DIN EN ISO 13849-1

DIN

ICS 13.110

Entwurf

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

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

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

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

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2021-07-09 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

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

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

Gesamtumfang 332 Seiten

DIN-Normenausschuss Sicherheitstechnische Grundsätze (NASG)

www.din.de
www.beuth.de
3271637

Nationales Vorwort

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

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

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

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

IEC 60204-1:2016	siehe	DIN EN 60204-1 (VDE 0113-1):2019-06
IEC 60447	siehe	DIN EN 60447 (VDE 0196)
IEC 60529:1989+AMD2:2013	siehe	DIN EN 60529 (VDE 0470-1):2014-09
IEC 60812	siehe	DIN EN 60812
IEC 60947 (all parts)	siehe	DIN EN 60947 (VDE 0660) (alle Teile)
IEC 61000-1-2:2016	siehe	DIN EN 61000-1-2:2017-07
IEC 61000-6-2:2016	siehe	DIN EN IEC 61000-6-2:2019-11
IEC 61000-6-7:2014	siehe	DIN EN 61000-6-7 (VDE 0839-6-7):2015-12
IEC 61078:2016	siehe	DIN EN 61078:2018-03
IEC 61131-3:2013	siehe	DIN EN 61131-3:2014-06
IEC 61300 (all parts)	siehe	DIN EN 61300-1 (VDE 0885-300) (alle Teile)
IEC 61310 (all parts)	siehe	DIN EN 61310 (VDE 0113) (alle Teile)
IEC 61310-1:2007	siehe	DIN EN 61310-1 (VDE 0113-101):2008-09
IEC 61326-3-1:2017	siehe	DIN EN 61326-3-1 (VDE 0843-20-3-1):2018-04
IEC 61496-1	siehe	DIN EN 61496-1 (VDE 0113-201)
IEC 61508-1:2010	siehe	DIN EN 61508-1 (VDE 0803-1):2011-02
IEC 61508-2:2010	siehe	DIN EN 61508-2 (VDE 0803-2):2011-02
IEC 61508-3:2010	siehe	DIN EN 61508-3 (VDE 0803-3):2011-02
IEC 61508-4:2010	siehe	DIN EN 61508-4 (VDE 0803-4):2011-02
IEC 61508-5:2010	siehe	DIN EN 61508-5 (VDE 0803-5):2011-02
IEC 61508-6:2010	siehe	DIN EN 61508-6 (VDE 0803-6):2011-02
IEC 61508-7:2010	siehe	DIN EN 61508-7 (VDE 0803-7):2011-02
IEC 61800-3:2017	siehe	DIN EN IEC 61800-3 (VDE 0160-103):2019-04

IEC 61800-5-2:2016	siehe	DIN EN 61800-5-2 (VDE 0160-105-2):2017-11
IEC 61810 (all parts)	siehe	DIN EN IEC 61810 (VDE 0435) (alle Teile)
IEC 62046:2018	siehe	DIN EN IEC 62046 (VDE 0113-211):2019-03
IEC 62061:2005+AMD1:2012	siehe	DIN EN 62061 (VDE 0113-50):2016-05
ISO 4413:2010	siehe	DIN EN ISO 4413:2011-04
ISO 4414:2010	siehe	DIN EN ISO 4414:2011-04
ISO 7731	siehe	DIN EN ISO 7731
ISO 9001	siehe	DIN EN ISO 9001
ISO 9355-1:1999	siehe	DIN EN 894-1:1997-04*
ISO 9355-2:1999	siehe	DIN EN 894-2:1997-04**
ISO 9355-3:2006	siehe	DIN EN 894-3:2000-06***
ISO 10218-1:2011	siehe	DIN EN ISO 10218-1:2012-01
ISO 10218-2:2011	siehe	DIN EN ISO 10218-2:2012-06
ISO 11161:2007	siehe	DIN EN ISO 11161:2010-10
ISO 12100:2010	siehe	DIN EN ISO 12100:2011-03
ISO 13849-2:2012	siehe	DIN EN ISO 13849-2:2013-02
ISO 13850:2015	siehe	DIN EN ISO 13850:2016-05
ISO 13851:2019	siehe	DIN EN ISO 13851:2019-11
ISO 13855:2010	siehe	DIN EN ISO 13855:2010-10
ISO 13856-1:2013	siehe	DIN EN ISO 13856-1:2013-08
ISO 13856-2:2013	siehe	DIN EN ISO 13856-2:2013-08
ISO 14118:2017	siehe	DIN EN ISO 14118:2018-07
ISO 14119:2013	siehe	DIN EN ISO 14119:2014-03
ISO 16090 1:2017	siehe	DIN EN ISO 16090-1:2019-12
ISO 20607:2019	siehe	DIN EN ISO 20607:2019-10
ISO 23125:2015	siehe	DIN EN ISO 23125:2015-04
ISO/TR 14121-2:2012	siehe	DIN ISO/TR 14121-2 (DIN SPEC 33885):2013-02
ISO/TR 22100-2:2013	siehe	DIN ISO/TR 22100-2 (DIN SPEC 33887):2014-09
ISO/TR 22100-4	siehe	DIN CEN ISO/TR 22100-4
IEC/TR 63074	siehe	DIN IEC/TR 63074 (VDE 0113 74)

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

---

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

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

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

Änderungen

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

a) Verweisungen überarbeitet und aktualisiert;

b) normative Verweisungen und Begriffe und Definitionen überarbeitet;

c) Integration eines Abschnitts zur Risikobeurteilung (Abschnitt 4);

d) Anforderungen an die Spezifikation der Sicherheitsfunktion überarbeitet (Abschnitt 5);

e) Beschreibung der Anforderungen an das Design und die verschiedenen Performance Levels (Abschnitt 6);

f) Integration eines neuen Abschnittes (7) zu Softwaresicherheit;

g) Integration eines neuen Abschnittes (9) zu Ergonomieaspekten;

h) detaillierte Beschreibung von Validierungsprozessen (Abschnitt 10);

i) Integration von Anhang L zu Immunitätsanforderungen für elektromagnetische Kompatibilität;

j) Integration von Anhang M mit zusätzlichen Informationen für das SRS-System;

k) Integration von Anhang N zur Vermeidung von systematischen Fehlern im Software-Design;

l) Integration von Anhang O mit Beschreibung der sicherheitsbezogene Werte von Komponenten oder Teilen der Steuerungen.

Nationaler Anhang NA
(informativ)

Literaturhinweise

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

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

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

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

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

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

DIN EN 60529 (VDE 0470-1): 2014-09, *Schutzarten durch Gehäuse (IP-Code) (IEC 60529:1989 + A1:1999 + A2:2013); Deutsche Fassung EN 60529:1991 + A1:2000 + A2:2013*

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

DIN EN 60947 (alle Teile), *Niederspannungsschaltgeräte*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

DIN EN ISO 9001, *Qualitätsmanagementsysteme — Anforderungen*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

DIN ISO/TR 22100-2 (DIN SPEC 33887):2014-09, *Sicherheit von Maschinen — Beziehung zu ISO 12100 — Teil 2: Wie ISO 12100 und ISO 13849-1 zusammenhängen (ISO/TR 22100-2:2013)*

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

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

– Entwurf –

2021-07

prEN ISO 13849-1:2021

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

Inhalt

Seite

Europäisches Vorwort

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

Dieses Dokument ist derzeit zur zweiten parallelen Umfrage vorgelegt.

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

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

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

Anerkennungsnotiz

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

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

Anhang ZA
(informativ)

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

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

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

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

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

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

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

Vorwort

ISO (die Internationale Organisation für Normung) ist eine weltweite Vereinigung nationaler Normungsinstitute (ISO Mitgliedsorganisationen). Die Erstellung von Internationalen Normen wird üblicherweise von Technischen Komitees von ISO durchgeführt. Jede Mitgliedsorganisation, die Interesse an einem Thema hat, für welches ein Technisches Komitee gegründet wurde, hat das Recht, in diesem Komitee vertreten zu sein. Internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO stehen, nehmen ebenfalls an der Arbeit teil. ISO arbeitet bei allen elektrotechnischen Normungsthemen eng mit der Internationalen Elektrotechnischen Kommission (IEC) zusammen.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Es sollten insbesondere die unterschiedlichen Annahmekriterien für die verschiedenen ISO-Dokumentenarten beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents).

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

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

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

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

Die wesentlichen Änderungen im Vergleich zur Vorgängerausgabe sind folgende Neuerungen:

— Spezifikation der Sicherheitsfunktionen (Abschnitt 5);

— Software (Abschnitt 7);

— Validierung (Abschnitt 10);

— Kombination von mehreren Teilsystemen;

— Management der funktionalen Sicherheit (G.5);

— elektromagnetische Störfestigkeit (Anhang L);

— ergänzende Informationen für die Spezifikation der Sicherheitsanforderungen (Anhang M);

— Vermeiden von Fehlern/Maßnahmen zur Fehlervermeidung für den sicherheitsbezogenen Softwareentwurf (Anhang N);

— sicherheitsbezogene Werte von Bauteilen oder Komponenten der Steuerungen (Anhang O).

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

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

Einleitung

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

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

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

Die dritte Ausgabe wurde 2015 geändert und veröffentlicht.

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

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

— Maschinenhersteller (kleine, mittlere und große Unternehmen);

— Organisationen des Arbeits- und Gesundheitsschutzes (Gesetzgeber, Unfallversicherungen, Marktaufsicht).

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

— Maschinenanwender/Arbeitgeber (kleine, mittlere und große Unternehmen);

— Maschinenanwender/Arbeitnehmer (z. B. Gewerkschaften);

— Dienstleister (kleine, mittlere und große Unternehmen), z. B. für die Instandhaltung;

— Verbraucher (falls die behandelten Maschinen für die Nutzung durch Verbraucher bestimmt sind).

Den oben genannten Interessengruppen wurde die Möglichkeit eingeräumt, am Erarbeitungsprozess dieses Dokuments mitzuwirken.

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

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

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

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

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

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

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

Dieses Dokument ist maßgebend für die Sicherheitsfunktionen eines SRP/CS, die ausgeführt werden, um Risiken abzudecken, für die eine Risikobeurteilung nach ISO 12100 erforderlich ist. ISO 12100 legt fest, dass eine risikomindernde Maßnahme notwendig ist, die auf einer Sicherheitsfunktion beruht (z. B. verriegelte trennende Schutzeinrichtung). In solchen Fällen muss die sicherheitsbezogene Steuerung eine Sicherheitsfunktion ausführen. Dieses Dokument sollte bei der Gestaltung und Bewertung der sicherheitsbezogenen Teile der Steuerung angewendet werden. Nur derjenige Teil der Steuerung, der in Bezug zur Sicherheit steht (sicherheitsbezogen ist), wird vom Anwendungsbereich dieses Dokuments abgedeckt.

