maximal erreichbarer PL und SIL für die einkanalige Verwendung angegeben werden.

Um die oben genannten Informationen anzugeben, müssen die Geräte in Übereinstimmung mit den Sicherheitsnormen (z. B. der Normenreihe IEC 61508) beurteilt werden.

O.2 Zusätzliche Informationen

O.2.1 Software

Wird im Bauteil eine Software verwendet, sollte der Gerätehersteller Angaben zur Eignung der Software entsprechend dem PL bereitstellen.

O.2.2 Grundlegende Sicherheitsprinzipien

Für Bauteile der Kategorie B bis Kategorie 4 sollte der Gerätehersteller Angaben darüber machen, ob das Bauteil entsprechend den grundlegenden Sicherheitsprinzipien entworfen und hergestellt wurde.

O.2.3 Bewährte Sicherheitsprinzipien

Für Bauteile der Kategorie 1 bis Kategorie 4 sollte der Gerätehersteller Angaben darüber machen, ob das Bauteil entsprechend den bewährten Sicherheitsprinzipien entworfen und hergestellt wurde.

Literaturhinweise

[1] ISO/IEC Guide 51:2014, *Safety aspects — Guidelines for their inclusion in standards*

[2] ISO 4413:2010, *Hydraulic fluid power — General rules and safety requirements for systems and their components*

[3] ISO 4414:2010, *Pneumatic fluid power — General rules and safety requirements for systems and their components*

[4] ISO 7731:2003, *Ergonomics — Danger signals for public and work areas — Auditory danger signals*

[5] ISO 8573-1, *Compressed air — Part 1: Contaminants and purity classes*

[6] ISO 9000:2015, *Quality management systems — Fundamentals and vocabulary*

[7] ISO 9001:2015, *Quality management systems — Requirements*

[8] ISO 9241-210, *Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems*

[9] ISO 10218-1:2011, *Robots and robotic devices — Safety requirements for industrial robots — Part 1: Robots*

[10] ISO 10218-2, *Robots and robotic devices — Safety requirements for industrial robots — Part 2: Robot systems and integration*

[11] ISO 11161:2007, *Safety of machinery — Integrated manufacturing systems — Basic requirements*

[12] ISO 11428:1996, *Ergonomics — Visual danger signals — General requirements, design and testing*

[13] ISO 11429:1996, *Ergonomics — System of auditory and visual danger and information signals*

[14] ISO 13850:2015, *Safety of machinery — Emergency stop function — Principles for design*

[15] ISO 13851, *Safety of machinery — Two-hand control devices — Principles for design and selection*

[16] ISO 13856-1, *Safety of machinery — Pressure-sensitive protective devices — Part 1: General principles for design and testing of pressure-sensitive mats and pressure-sensitive floors*

[17] ISO 13856-2, *Safety of machinery — Pressure-sensitive protective devices — Part 2: General principles for design and testing of pressure-sensitive edges and pressure-sensitive bars*

[18] ISO 14118:2017, *Safety of machinery — Prevention of unexpected start-up*

[19] ISO 14119:2013, *Safety of machinery — Interlocking devices associated with guards — Principles for design and selection*

[20] ISO/TR 14121-2, *Safety of machinery — Risk assessment — Part 2: Practical guidance and examples of methods*

[21] ISO/TS 15066:2016, *Robots and robotic devices — Collaborative robots*

[22] ISO 16090-1, *Machine tools safety — Machining centres, Milling machines, Transfer machines — Part 1: Safety requirements*

[23] ISO 19973 (alle Teile), *Pneumatic fluid power — Assessment of component reliability by testing*

[24] ISO/TR 22100-2:2013, *Safety of machinery — Relationship with ISO 12100 — Part 2: How ISO 12100 relates to ISO 13849-1*

[25] ISO/TR 22100-3, *Safety of machinery — Relationship with ISO 12100 — Part 3: Implementation of ergonomic principles in safety standards*

[26] ISO/TR 22100-4, *Safety of machinery — Relationship with ISO 12100 — Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects*

[27] ISO 23125, *Machine tools — Safety — Turning machines*

[28] ISO/IEC/IEEE 26512, *Systems and software engineering — Requirements for acquirers and suppliers of information for users*

[29] EN 614-1, *Sicherheit von Maschinen — Ergonomische Gestaltungsgrundsätze — Teil 1: Begriffe und allgemeine Leitsätze*

[30] EN 1005-3, *Sicherheit von Maschinen — Menschliche körperliche Leistung — Teil 3: Empfohlene Kraftgrenzen bei Maschinenbetätigung*

[31] EN 50178, *Ausrüstung von Starkstromanlagen mit elektronischen Betriebsmitteln*

[32] IEC 60204-1:2016+AMD1:2021, *Safety of machinery — Electrical equipment of machines — Part 1: General requirements*

[33] IEC 60447, *Basic and safety principles for man-machine interface (MMI) — Actuating principles*

[34] IEC 60050-192:2015, *International electrotechnical vocabulary — Part 192: Dependability*

[35] IEC 60529, *Degrees of protection provided by enclosures (IP code)*

[36] IEC 60812, *Analysis techniques for system reliability — Procedure for failure mode and effects analysis (FMEA)*

[37] IEC 60947 (alle Teile), *Low-voltage switchgear and controlgear*

[38] IEC 60950-1, *Information technology equipment —- Safety — Part 1: General requirements*

[39] IEC 61000-1-2, *Electromagnetic compatibility (EMC) — Part 1-2: General — Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena*

[40] IEC 61000-6-2, *Electromagnetic compatibility (EMC) — Part 6-2: Generic standards — Immunity for industrial environments*

[41] IEC 61000-6-7:2014, *Electromagnetic compatibility (EMC) — Part 6-7: Generic standards — Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations*