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

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

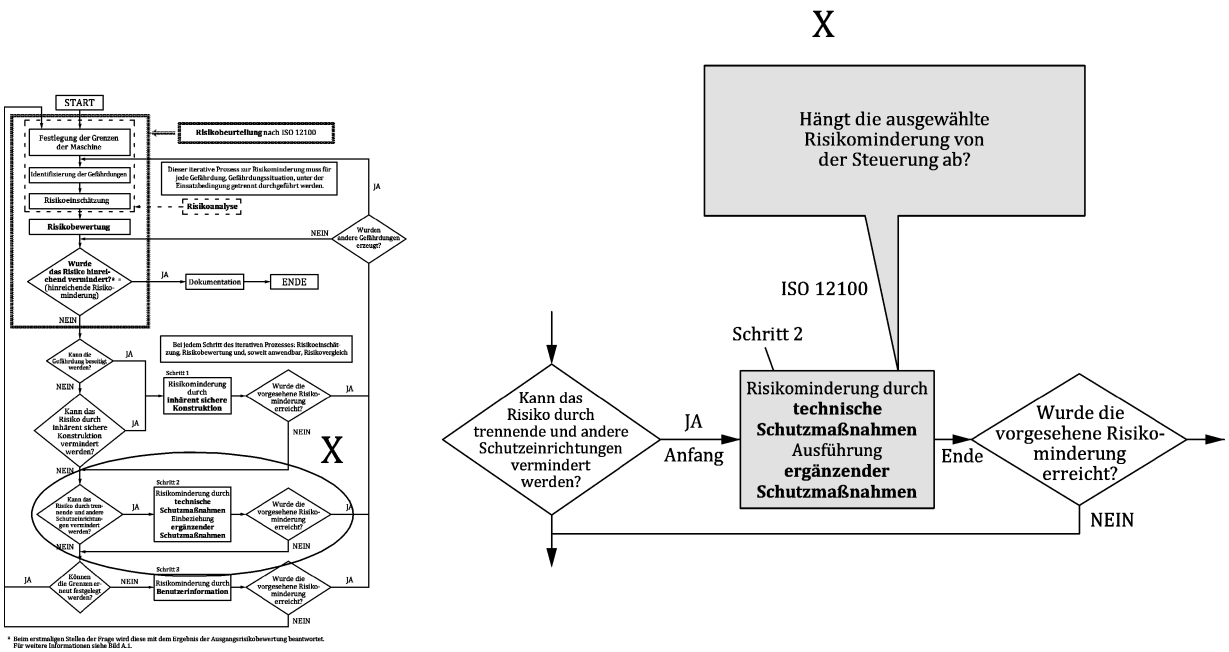


Bild 1 — Integration von ISO 13849-1 in den Prozess zur Risikominderung nach ISO 12100

ANMERKUNG 3 Bild 1 zeigt auf, wo das SRP/CS zum Prozess der Risikominderung von ISO 12100:2010, 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 Levels (PL).

Der erforderliche Performance Level (PL_r) für eine bestimmte Sicherheitsfunktion wird durch Risikoeinschätzung ermittelt.

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

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

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

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

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

— Steuerungsbaugruppen (z. B. die Logik für Steuerungsfunktionen, Datenverarbeitung, Überwachung); und

— berührungslos wirkende Schutzeinrichtungen (z. B. Lichtschranken), druckempfindliche Schutzeinrichtungen.

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

— Schutzeinrichtungen (z. B. Zweihandschaltungen, Verriegelungseinrichtungen);

— leistungssteuernde Elemente (z. B. Relais, Ventile);

— Sensoren und HMI-Elemente (Wegmesseinrichtungen, Freigabeschalter).

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

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

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

1 Anwendungsbereich

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

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

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

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

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

ANMERKUNG 3 Dieses Dokument legt ein Verfahren für die Gestaltung von SRP/CS fest, ohne dabei zu berücksichtigen, ob für bestimmte Maschinen (z. B. ortsveränderliche Maschinen) spezifische Anforderungen gelten. Diese spezifischen Anforderungen können in einer Typ-C-Norm festgelegt sein.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO 12100:2010, *Safety of machinery — General principles for design — Risk assessment and risk reduction*

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

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

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

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

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

3 Begriffe, Symbole und Abkürzungen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO 12100:2010 und die folgenden Begriffe.

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

— IEC Electropedia: verfügbar unter https://www.electropedia.org/

— ISO Online Browsing Platform: verfügbar unter https://www.iso.org/obp

3.1.1
sicherheitsbezogenes Teil einer Steuerung
SRP/CS, en: safety–related part of a control system
Teil einer Steuerung, der eine Sicherheitsfunktion ausführt, beginnend mit (einer) sicherheitsbezogenen Eingabe(n) bis hin zur Erzeugung von (einer) sicherheitsbezogenen Ausgabe(n)

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

3.1.2
Maschinensteuerung
System, das auf Eingangssignale von Teilen der Maschine, der Bediener, externer Steuerungseinrichtungen oder irgendeiner Kombination dieser reagiert und Ausgangssignale erzeugt, damit sich die Maschine in der bestimmungsgemäßen Art und Weise verhält

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

3.1.3
Spezifikation der Sicherheitsanforderungen
SRS, en: safety requirement specification
Spezifikation der Anforderungen an die Sicherheitsfunktionen, die von der sicherheitsbezogenen Steuerung erfüllt werden müssen; die Spezifikation erfolgt im Hinblick auf die Eigenschaften der Sicherheitsfunktionen (funktionale Eigenschaften) und die erforderlichen Performance Levels

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

3.1.4
Kategorie
Einstufung des Teilsystems bezüglich des Widerstands gegen Fehler und des nachfolgenden Verhaltens bei einem Fehler, das erreicht wird durch die Struktur der Anordnung der Teile, der Fehlererkennung und/oder ihrer Zuverlässigkeit

3.1.5
Performance Level
PL
diskrete Stufe, welche die Fähigkeit von sicherheitsbezogenen Teilen einer Steuerung spezifiziert, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen

Anmerkung 1 zum Begriff: Siehe 6.1.

3.1.6
erforderlicher Performance Level
PL_r
Performance Level, der erforderlich ist, um die erforderliche Risikominderung für jede Sicherheitsfunktion zu erreichen

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

3.1.7
Sicherheits-Integritätslevel
SIL
diskrete Stufe (eine von vier möglichen) zur Festlegung der Anforderungen an die Sicherheitsintegrität der Sicherheitsfunktionen, die den sicherheitsbezogenen Systemen zugeordnet werden, wobei der Sicherheits-Integritätslevel 4 die höchste Stufe der Sicherheitsintegrität und der Sicherheits-Integritätslevel 1 die niedrigste darstellt

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

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

3.1.8
Fehler
Fehlzustand
Zustand eines Geräts, in dem es unfähig ist, eine geforderte Funktion zu erfüllen, wobei die durch Wartung oder andere geplante Handlungen verursachte Funktionsunfähigkeit ausgeschlossen ist

Anmerkung 1 zum Begriff: Ein Fehler ist oft das Ergebnis eines Ausfalls der Einheit selbst, er kann aber auch ohne vorherigen Ausfall vorhanden sein.

Anmerkung 2 zum Begriff: In diesem Dokument bedeutet der Begriff „Fehler“ entweder „zufälliger Fehler“ oder „durch systematischen Ausfall hervorgerufener Fehler“.

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

3.1.9
Fehlerausschluss
Ausschluss von bestimmten Fehlern eines SRP/CS, wenn dies aufgrund ihrer Unwahrscheinlichkeit und ihres unbedeutenden Beitrags zur Zuverlässigkeit des SRP/CS gerechtfertigt ist

3.1.10
Ausfall
Beendigung der Fähigkeit eines Geräts, eine geforderte Funktion auszuführen

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

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

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

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

3.1.11
permanenter Fehlzustand
Fehler einer Einheit, der solange besteht, bis eine Instandsetzung ausgeführt worden ist

[QUELLE: IEC 60050-192:2015]

3.1.12
gefahrbringender Ausfall
Ausfall eines Elements und/oder Teilsystems und/oder Systems, das Anteil an der Ausführung der Sicherheitsfunktion hat, der:

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

b) die Wahrscheinlichkeit vermindert, die Sicherheitsfunktion bei Anforderung ordnungsgemäß auszuführen

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

3.1.13
Ausfall infolge gemeinsamer Ursache
CCF, en: common cause failure
Ausfall, der das Ergebnis eines oder mehrerer Ereignisse ist, die gleichzeitige Ausfälle von zwei oder mehreren getrennten Kanälen in einem mehrkanaligen Teilsystems verursachen und zu einem Ausfall einer Sicherheitsfunktion führen

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

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

3.1.14
systematischer Ausfall
Ausfall mit deterministischem Bezug zu einer bestimmten Ursache, die nur durch Änderung der Gestaltung oder des Herstellungsprozesses, der Betriebsverfahren, der Dokumentation oder der zugehörigen Faktoren beseitigt werden kann

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

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

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

— der Spezifikation der Sicherheitsanforderungen,

— der Gestaltung, der Herstellung, der Installation und des Betriebs der Hardware, und

— der Gestaltung, Realisierung der Software.

[QUELLE: IEC 60050-192:2015]

3.1.15
Überbrückungsfunktion
vorübergehende automatische Überbrückung einer Sicherheitsfunktion bzw. von Sicherheitsfunktionen durch das SRP/CS

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

3.1.16
manuelle Rückstellung
Sicherheitsfunktion des SRP/CS zum manuellen Wiederherstellen einer oder mehrerer Sicherheitsfunktionen vor dem Wiederanlaufen einer Maschine

3.1.17
Schaden
physische Verletzung oder Gesundheitsschädigung

[QUELLE: ISO 12100:2010, 3.5]

3.1.18
Gefährdung
potentielle Schadensquelle

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

Anmerkung 2 zum Begriff: Die Gefährdung im Sinne dieser Definition ist entweder:

— bei der bestimmungsgemäßen Verwendung der Maschine dauerhaft vorhanden (z. B. Bewegung von gefährdenden beweglichen Teilen, Lichtbogen beim Schweißen, ungesunde Körperhaltung, Geräuschemission, hohe Temperatur); oder

— kann unerwartet auftreten (z. B. Explosion, Gefährdung durch Quetschen als Folge eines unbeabsichtigten/unerwarteten Anlaufs, Herausschleudern als Folge eines Bruchs, Stürzen als Folge von Beschleunigung/Abbremsen).

[QUELLE: ISO 12100:2010, 3.6, modifiziert — Anmerkung 3 zum Begriff wurde gestrichen.]

3.1.19
Gefährdungssituation
Sachlage, bei der eine Person mindestens einer Gefährdung ausgesetzt ist

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

[QUELLE: ISO 12100:2010, 3.10]

3.1.20
Risiko
Kombination der Wahrscheinlichkeit des Eintritts eines Schadens und seines Schadensausmaßes

[QUELLE: ISO 12100:2010, 3.12]

3.1.21
Restrisiko
Risiko, das verbleibt, nachdem risikomindernde Maßnahmen (Schutzmaßnahmen) umgesetzt wurden

Anmerkung 1 zum Begriff: Siehe Bild 3.

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

3.1.22
Risikobeurteilung
Gesamtheit des Verfahrens, das eine Risikoanalyse und Risikobewertung umfasst

[QUELLE: ISO 12100:2010, 3.17]

3.1.23
risikomindernde Maßnahme
Schutzmaßnahme
Handlung oder Mittel zur Beseitigung von Gefährdungen oder zur Verminderung von Risiken

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

[QUELLE: ISO Guide 51:2014, 3.13]

3.1.24
Risikoanalyse
Kombination aus Festlegung der Grenzen der Maschine, Identifizierung der Gefährdungen und Risikoeinschätzung

[QUELLE: ISO 12100:2010, 3.15]

3.1.25
Risikobewertung
auf der Risikoanalyse beruhende Beurteilung, ob die Ziele zur Risikominderung erreicht wurden

[QUELLE: ISO 12100:2010, 3.16]

3.1.26
bestimmungsgemäße Verwendung einer Maschine
Verwendung einer Maschine in Übereinstimmung mit den in der Benutzerinformation bereitgestellten Informationen

[QUELLE: ISO 12100:2010, 3.23]

3.1.27
vernünftigerweise vorhersehbare Fehlanwendung
Verwendung einer Maschine in einer Weise, die vom Konstrukteur nicht vorgesehen ist, sich jedoch aus dem leicht vorhersehbaren menschlichen Verhalten ergeben kann

[QUELLE: ISO 12100:2010, 3.24]

3.1.28
Sicherheitsfunktion
Funktion der Maschine, wobei ein Ausfall der Funktion zur unmittelbaren Erhöhung des Risikos (der Risiken) führen kann

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

[QUELLE: ISO 12100:2010, 3.30]

3.1.29
Teilfunktion
Teil einer Sicherheitsfunktion, dessen Ausfall zu einem Ausfall der Sicherheitsfunktion führt

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

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

3.1.30
Überwachung
Diagnosemaßnahme, mit der ein Zustand erkannt und mit einem erwarteten Wert verglichen wird

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

3.1.31
Kreuzvergleich
Diagnosemaßnahme zur Überprüfung der Plausibilität von redundanten Signalen in beiden Kanälen eines redundanten Teilsystems

3.1.32
programmierbares elektronisches System
PE-System
System zur Steuerung, zum Schutz oder zur Überwachung, basierend auf einem oder mehreren programmierbaren elektronischen Geräten, einschließlich aller Elemente des Systems wie z. B. Energieversorgung, Sensoren und anderer Eingabegeräte, Datenverbindungen und anderer Kommunikationswege sowie Aktoren und anderer Ausgabeeinrichtungen

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

3.1.33
mittlere Dauer bis zum gefahrbringenden Ausfall
$MTTF_D$, en: mean time to dangerous failure
Erwartungswert der Verteilung der Dauern bis zum gefahrbringenden Ausfall

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

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

3.1.34
mittlere Betriebsdauer zwischen Ausfällen
MTBF, en: mean time between failure
erwarteter Wert der Betriebsdauer zwischen aufeinanderfolgenden Ausfällen

3.1.35
gefährliche Ausfallrate
RDF, en: ratio of dangerous failures
Anteil der gesamten Ausfallrate eines Elements, der zu einem gefahrbringenden Ausfall führen kann

3.1.36
Diagnosedeckungsgrad
DC, en: diagnostic coverage
Maß für die Wirksamkeit der Diagnosemaßnahmen, bestimmt als das Verhältnis der Rate der erkannten gefahrbringenden Ausfälle zur Gesamtrate der gefahrbringenden Ausfälle

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

3.1.37
Gebrauchsdauer
T_{M}
Zeitraum, der die bestimmungsgemäße Verwendung eines SRP/CS abdeckt

3.1.38
Testrate
r_{t}
Häufigkeit der Tests, um Fehler in einem SRP/CS zu erkennen, Kehrwert des Diagnose-Testintervalls

3.1.39
Anforderungsrate
r_{d}
Häufigkeit von Anforderungen für eine von einem SRP/CS auszuführende Sicherheitsfunktion

3.1.40
Programmiersprache mit eingeschränktem Sprachumfang
LVL, en: limited variability language
Art von Programmiersprache, die die Möglichkeit bietet, vorgegebene anwendungsspezifische Funktionen aus einer Bibliothek zu kombinieren, um die festgelegten Sicherheitsanforderungen zu implementieren

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

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

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

[QUELLE: IEC 62061, FDIS 2020, 3.2.62]

3.1.41
Programmiersprache mit nicht eingeschränktem Sprachumfang
FVL, en: full variability language
Programmiersprache, die die Möglichkeit bietet, eine große Vielzahl unterschiedlicher Funktionen und Anwendungen zu implementieren

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

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

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

[QUELLE: IEC 62061, FDIS 2020, 3.2.61]

3.1.42
sicherheitsbezogene Anwendungssoftware
SRASW, en: safety related application software
anwendungsspezifische Software, die üblicherweise logische Sequenzen, Grenzwerte und Ausdrücke zum Steuern der entsprechenden Eingänge, Ausgänge, Berechnungen und Entscheidungen enthält, um die notwendigen Anforderungen des SRP/CS zu erfüllen

3.1.43
sicherheitsbezogene Embedded-Software
SRESW, en: safety related embedded software
Firmware
Software, die als Bestandteil des Systems vom Hersteller mitgeliefert wird

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

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

3.1.44
Betriebsart mit hoher Anforderungsrate oder Betriebsart mit kontinuierlicher Anforderung
Betriebsart, in der die Häufigkeit von Anforderungen an ein SRP/CS für die Ausführung seiner Sicherheitsfunktion mehr als einmal je Jahr beträgt oder die Sicherheitsfunktion die Maschine als Teil des normalen Betriebs in einem sicheren Zustand hält

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

3.1.45
Betriebsart mit niedriger Anforderungsrate
Betriebsart, in der die Häufigkeit von Anforderungen an ein SRP/CS für die Ausführung seiner Sicherheitsfunktion nicht mehr als einmal je Jahr beträgt

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

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

3.1.46
Teilsystem
Einheit, die aus der Zerlegung eines SRP/CS auf erster Ebene resultiert und deren gefahrbringender Ausfall zu einem gefahrbringenden Ausfall einer Sicherheitsfunktion führt

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

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

3.1.47
Teilsystemelement
Teil eines Teilsystems, bestehend aus einem einzelnen Bauteil oder einer Baugruppe

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

3.1.48
Kanal
Element oder Gruppe von Elementen, das bzw. die eine Sicherheitsfunktion oder einen Teil davon unabhängig ausführt

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

3.1.49
bewährte Sicherheitsprinzipien
Prinzipien, die sich in der Vergangenheit bei der Gestaltung oder Integration von sicherheitsbezogenen Steuerungen als wirkungsvoll erwiesen haben, und so kritische Fehler oder Ausfälle, welche die Leistung einer Sicherheitsfunktion beeinflussen können, vermeiden oder steuern

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

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

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

3.1.50
bewährtes Bauteil
Bauteil, das erfolgreich in sicherheitsbezogenen Anwendungen eingesetzt wurde

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

3.1.51
Betriebsart
Betriebsweise einer Maschine (z. B. Automatikbetrieb, manueller Betrieb, Instandhaltungsbetrieb), in der vordefinierte Maschinenfunktionen und Sicherheitsmaßnahmen in Verbindung mit diesen Funktionen ausgewählt sind

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

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

3.1.52
dynamisches Testen
überwachte Diagnosemaßnahme, die in geeigneten Abständen eine Signaländerung zu Testzwecken ausführt

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

Anmerkung 2 zum Begriff: Beim dynamischen Testen werden üblicherweise Testimpulse verwendet, um Kurzschlüsse oder Unterbrechungen in Signalpfaden zu erkennen oder um Fehlfunktionen aufzudecken.

3.1.53
Plausibilitätsprüfung
Diagnosemaßnahme, die überwacht, ob der Status eines Eingangs (Ausgangs) zu dem Status des Systems oder anderer Eingänge (Ausgänge) passt

3.1.54
Verifizierung
Bestätigung durch Bereitstellung eines objektiven Nachweises, dass festgelegte Anforderungen erfüllt worden sind

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

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

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

[QUELLE: ISO 9000:2015, 3.8.12]

3.1.55
Validierung
Bestätigen aufgrund einer Untersuchung und durch Bereitstellung eines objektiven Nachweises, dass die besonderen Anforderungen für eine spezielle beabsichtigte Verwendung erfüllt worden sind

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

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

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

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

3.1.56
Fachkraft
Person, die aufgrund ihrer Weiterbildung, ihrer Ausbildung und ihrer Erfahrung fähig ist, Risiken zu erkennen und Gefährdungen im Zusammenhang mit der jeweiligen Ausrüstung zu vermeiden

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

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

3.1.57
Black Box
Gerät, System oder Objekt, das hinsichtlich seiner Eingänge und Ausgänge überprüft werden kann

3.1.58
Grey Box
Gerät, System oder Objekt, von dem einige der internen Funktionen bekannt sind

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

3.2 Symbole und Abkürzungen

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

Tabelle 1 — Symbole und Abkürzungen

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

Symbol oder Abkürzung	Beschreibung	Definition oder Fundort
I/O	Eingänge/Ausgänge	Tabelle E.1 und Tabelle E.2
i_m	Verbindungsmittel	Bild 7, Bild 8, Bild 9, Bild 10
K1A, K1B	Schütze	Anhang I
L, L1, L2	Logik	6.1
LVL	Programmiersprache mit eingeschränktem Sprachumfang (en: limited variability language)	3.1.38
λ_D	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	3.1.28
n, N, $\tilde{N}$	Anzahl von Einheiten	6.2, D.1
$N_{niedrig}$	Anzahl von Teilsystemen mit $PL_{niedrig}$ in einer Kombination von Teilsystemen	6.2
n_{op}	mittlere Anzahl der jährlichen Betätigungen	Anhang C
O, O1, O2, OTE	Ausgabegerät, z. B. leistungssteuernde Elemente	6.1
P, P1, P2	Möglichkeit zum Vermeiden der Gefährdung	A.2.3
PES	programmierbares elektronisches System (en: programmable electronic system)	3.1.26
PFH_D	durchschnittliche Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde	Tabelle 2 und Tabelle K.1
PL	Performance Level	3.1.27
SPS	speicherprogrammierbare Steuerung	Anhang I
$PL_{niedrig}$	niedrigster Performance Level eines Teilsystems in einer Kombination von Teilsystemen	6.2
PL_r	erforderlicher Performance Level	3.1.27
r_d	Anforderungsrate	3.1.35
r_t	Testrate	3.1.34
RDF	gefährliche Ausfallrate (en: ratio of dangerous failures)	C.4.2
RS	Drehgeber (en: rotation sensor)	Anhang I
S, S1, S2	Schwere der Verletzung	A.2.1
SB	Teilsystem	Bild 13, Bild H.1, Bild H.2
SOS	sicherer Betriebshalt	5.2.3.1
SS2	sicherer Stopp 2	5.2.3.1
SW1A, SW1B, SW2	Positionsschalter	Anhang I
SIL	Sicherheits-Integritätslevel	3.1.38, Abschnitt 6

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

4 Überblick

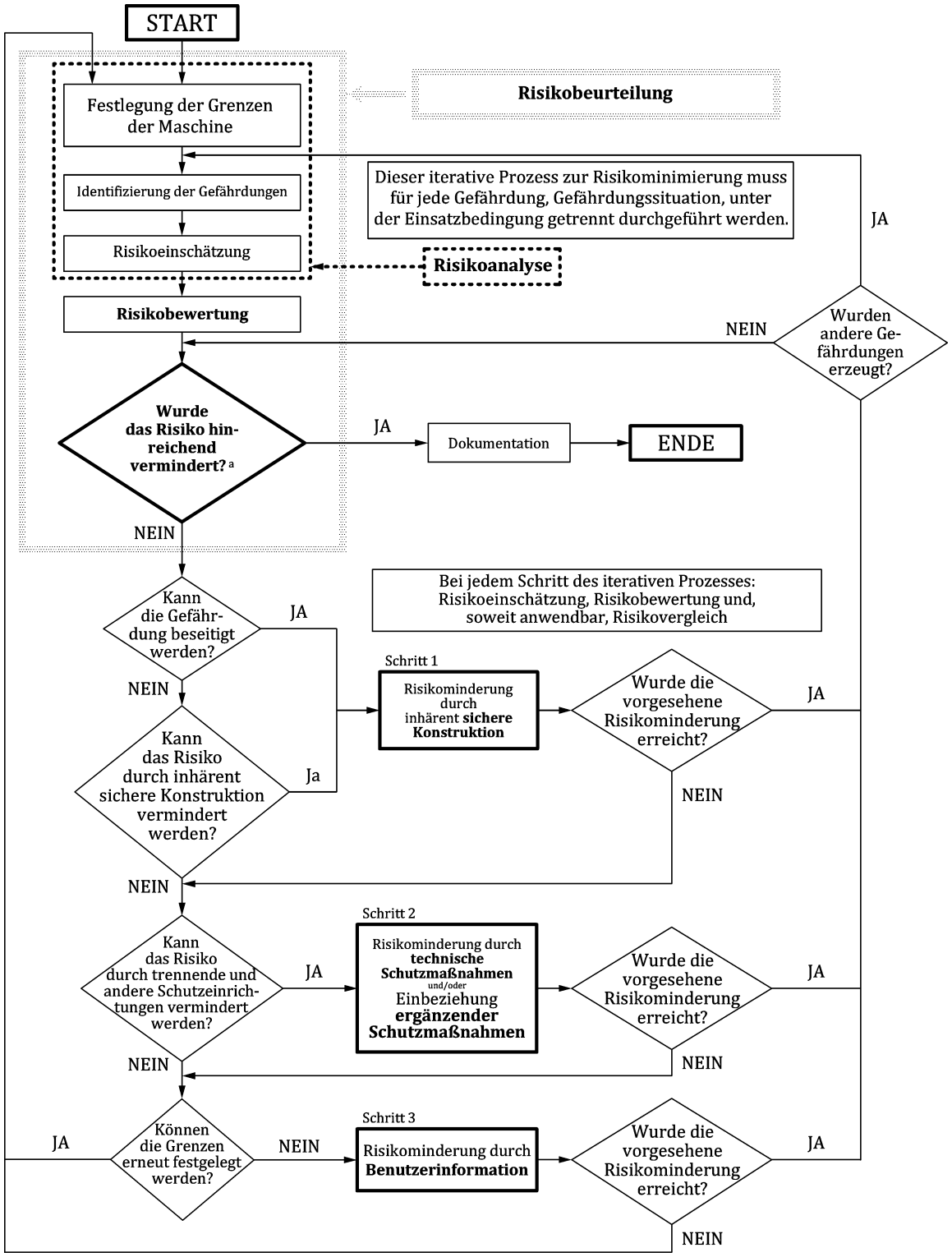
4.1 Prozess zur Risikobeurteilung und Risikominderung an der Maschine

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

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

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

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



Legende

[a] Beim erstmaligen Stellen der Frage wird diese mit dem Ergebnis der Ausgangsrisikobeurteilung beantwortet.