[42] IEC 61025, *Fault tree analysis (FTA)*

[43] IEC 61078, *Reliability block diagrams*

[44] IEC 61300 (alle Teile), *Fibre optic interconnecting devices and passive components — Basic test and measurement procedures*

[45] IEC 61310 (alle Teile), *Safety of machinery — Indication, marking and actuation*

[46] IEC 61131-3:2013, *Programmable controllers — Part 3: Programming languages*

[47] IEC 61310-1:2007, *Safety of machinery — Indication, marking and actuation — Part 1: Requirements for visual, acoustic and tactile signals*

[48] IEC 61326-3-1, *Electrical equipment for measurement, control and laboratory use — EMC requirements — Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) — General industrial applications*

[49] IEC 61496-1:2020, *Safety of machinery — Electro-sensitive protective equipment — Part 1: General requirements and tests*

[50] IEC 61496-2, *Safety of machinery — Electro-sensitive protective equipment — Part 2: Particular requirements for equipment using active opto-electronic protective devices*

[51] IEC 61496-3, *Safety of machinery — Electro-sensitive protective equipment — Part 3: Particular requirements for active opto-electronic protective devices responsive to diffuse reflection (AOPDDR)*

[52] IEC 61506, *Industrial-process measurement and control — Documentation of software for process control systems and facilities*

[53] IEC 61508-1, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements*

[54] IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

[55] IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations*

[56] IEC 61508-5, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 5: Examples of methods for the determination of safety integrity levels*

[57] IEC 61508-6:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

[58] IEC 61508-7:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures*

[59] IEC 61511-1:2016, *Functional safety — Safety instrumented systems for the process industry sector — Part 1: Framework, definitions, system, hardware and application programming requirements*

[60] IEC 61558-2-16, *Safety of transformers, reactors, power supply units and combinations thereof - Part 2-16: Particular requirements and tests for switch mode power supply units and transformers for switch mode power supply units for general applications*

[61] IEC 61709,[2] *Electric components — Reliability — Reference conditions for failure rates and stress models for conversion*

[62] IEC 61784 (alle Teile), *Industrial communication networks — Profiles*

[63] IEC 61800-3, *Adjustable speed electrical power drive systems — Part 3: EMC requirements and specific test methods*

[64] IEC 61800-5-2:2016, *Adjustable speed electrical power drive systems — Part 5-2: Safety requirements — Functional*

[65] IEC 61810-2-1, *Electromechanical elementary relays — Part 2-1: Reliability — Procedure for the verification of B_{10} values*

[66] IEC 61810-3, *Electromechanical elementary relays — Part 3: Relays with forcibly guided (mechanically linked) contacts*

[67] IEC 62021 (alle Teile), *Insulating liquids — Determination of acidity*

[68] IEC 62024 (alle Teile), *High frequency inductive components — Electrical characteristics and measuring methods*

[69] IEC 62368-1, *Audio/video, information and communication technology equipment — Part 1: Safety requirements*

[70] IEC 62502, *Analysis techniques for dependability — Event tree analysis (ETA)*

[71] IEC/TR 63074, *Safety of machinery — Security aspects related to functional safety of safety-related control systems*

[72] EN 50495:2010, *Sicherheitseinrichtungen für den sicheren Betrieb von Geräten im Hinblick auf Explosionsgefahren*

[73] ANSI B11.26:2018 *Functional Safety for Equipment: General Principles for the Design of Safety Control Systems Using ISO 13849-1*

[74] SN 29500 (alle Teile), *Failure rates of components, Edition 1999-11, Siemens AG 1999s*

[75] VDMA 66413, *Funktionale Sicherheit — Universelle Datenbasis für sicherheitsbezogene Kennwerte von Komponenten oder Teilen von Steuerungen*

[76] VDMA 24584:2020, *Sicherheitsfunktionen geregelter und nicht geregelter (fluid-)mechanischer Systeme*

[77] Goble W.M. Control systems Safety Evaluation and Reliability. 3rd Edition:2010 (ISBN-101934394807)

[78] IFA-Report 2/2017e, *Functional safety of machine controls — Application of ISO 13849*, German Social Accident Insurance (DGUV), June 2009, ISBN 978-3-88383-793-2, kostenloser Download im Internet: www.dguv.de/ifa/13849e

2 Identisch mit RDF 2000/*Reliability Data Handbook*, UTE C 80-810, Union Technique de l'Electricité et de la Communication.

[79] CHINNIAH YUVIN, (2015) Analysis and prevention of serious and fatal accidents related to moving parts of machinery, Safety Science 75 (2015) 163–173

[80] HAGHIGHI A., JOCELYN S., CHINNIAH Y. "Testing and Improving an ISO 14119-Inspired Tool to Prevent Bypassing Safeguards on Industrial Machines"; Safety, volume 6, issue 3, 2020 https://www.mdpi.com/2313-576X/6/3/42

[81] IFA. "*SISTEMA Cookbook 6: Definition of safety functions: what is important?*" (https://www.dguv.de/webcode.jsp?query=e109249)

[82] *Reliability Prediction of Electronic Equipment, MIL-HDBK 217E*, Notice-2, Department of Defense, Washington, DC, 1995

[83] *British Handbook for Reliability Data for Components used in Telecommunication Systems*, British Telecom (HRD5, last issue)

[84] Chinese Military Standard, GJB/Z 299C-2006 *Reliability prediction handbook for electronic equipment (English Version)*

[85] *EMC The easy way*, Pocket guide, published by Division of Switching Devices, Switchboards and Industrial Controls of the ZVEI (German Electrical and Electronic Manufacturer's Association), Frankfurt/Main, Germany (https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2008/Januar/EMC-Pocket-Guide-ZVEI-english.pdf)