☐ Risikominderung durch technische Schutzmaßnahmen darf durch die SRP/CS erfolgen, die Sicherheitsfunktionen ausführen. In diesem Fall, dieses Dokument.

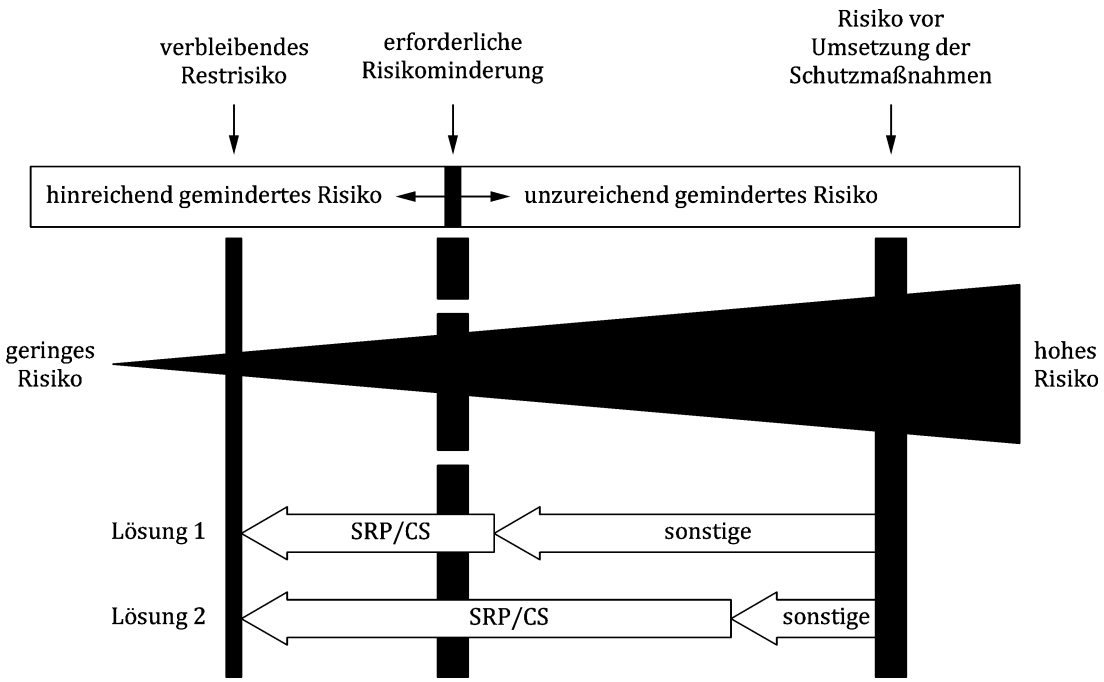
Bild 2 — Schematische Darstellung des Prozesses zur Risikominderung einschließlich des dreistufigen iterativen Prozesses nach ISO 12100:2010

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

4.2 Beitrag zur Risikominderung

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

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



Legende

Lösung 1 Ein wesentlicher Teil der Risikominderung erfolgt durch andere Schutzmaßnahmen als durch ein SRP/CS (z. B. mechanische Maßnahmen), ein kleiner Beitrag zur Risikominderung erfolgt durch ein SRP/CS (z. B. Lichtschranke).

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

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

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

4.3 Entwurfsprozess eines SRP/CS

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

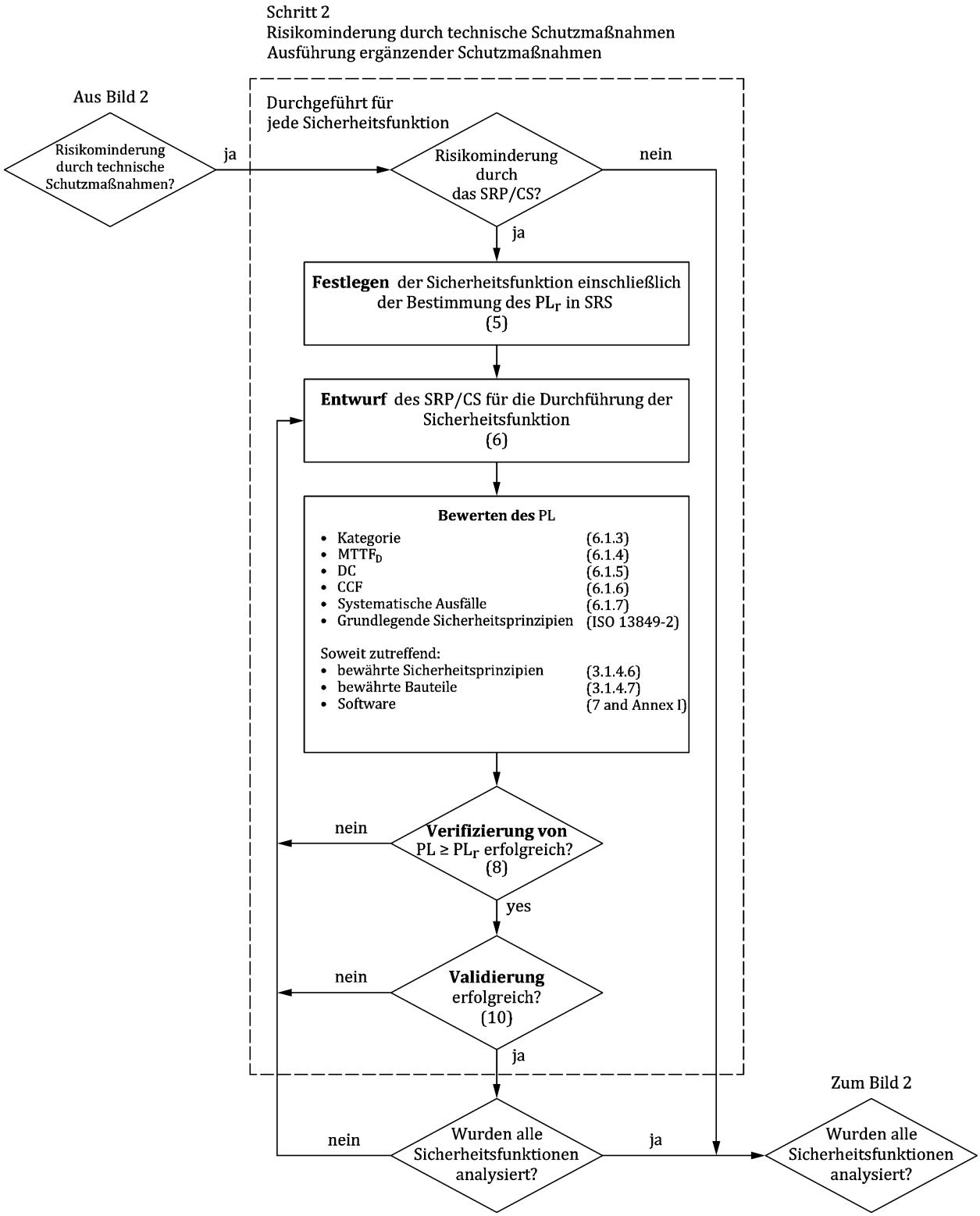


Bild 4 — Iterativer Prozess für den Entwurf von sicherheitsbezogenen Teilen von Steuerungen

4.4 Verfahren

Dieses Dokument beschreibt das folgende Verfahren:

1) Spezifikation der Sicherheitsfunktionen (Abschnitt 5);

2) Entwurf und technische Umsetzung der Sicherheitsfunktionen einschließlich der Identifizierung der SRP/CS und deren Teilsysteme, die alle Sicherheitsfunktionen ausführen;

   a) Entwurfsaspekte (Abschnitt 6);

   b) Software-Sicherheitsanforderungen (Abschnitt 7);

3) Verifizieren, ob der erreichte PL dem PL_r entspricht (Abschnitt 8);

4) ergonomische Entwurfsaspekte (Abschnitt 9);

5) Validierung (Abschnitt 10 oder ISO 13849-2);

6) Instandhaltung (Abschnitt 11);

7) technische Dokumentation (Abschnitt 12);

8) Benutzerinformation (Abschnitt 13).

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

Tabelle 2 — Performance Levels

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

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

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

4.5 Erforderliche Informationen

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

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

— Informationen über alle Sicherheitsfunktionen (siehe Abschnitt 5), die für den Prozess zur Risikominderung bei jeder Gefährdung als notwendig ermittelt wurden. Dazu gehört:

  — eine ausführliche Beschreibung jeder Sicherheitsfunktion (siehe 5.2);

  — die Bestimmung des erforderlichen Performance Levels (PL_r) für jede Sicherheitsfunktion (siehe 6.3).

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

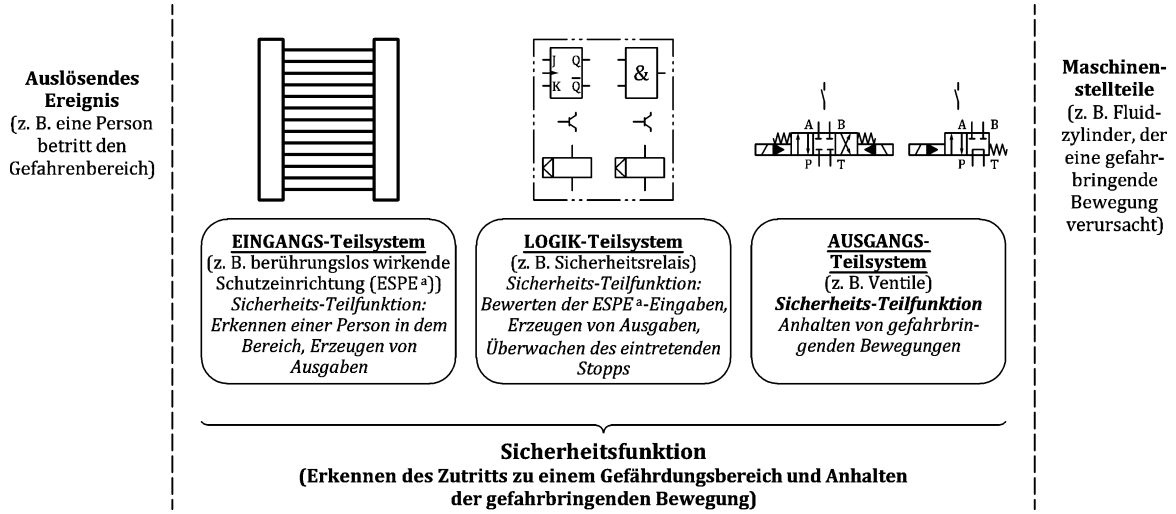
4.6 Ausführung von Sicherheitsfunktionen mithilfe von Teilsystemen

Die Ausführung einer Sicherheitsfunktion darf erfolgen:

— mithilfe von bereits zuvor nach diesem Dokument, nach IEC 62061, nach IEC 61508 oder nach sonstigen maßgebenden sicherheitsbezogenen Produktnormen (z. B. IEC 61496-1 und IEC 61800-5-2) validierten Teilsystemen;

— durch den Entwurf neuer Teilsysteme nach diesem Dokument; oder

— durch eine Kombination der beiden vorstehenden Optionen (siehe Beispiel in Bild 5).



a berührungslos wirkende Schutzeinrichtung (BWS)

Bild 5 — Beispiel für eine Kombination von Teilsystemen

5 Spezifikation der Sicherheitsfunktionen

5.1 Identifizierung und allgemeine Beschreibung der Sicherheitsfunktion

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

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

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

Abschnitt 5 behandelt die folgenden Schritte:

1) allgemeine Beschreibung der Sicherheitsfunktion (Verknüpfung der Gefährdungen mit den Sicherheitsfunktionen);

2) ausführliche Beschreibung der Sicherheitsanforderungen (siehe 5.2);

3) Bestimmung des PL_r für jede Sicherheitsfunktion, d. h. wie zuverlässig die Sicherheitsfunktion sein muss, siehe 5.3;

4) Überprüfung der Spezifikation der Sicherheitsanforderungen (siehe 5.4).

Eine Sicherheitsfunktion muss allgemein beschrieben sein, um den Beitrag des SRP/CS zur Risikominderung festzulegen. Die Beschreibung muss auf die Gefährdungen Bezug nehmen, die in der Risikobeurteilung definiert sind, und muss angeben, wie die Funktion bis zum Erreichen der erforderlichen Sicherheit arbeitet. Der Prozess zum Festlegen von Sicherheitsfunktionen erfordert ausführliche Angaben aus der Risikobeurteilung, die nach ISO 12100:2010 durchgeführt wurde.

5.2 Spezifikation der Sicherheitsanforderungen

5.2.1 Allgemeine Anforderungen

5.2.1.1 Allgemeines

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

Die Spezifikation der Sicherheitsanforderungen ist dafür vorgesehen, Fehler beim Übergang vom Risikobeurteilungs- und -minderungsprozess nach ISO 12100:2010 zum SRP/CS-Entwurfs- und -Bewertungsprozess nach diesem Dokument zu verhindern, insbesondere wenn diese beiden Prozesse von unterschiedlichen Personen oder Organisationen durchgeführt werden (siehe Tabelle 3).

Tabelle 3 — Übergang vom Risikobeurteilungs- und -minderungsprozess nach ISO 12100 zum SRP/CS-Entwurfs- und -Bewertungsprozess nach ISO 13849-1

Erforderliche Informationen für das Erstellen der SRS (siehe 5.2.1.2)	Umwandlung	Beispiele für die Festlegung der Sicherheitsfunktionen in der SRS (siehe 5.2.1.3)
— Ergebnisse der Risikobeurteilung der Maschine oder eines Teils davon, einschließlich gefährlicher Teile — Betriebseigenschaften der Maschine, z. B. bestimmungsgemäße Verwendung — Handlungen im Notfall — Beschreibung der Wechselwirkung verschiedener Arbeitsprozesse und manueller Aktionen, z. B. Instandsetzung — ergonomische Aspekte — Anwendungsgrenzen in Zusammenhang mit den Umgebungsbedingungen	⇨	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 — PLr c — Ansprechzeit — usw.

5.2.1.2 Notwendige Informationen für die Erstellung der Spezifikation der Sicherheitsanforderungen

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

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

a) Ergebnisse der Risikobeurteilung der Maschine oder eines Teils davon für jede spezifische Gefährdung, wobei die dazugehörige(n) risikomindernde(n) Maßnahme(n) auf einer sicherheitsbezogenen Steuerung beruht/beruhen, um so eine Sicherheitsfunktion auszuführen;

b) Betriebseigenschaften der Maschine, einschließlich:

   1) der bestimmungsgemäßen Verwendung der Maschine;

   2) der vernünftigerweise vorhersehbaren Fehlanwendung;

   3) des Einflusses von überlagerten Gefährdungen;

4) der Betriebsarten (z. B. lokale Betriebsart, Automatikbetrieb, Betrieb mit Bezug zu einem Bereich oder Teil der Maschine);

5) der/den Betriebsart(en), während der/denen die Sicherheitsfunktion aktiviert sein muss;

6) der Zyklusdauer; und

7) der Ansprechzeit bis ein sicherer Zustand erreicht ist (siehe auch ISO 13855:2010, 5.1);

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

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

c) Handlungen im Notfall (IEC 60204-1:2016, Anhang E);

d) Beschreibung der Wechselwirkung verschiedener Arbeitsprozesse und manueller Aktionen (z. B. Instandsetzen, Einrichten, Reinigen, Fehlersuche, Betriebsarten mit deaktivierten Schutzeinrichtungen);

e) ergonomische Aspekte zum Minimieren einer fehlerhaften Bedienung oder Umgehung;

f) Anwendungsgrenzen in Zusammenhang mit den Umgebungsbedingungen;

g) Einfluss von überlagerten Gefährdungen (siehe A.3).

5.2.1.3 Festlegung aller Sicherheitsfunktionen in der Spezifikation der Sicherheitsanforderungen

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

a) die Kurzbeschreibung/Bezeichnung der Sicherheitsfunktion für eine klare Bezugnahme;

b) das Ereignis, das die Sicherheitsfunktion auslöst;

c) die Reaktion, die durch die Ausgabe(n) der Sicherheitsfunktion auszulösen ist, um den beabsichtigten sicheren Zustand zu erreichen;

BEISPIEL 1 Anhalten von gefahrbringenden Bewegungen.

d) den erforderlichen Performance Level PL_r für jede Sicherheitsfunktion (siehe 5.3);

e) die Ansprechzeit d er Maschine zum Erreichen eines sicheren Zustands, nachdem der Befehl im Zuge der Sicherheitsfunktion ausgelöst wurde, z. B. das Gesamt-Anhaltevermögen des Systems (Reaktionszeit plus Anhaltezeit) nach ISO 13855:2010;

f) die Betriebsart(en), während der/denen die Sicherheitsfunktion aktiviert sein muss;

g) Schnittstellen der Sicherheitsfunktionen;

h) falls notwendig, im Falle einer Fehlererkennung in einem Funktionskanal, Verfahren, um die Maschine in einen sicheren Zustand zu bringen, einschließlich der Art und Weise, wie der sichere Zustand aufrechterhalten wird, bis der Fehler behoben ist;

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

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

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

j) die Anforderungsrate der Sicherheitsfunktion und/oder die Betriebshäufigkeit des SRP/CS;

k) die Priorität der Sicherheitsfunktionen, die gleichzeitig aktiv sein können und dadurch zu Konflikten führen können;

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

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

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

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

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

5.2.2 Anforderungen an spezifische Sicherheitsfunktionen

5.2.2.1 Sicherheitsbezogene Stopp-Funktion

Eine sicherheitsbezogene Stopp-Funktion (z. B. eingeleitet durch eine Schutzeinrichtung) muss so schnell wie notwendig nach ihrer Auslösung die Maschine in den sicheren Zustand bringen. Solch eine sicherheitsbezogene Stopp-Funktion muss Vorrang vor allen maßgebenden Startfunktionen und nicht sicherheitsbezogenen Stopp-Funktionen haben. Wenn eine Gruppe von Maschinen koordiniert zusammenarbeitet, müssen Vorkehrungen getroffen werden, um der übergeordneten Steuerung und/oder den anderen Maschinen eine solche Stopp-Bedingung zu signalisieren.

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

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

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

5.2.2.2 Manuelle Rückstellfunktion

Die Wiederherstellung der Sicherheitsfunktion durch die Rückstellung der Schutzeinrichtung hebt den Stopp-Befehl auf. Wenn dies in der Risikobeurteilung angegeben ist, muss diese Aufhebung des Stopp-Befehls durch eine manuelle, separate und beabsichtigte Handlung (manuelle Rückstellung) bestätigt werden.

Die manuelle Rückstellfunktion:

— muss durch ein getrenntes, manuell zu bedienendes Gerät, das vom Start-Befehl getrennt ist, bereitgestellt werden;

— darf nur dann ausgeführt werden, wenn alle davon beeinflussten Sicherheitsfunktionen und Schutzeinrichtungen funktionsfähig sind;

— darf selbst keine Gefährdungssituation einleiten;

— muss durch eine beabsichtigte Handlung ausgelöst werden;

— muss der Steuerung ermöglichen, einen separaten Start-Befehl anzunehmen; und

— muss von einer überwachten Signaländerung akzeptiert werden, um eine vorhersehbare Fehlanwendung zu vermeiden.

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

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

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

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

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

Siehe auch Tabelle M.1.

5.2.2.3 Wiederanlauffunktion

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

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 verriegelten trennenden Schutzeinrichtung keinen Vorrang vor der automatischen Steuerung hat, könnte 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.

5.2.2.4 Lokale Steuerungsfunktion

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

— 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.

5.2.2.5 Überbrückungsfunktion

Die Überbrückungsfunktion ist ein vorübergehendes automatisches Deaktivieren einer Sicherheitsfunktion durch die sicherheitsbezogene Steuerung einer Maschine. Sie kann ausgeführt werden, um den Zutritt von Personen oder die Beförderung von Materialien zu ermöglichen:

— während eines ungefährlichen Abschnitts des Maschinenzyklus; oder

— wenn die Sicherheit durch andere Maßnahmen aufrechterhalten wird.

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

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

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

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

5.2.2.6 Sicherheitsbezogene Parameter

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

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

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

5.2.2.7 Schwankungen, Verlust und Wiederkehr der Spannungsversorgung

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

5.2.2.8 Anforderungen an die Betriebsartenwahl

Die Wahl der Betriebsart ist eine Sicherheitsfunktion, durch die (eine) Sicherheitsfunktion(en) freigegeben oder abgeschaltet wird/werden. Es gelten die folgenden Anforderungen:

a) es darf nur eine Betriebsart nach der anderen aktiviert werden; jede gewählte Betriebsart muss deutlich erkennbar sein bzw. angezeigt werden;

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

b) durch die Betriebsartenwahl selbst darf keine Maschinenbewegung ausgelöst werden. Hierzu muss eine separate Betätigung der Anlaufsteuerung erforderlich sein;

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

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

5.2.2.9 Sicherheitsfunktion(en) für Instandhaltungsaufgaben

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

ANMERKUNG 1 Zu den Instandhaltungsaufgaben können unter anderem folgende gehören:

— Einrichten;

— Einlernen (Teachen)/Programmieren;

— Umrüsten;

— Reinigung und Sauberhaltung;

— Desinfizieren;

— geplante oder ungeplante vorbeugende Instandhaltung oder Instandsetzung;

— Fehlersuche/Fehlerbehandlung;

— Fehlerdiagnose.

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

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

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

a) Steuerung mit selbsttätiger Rückstellung;

b) Steuerung mit Zustimmeinrichtung;

c) Überwachung oder Begrenzung der Geschwindigkeit, des Drehmoments, der Leistung, der Position, der Temperatur, der Stufe usw.;

d) Verhindern des unerwarteten Anlaufs;

e) Isolations- und Energieableitungsfunktion;

f) mechanische Rückhaltung oder Einhausung.

ANMERKUNG 2 Siehe Anhang M für ergänzende Informationen.

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

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

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

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

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

5.2.2.10 Anreiz zum Übergehen von Sicherheitsfunktionen

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

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

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

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

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

— dass die risikomindernde Maßnahme verhindert, dass die Aufgabe ausgeführt wird; es besteht die Notwendigkeit, eine Aufgabe auszuführen, die hinsichtlich Gefährdungen und Risiken nicht identifiziert und bewertet wurde;

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

— die risikomindernde Maßnahme ist schwierig anzuwenden;

— die risikomindernde Maßnahme und/oder deren zugehörige Gefährdung wird/werden vom Personal nicht als solche erkannt;

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

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

5.2.2.11 Fernzugriff

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

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

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

5.3 Bestimmung des erforderlichen Performance Levels für jede Sicherheitsfunktion

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

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

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

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

ANMERKUNG 3 Der PL_r für eine Sicherheitsfunktion bestimmt die Zuverlässigkeit, mit der die Steuerung diese Sicherheitsfunktion ausführt und die vorgesehene Risikominderung erreicht wird. Der PL_r wird mithilfe verschiedener Risikofaktoren bestimmt. Siehe auch Anhang A.

5.4 Überprüfung der Spezifikation der Sicherheitsanforderungen

Die Spezifikation der Sicherheitsanforderungen muss mit der Risikobeurteilung abgeglichen werden, bevor mit dem Entwurf begonnen wird, da jedes weitere Vorgehen auf diesen Anforderungen basiert. Durch die Überprüfung muss sichergestellt werden, dass alle Sicherheitsfunktionen festgelegt sind, um die vorgesehene Risikominderung an der Maschine zu erreichen. Siehe auch 10.4 für die Validierung der SRS.

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

5.5 Zerlegung eines SRP/CS in Teilsysteme

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

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

— Eingänge und Ausgänge jeder Teilfunktion.

Ein SRP/CS kann Folgendes umfassen:

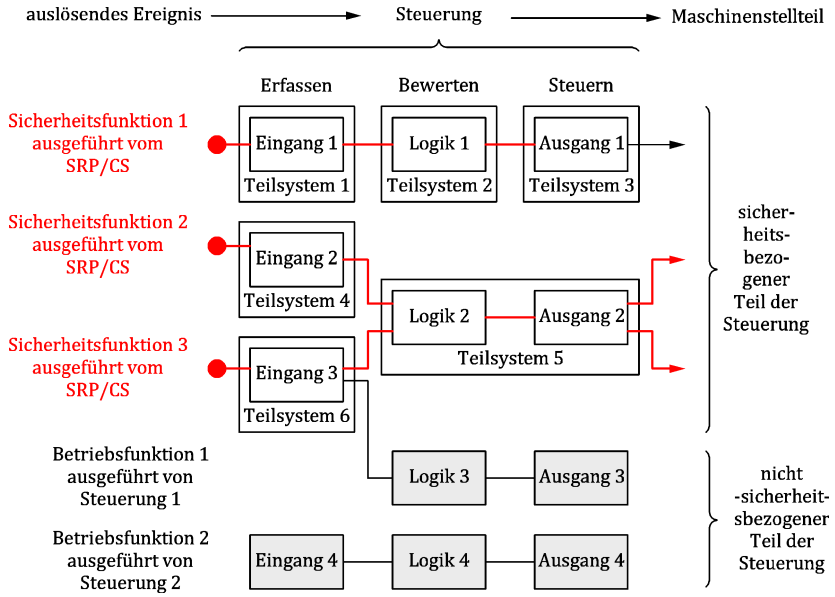
— ein oder mehrere zuvor validierte(s) Teilsystem(e);

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

— eine Kombination der beiden vorstehenden Optionen.

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

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



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

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

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

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

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

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

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

— Logik/Verarbeitung (Teilsysteme 2 und 5);

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

— Maschinenstellteil (z. B. Motor, Zylinder);

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

ANMERKUNG 1 Die Zerlegung eines SRP/CS in Teilsysteme nach Bild 6 ist typisch, aber das gesamte SRP/CS darf auch durch ein einziges Teilsystem oder durch mehr als drei Teilsysteme verwirklicht werden.

ANMERKUNG 2 Ein SRP/CS kann als ein einziges Teilsystem mit einem Sensor, Logikeinheiten und leistungssteuernden Elementen ausgeführt werden. Ein Beispiel für die Ausführung eines SRP/CS aus einem einzigen Teilsystem ist eine „intelligente“ Sensoreinheit (z. B. Lichtvorhang, Laserscanner) mit integrierter Ausgangsschalteinrichtung (z. B. Relais zum Ausschalten einer gefährlichen Bewegung).

ANMERKUNG 3 Es ist aber auch möglich, dass ein Teilsystem oder ein SRP/CS Sicherheitsfunktionen und normale Steuerungsfunktionen ausführt. Der Konstrukteur kann jede verfügbare Technologie, einzeln oder in Kombination, verwenden. Ein SRP/CS kann auch eine Betriebsfunktion bereitstellen (z. B. eine AOPD als Möglichkeit zur Auslösung eines Zyklus).

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

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

6 Entwurfsaspekte

6.1 Bewertung des erreichten Performance Levels

6.1.1 Allgemeine Übersicht der Performance Levels

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

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

1) der Architektur (siehe 6.1.3);

   a) Zuweisen einer Kategorie zum Teilsystem und Bewerten des Ergebnisses;

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

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

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

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

   c) Bewerten, ob das erforderliche Verhalten bei (einem) Fehler(n) eingehalten wird;

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

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

4) des CCF (siehe 6.1.6 und Anhang F);

5) des Einflusses des Entwurfs der sicherheitsbezogenen Software auf den Bediener der Hardware (siehe Abschnitt 7 und Anhang J);

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

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

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

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

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

ANMERKUNG 2 Der Beitrag der Zuverlässigkeit (z. B. $MTTF_D$, Architektur) kann in Abhängigkeit von den verwendeten sicherheitsbezogenen Teilen variieren.

ANMERKUNG 3 Es gibt mehrere Verfahren zur Abschätzung der quantifizierbaren Aspekte des PL für beliebige Systemtypen (z. B. einer komplexen Struktur), z. B. Markov-Modelle, allgemeine stochastische Petri-Netze (GSPN), Zuverlässigkeitsblockdiagramme (siehe z. B. IEC 61508, IEC 61078, 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), 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 Teilsystemkombinationen siehe 6.2.

Die qualitativen Aspekte des PL und das Vermeiden von systematischen Ausfällen müssen durch Erfüllen der in diesem Dokument, einschließlich Anhang G, angegebenen Anforderungen und Anleitungen erreicht werden.

Wenn in produktspezifischen Normen, wie der Normenreihe IEC 61496 für berührungslos wirkende Schutzeinrichtungen (BWS) oder 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 Auswahl von bewährten Bauteilen und/oder die Anwendung von bewährten Sicherheitsprinzipien, um damit kritische Fehler oder Ausfälle zu minimieren oder auszuschließen (siehe ISO 13849-2:2012).

— Verbesserung der Struktur des Teilsystems, um den gefährlichen Einfluss eines Fehlers zu vermeiden. Einige Fehler könnten eine Erkennung erfordern, wodurch eine redundante und/oder überwachte Struktur 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 einer redundanten und/oder überwachten Struktur.

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

Die Anforderungen hinsichtlich Ausfälle infolge gemeinsamer Ursache (CCF) müssen erfüllt sein.

Für Teilsysteme, deren PL- oder SIL-Werte und PFH_D-Werte vom Hersteller angegeben werden, ist keine weitere Einschätzung (z. B. Bewertung von DC, MTTF, CCF, SRESW) notwendig.

6.1.2 Zusammenhang zwischen dem Performance Level und dem Sicherheits-Integritätslevel

Wenn eine Sicherheitsfunktion mit einem oder mehreren Teilsystem(en) entworfen wird, muss jedes Teilsystem entweder mithilfe von PLs nach diesem Dokument oder mithilfe von SILs nach IEC 62061 und IEC 61508 ausgelegt werden. Teilsysteme, die nach IEC 61508 oder IEC 62061 entworfen sind, dürfen zwar angewendet werden, müssen sich aber auf solche Teilsysteme 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 PLs und SILs.

Tabelle 4 — Zusammenhang zwischen dem Performance Level und dem Sicherheits-Integritätslevel

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

ANMERKUNG 1 PL a zeigt keine Gemeinsamkeit mit 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

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 Abschnitt 4 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 ein verbessertes Leistungsverhalten vorwiegend durch die Verbesserung der Fehlertoleranz und/oder der Diagnosemaßnahmen 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, 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 bei Auftreten von Fehlern.

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)	Teilsysteme und/oder deren Schutzeinrichtungen 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 Funktions-kanals	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 überprüft werden.	Zwischen den Prüfungen kann das Auftreten eines Fehlers zum Verlust der Teilfunktion führen. Der Verlust der Teilfunktion wird bei der Überprüfung 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. Sicherheitsbezogene Teile müssen so entworfen sein, 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	niedrig bis hoch	niedrig bis mittel	siehe Anhang F

Kategorie	Zusammenfassung der Anforderungen an die Teilsysteme	Verhalten der Teilfunktion	Prinzip zum Erreichen der Sicherheit	$MTTF_D$ jedes Funktions-kanals	DC_{avg}	CCF
4 (siehe 6.1.3.2.6)	Die Anforderungen von Kategorie B müssen erfüllt sein und bewährte Sicherheitsprinzipien müssen angewendet werden. Sicherheitsbezogene Teile müssen so entworfen sein, 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	hoch	hoch, einschließlich der Fehleranhäufung	siehe Anhang F
ANMERKUNG Für vollständige Anforderungen siehe 6.1.3.2.						

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

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;

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;

g) dem Diagnosedeckungsgrad; und

h) dem Ausfall infolge gemeinsamer Ursache 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 Dies bedeutet für Kategorie 3 und Kategorie 4 nicht notwendigerweise, dass alle Teile physisch redundant sind, sondern dass redundante Mittel bereitstehen, 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 Architekturen. Eine Abweichung von diesen Architekturen ist immer möglich, aber jede Abweichung muss durch angemessene analytische Werkzeuge (z. B. Markov-Modelle, Fehlerbaumanalyse) begründet werden, sodass das Teilsystem den erforderlichen Performance Level erreicht. Für ein Teilsystem, das von den vorgesehenen Architekturen abweicht, muss eine ausführliche Berechnung durchgeführt werden, um das Erreichen des erforderlichen Performance Levels nachzuweisen.

Die Linien und Pfeile in Bild 7 bis Bild 11 stellen logische Verbindungsmittel und, soweit zutreffend, logische Diagnosemittel 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 einer 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. Entwürfe, welche die Merkmale der entsprechenden Kategorie im Allgemeinen erfüllen, entsprechen der vorgesehenen Architektur der Kategorie.

6.1.3.2.2 Kategorie B

Ein Teilsystem der Kategorie B muss mindestens nach den maßgebenden Normen entworfen, gebaut, ausgewählt, zusammengestellt und kombiniert worden sein und die grundlegenden Sicherheitsprinzipien (siehe 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 bearbeiteten Materials, z. B. die Reinigungsmittel in einer Waschmaschine; und

— anderen relevanten äußeren Einflüssen, z. B. mechanische Schwingungen, elektromagnetische Störungen, Unterbrechungen oder Störungen der Energieversorgung.

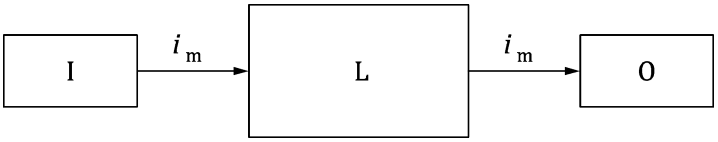
Die $MTTF_D$ des Kanals muss mindestens niedrig sein.

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

ANMERKUNG 1 In Systemen der Kategorie B gibt es keinen 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 (EMV) (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 EMV-Anforderungen 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

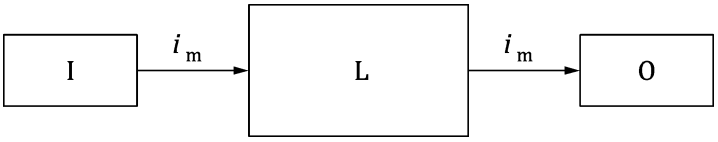
Für Kategorie 1 müssen die gleichen Anforderungen erfüllt sein wie für Kategorie B nach 6.1.3.2.2. Zusätzlich gilt Folgendes.

Teilsysteme der Kategorie 1 müssen unter Verwendung bewährter Bauteile nach 6.1.11 und bewährter Sicherheitsprinzipien (siehe ISO 13849-2:2012) entworfen und gebaut werden.

ANMERKUNG 1 In Systemen der Kategorie 1 gibt es keinen Diagnosedeckungsgrad (DC_{avg} = keiner). In solchen Strukturen (Einkanalsysteme) ist die Betrachtung von CCF nicht relevant. Die $MTTF_D$ des Kanals muss hoch sein.

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. „Bewährten Sicherheitsprinzipien“ nach 3.1.47 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; und/oder

b) vor dem Anlauf anderer Bewegungen; und/oder

c) unmittelbar bei Anforderung der Sicherheitsfunktion; und/oder

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 wurde.

Für PL_r d muss die Ausgabe (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 der Ausgang der Testeinrichtung (OTE) eine Warnung ausgibt.

Bei der Berechnung von DC_{avg} brauchen nur die Blöcke des Funktionskanals berücksichtigt zu werden (d. h. I, L und O in Bild 9) und nicht die Blöcke des Testkanals.

Für Kategorie 2 ist Folgendes erforderlich:

— Anforderungsrate $\leq$ 0,01 Testrate (siehe Anhang K, 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 (siehe Tabelle K.1, ANMERKUNG 1).

Der Diagnosedeckungsgrad aller Teile des Funktionskanals (I, L, O) muss mindestens niedrig sein. Die $MTTF_D$ des Funktionskanals muss, abhängig vom erforderlichen Performance Level, 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.

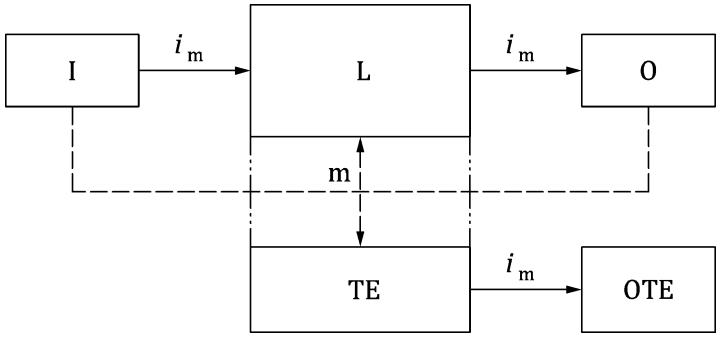
ANMERKUNG 1 Das Testen der Blöcke im Funktionskanal kann beispielsweise anhand einer direkten oder indirekten Überwachung erfolgen.

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

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

— der Verlust der Teilfunktion durch den Test erkannt wird.

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



Legende

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

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 3.1.47 müssen ebenfalls befolgt werden. Zusätzlich gilt Folgendes.

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

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 Diagnosedeckungsgrad 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).

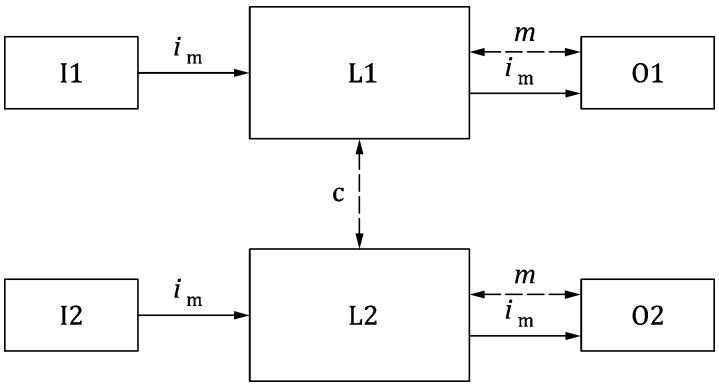
ANMERKUNG 2 Falls aufgrund der Technologie und Anwendung notwendig, kann das Normungsgremium, das Typ-C-Normen erarbeitet, weitere Einzelheiten zur Fehlererkennung nennen.

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 7.1.3.2.2. Die bewährten Sicherheitsprinzipien nach 3.1.47 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 z. B. FMEA brauchen unerkannte Ausfälle mit einer sehr geringen Wahrscheinlichkeit nicht bei der Fehleranhäufung berücksichtigt zu werden.

Der 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

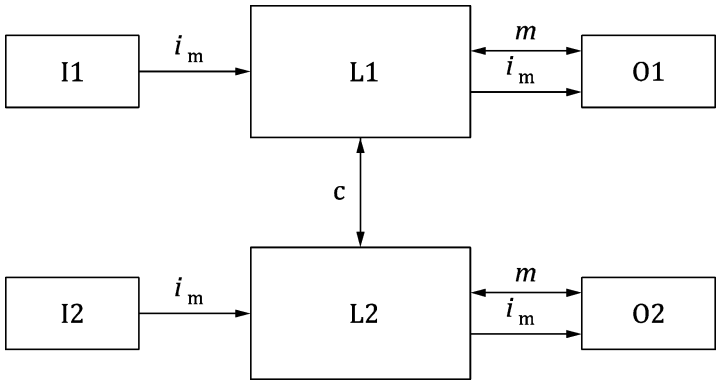
— bei Auftreten eines einzelnen Fehlers die Sicherheitsfunktion weiterhin ausgeführt wird,

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

— 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 Diagnosedeckungsgrad 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

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 gefährlicher Ausfallrate entspricht die $MTTF_D$ dem Kehrwert der gefährlichen Ausfallrate, umgerechnet in Jahre.

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

1) Verwendung von Herstellerdaten;

   ANMERKUNG 1 Bei der Verwendung der vom Hersteller angegebenen $MTTF_D$-Daten für elektromechanische Geräte wird die angenommene Schalthäufigkeit des Geräts so berücksichtigt, dass sie der tatsächlichen Anwendung entspricht.

2) Anwendung der Verfahren von Anhang C;

3) Felderfahrungswerte der Ausfallrate 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 Felderfahrungswerte sind in IEC 61508-7:2010, B.5.4, ausführlicher beschrieben.

4) Wählen von 10 Jahren.

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, was es erlaubt, in Kategorie 4 mehr als 3 Teilsysteme seriell zu kombinieren und 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 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]

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

Der Diagnosedeckungsgrad (DC) wird als das Verhältnis zwischen der Rate von erkannten gefahrbringenden Ausfällen und der Rate aller gefahrbringenden Ausfälle bestimmt. Der Diagnosedeckungsgrad 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 Diagnosedeckungsgrad muss entweder auf der Fehlzustandsart- und -auswirkungsanalyse (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 Fehlzustandsart- und -auswirkungsanalyse (FMEA, siehe IEC 60812 und EN 50495, Anhang B) oder ein ähnliches Verfahren angewendet werden, um alle maßgebenden Fehler und/oder Ausfallarten 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 (siehe Tabelle 7).

Tabelle 7 — Diagnosedeckungsgrad

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

ANMERKUNG 1 Für ein Teilsystem, das aus mehreren Teilen besteht, wird in dieser Norm 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 Diagnosedeckungsgrad und 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

Die Wahrscheinlichkeit, dass zwei oder mehr eigenständige Fehler eine gemeinsame Ursache haben, muss für Teilsysteme der Kategorien 2, 3 und 4 berücksichtigt werden. In Kategorie 2 bezieht sich CCF auf Fehler infolge gemeinsamer Ursache im Funktionskanal und im Testkanal. In Kategorie 3 und Kategorie 4 bezieht sich CCF auf Fehler 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 Umwelteinflüssen;

— Betriebsausfälle;

— menschliche Fehler bei der Spezifikation der Sicherheitsanforderungen, dem Hardware- und Softwareentwurf.

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 Funktionssicherheitsplan aufgeführt sein. Der Funktionssicherheitsplan ist dafür vorgesehen, Maßnahmen für das Verhindern einer fehlerhaften Spezifikation, einer fehlerhaften Umsetzung oder von Modifizierungsproblemen bereitzustellen.

Während des Entwurfsprozesses ist insbesondere auf die Steuerung und Vermeidung von systematischen Ausfällen zu achten (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, ist jedem Teilsystem eine vorgesehene Architektur zuzuordnen, wodurch ein einziges SRP/CS mehrere Architekturen enthalten kann.

Der vereinfachte Ansatz basiert auf Folgendem:

a) der Gebrauchsdauer (T_M), 20 Jahre (siehe 3.1.33);

b) den konstanten Ausfallraten innerhalb der Gebrauchsdauer;

c) ausreichenden Maßnahmen, um zu verhindern, dass Ausfälle infolge gemeinsamer Ursache eintreten (β-Faktor von 2 %, für einen Leitfaden siehe Anhang F oder IEC 61508-6:2010, Anhang D).

ANMERKUNG 1 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. Üblicherweise wird das SRP/CS ausgetauscht, wenn die Gebrauchsdauer erreicht ist.

Um eine Gebrauchsdauer von 20 Jahren zu beanspruchen, sind die Anforderungen von 6.1.3.2.2 für Kategorie B einzuhalten. 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 mittleren Dauer bis zum gefahrbringenden Ausfall ($MTTF_D$) jedes Kanals und vom DC_{avg} ab.

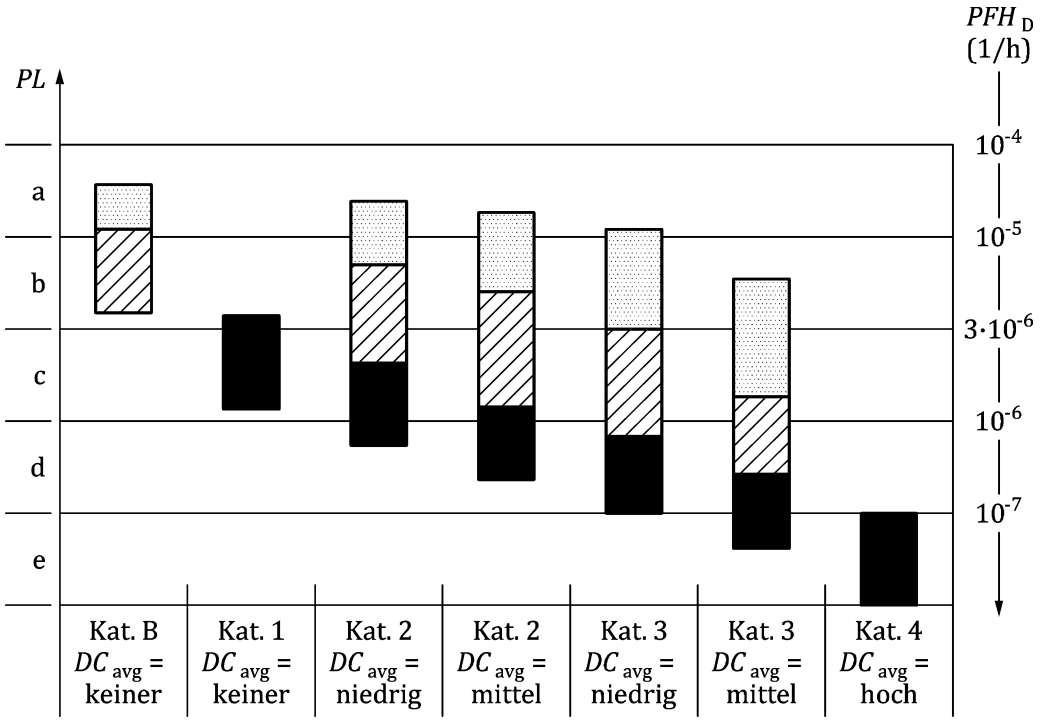
Enthalten die Teilsysteme Software, gelten die Anforderungen von Abschnitt 7.

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 Ausfälle infolge gemeinsamer Ursache 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 Ausfälle infolge gemeinsamer Ursache) 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.



Legende

PFH_D durchschnittliche Wahrscheinlichkeit 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 PL

6.1.9 Alternatives Verfahren für die Bestimmung des Performance Levels und der PFH_D 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 mit unterschiedlichen PL 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 Diagnosedeckungsgrad und die Maßnahmen gegen CCF umgesetzt werden.

Im schlimmsten Fall 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 des DC_{avg} auf den arithmetischen Mittelwert aus allen DC-Einzelwerten des Bauteils in dem Funktionskanal 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. an DC_{avg} und CCF sowie an systematische Ereignisse, müssen für jede Kategorie (siehe 6.1.3) erfüllt werden.

6.1.9.3 Eingaben und Ausgaben

Tabelle 8 zeigt den Zusammenhang zwischen erreichbarem PL (wie in Bild 12) und den Kategorien. PL a und PL b können mit Kategorie B erzielt werden, sofern die grundlegenden Sicherheitsprinzipien eingehalten werden. PL c kann mit Kategorie 1 oder Kategorie 2 erzielt werden, sofern bewährte Bauteile und bewährte Sicherheitsprinzipien angewendet werden.

PL d kann mit Kategorie 3 bzw. PL e kann mit Kategorie 4 erzielt werden, sofern bewährte Bauteile sowie grundlegende und bewährte Sicherheitsprinzipien angewendet werden.

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

Kategorie[a]	Zusätzliche Anforderungen		Abgeschätzte PFH_D (1/h)	Abgeschätzter erreichbarer PL[b]
B		→	$5{,}0 \times 10^{-6}$	b
1		→	$1{,}7 \times 10^{-6}$	c
2	Es werden ausschließlich bewährte Bauteile verwendet	→	$2{,}9 \times 10^{-7}$	c

Kategorie[a]	Zusätzliche Anforderungen		Abgeschätzte PFH_D (1/h)	Abgeschätzter erreichbarer PL[b]
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 MTTFD.

[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

Wenn keine $MTTF_D$-Daten verfügbar sind, kann ein konservativer Ansatz unter Anwendung von $MTTF_D$ 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 und bewährte Bauteile sind anzuwenden. Der maximale erreichbare PL ist PL c (siehe Anhang K).

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

Kategorie 4 ist von diesem Verfahren ausgeschlossen.

Anhand der Kategorie, der $MTTF_D$ und des DC_{avg} können der PL und die PFH_D 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 List 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 ob der Fehlerausschluss für diese Ausschlüsse verantwortlich gemacht wird. 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 listet die wichtigen Fehler und Ausfälle für die verschiedenen Technologien auf. Die Fehlerlisten sind nicht vollständig und es müssen gegebenenfalls weitere Fehler berücksichtigt und aufgezählt werden. In solchen Fällen muss das Verfahren für die Bewertung ebenfalls verständlich ausgearbeitet werden. Für Bauteile, die nicht in ISO 13849-2:2012 aufgelistet sind, muss ein Verfahren durchgeführt werden, mit dem der Einfluss von wahrscheinlichen Fehlern und/oder Ausfällen von Bauteilen bewertet wird, z. B. Fehlzustandsart- und -auswirkungsanalyse (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 Ausfall infolge gemeinsamer Ursache betrachtet werden (dies ist bekannt als ein CCF, 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.

Möglicherweise werden einige Fehler vom Hersteller ausgeschlossen und einige Fehler werden vom Teilsystemintegrator ausgeschlossen.

Es muss eine spezifische Charakterisierung der Art des Fehlers, der ausgeschlossen wird, vorliegen. Es wäre nicht akzeptabel, einfach zu sagen, dass ein Bauteil aufgrund von Verschleiß nicht bricht, sich verzieht oder verschlechtert. Es müsste angegeben werden, unter welchem direkten Einfluss das Bauteil aufgrund von Verschleiß nicht 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 dem 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,

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

b) in den informativen Anhängen A bis D von ISO 13849-2:2012 aufgelistet sein muss, oder

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

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

Komplexe elektronische 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 Abschnitt 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 leistungssteuernden Elemente. Die Kombination der Teilsysteme könnte 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 oder 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 bezogen werden. Die nach IEC 61508 oder IEC 62061 berechneten PFH-Werte mit den vorstehenden Beschränkungen können als PFH_D-Werte nach diesem Dokument betrachtet werden.

Die Kategorie kann nicht immer von einem nach IEC 62061 oder IEC 61508 validierten Teilsystem abgeleitet werden und ist auch nicht erforderlich.

6.2.2 Bekannte PFH_D-Werte

Bei der Kombination von Teilsystemen mit bekannten PFH_D-Werten können die PFH_D-Werte wie unten angegeben miteinander kombiniert werden. Es wird angenommen, dass *n* separate Teilsysteme SB_1 bis SB_n vorliegen. 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_D-Werte aller SB_n bekannt sind, dann ist die PFH_D des SRP/CS die Summe aller PFH_D-Werte der *n* einzelnen SB_n. Der PL des SRP/CS wird beschränkt durch:

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

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

ANMERKUNG Ein Beispiel dieses Verfahrens ist in Anhang H enthalten.

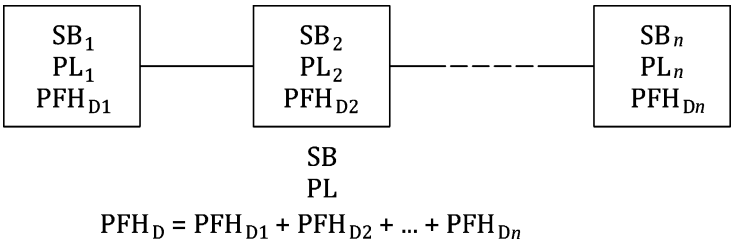


Bild 13 — Kombination von Teilsystemen zum Erreichen des Gesamt-PL

6.2.3 Unbekannte PFH_D-Werte

Wenn die PFH_D-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 — Berechnung 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_D-Bereichen für jeden PL (siehe Tabelle 2), die eine Art logarithmische Skala bilden.			

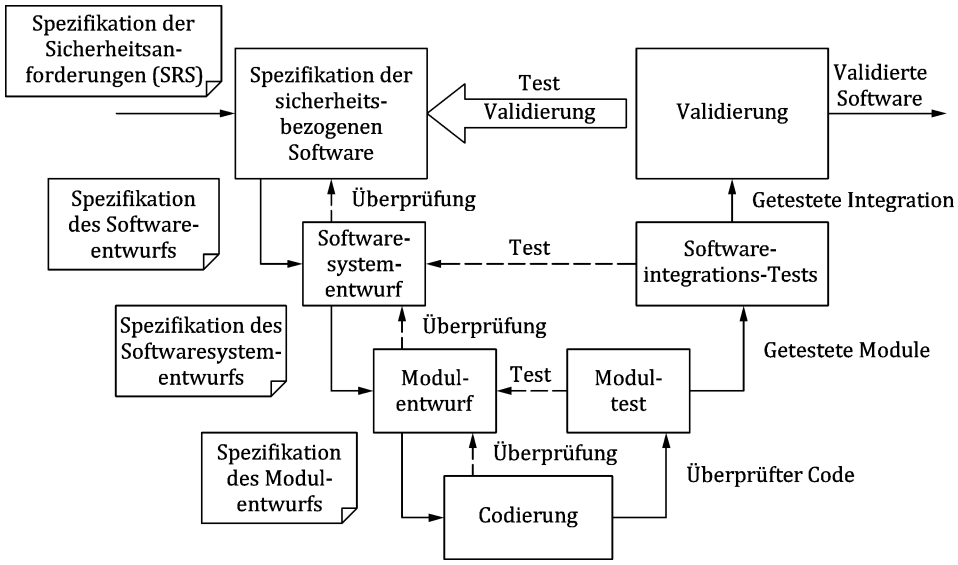
7 Software-Sicherheitsanforderungen

7.1 Allgemeines

Aktivitäten in Zusammenhang mit der Entwicklung von sicherheitsbezogener Embedded-Software oder sicherheitsbezogener Anwendungssoftware müssen im Wesentlichen darauf abzielen, Fehler während der Lebensdauer der Software 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 darüber, welche Maßnahmen für SRASW gelten, die unter Verwendung von LVL ausgeführt wird, und welche Maßnahmen für SRASW gelten, die unter Verwendung von FVL ausgeführt wird.



Legende
⟶ Ergebnis
⇢ Verifizierung

Bild 14 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. Dies gilt normalerweise für die Verwendung der modulbasierten Programmierung mit LVL, bei der nur einfache Zusammenschaltungen konfiguriert werden müssen, wodurch die Eingaben und Ausgaben auf einen vordefinierten Wertesatz beschränkt werden, einschließlich einer Kombination von Modulen.

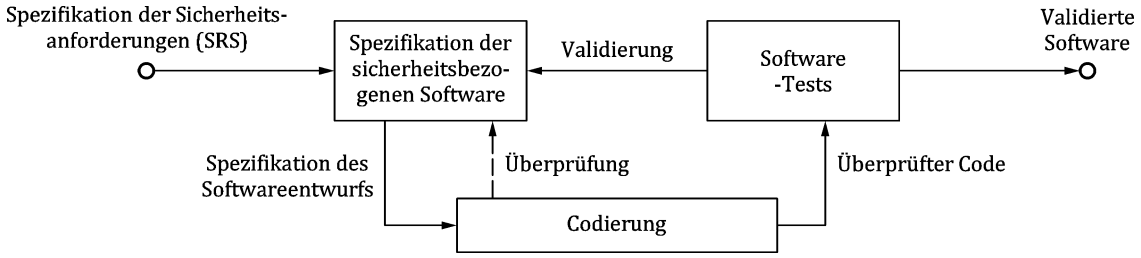


Bild 14 b — Vereinfachtes V-Modell für Software, falls zuvor beurteilte sicherheitsbezogene Hardware- und Softwaremodule in Kombination mit LVL verwendet werden

7.2 Programmiersprache mit eingeschränktem Sprachumfang und Programmiersprache mit nicht eingeschränktem Sprachumfang

7.2.1 Programmiersprache mit eingeschränktem Sprachumfang

Die Programmiersprache mit eingeschränktem Sprachumfang ist eine Software-Programmiersprache, deren Notation textuell oder graphisch ist oder Eigenschaften sowohl für kommerzielle als auch für industrielle programmierbare elektronische Steuerungen mit einer Reihe von Funktionen aufweist, die auf ihre Anwendung beschränkt sind (IEC 61508-4:2010, 3.2.14).

ANMERKUNG Die Programmiersprache mit eingeschränktem Sprachumfang (LVL) sollte vom Softwareentwickler so entworfen werden, dass sie leicht verständlich ist, und sollte sich streng auf die durchzuführenden Anwendungen konzentrieren.

Wenn Sicherheitsfunktionen und nicht sicherheitsbezogene Funktionen in derselben Hardware-Umgebung ausgeführt werden, dann ist nachzuweisen, dass die Sicherheitsfunktionen unter Fehlerbedingungen von der nicht sicherheitsbezogenen Funktion nicht beeinflusst werden. Dies kann unter anderem das Blockieren oder das Verzögern einer Sicherheitsantwort sein, die jederzeit ausgeführt werden muss.

Im Folgenden sind Beispiele für Programmiersprachen mit eingeschränktem Sprachumfang 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

Diese Art von Sprache wurde für Softwareentwickler entwickelt und bietet die Möglichkeiten, eine Vielzahl von Funktionen und Anwendungen zu implementieren.

Typische Beispiele für Systeme, die die Programmiersprache mit nicht eingeschränktem Sprachumfang (FVL) nutzen, sind Universalrechner. Im Maschinenbereich wird FVL in Embedded-Software und gelegentlich in Anwendungssoftware eingesetzt.

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

7.2.3 Entscheidung zwischen Programmiersprache mit eingeschränktem Sprachumfang und Programmiersprache mit nicht eingeschränktem Sprachumfang

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.

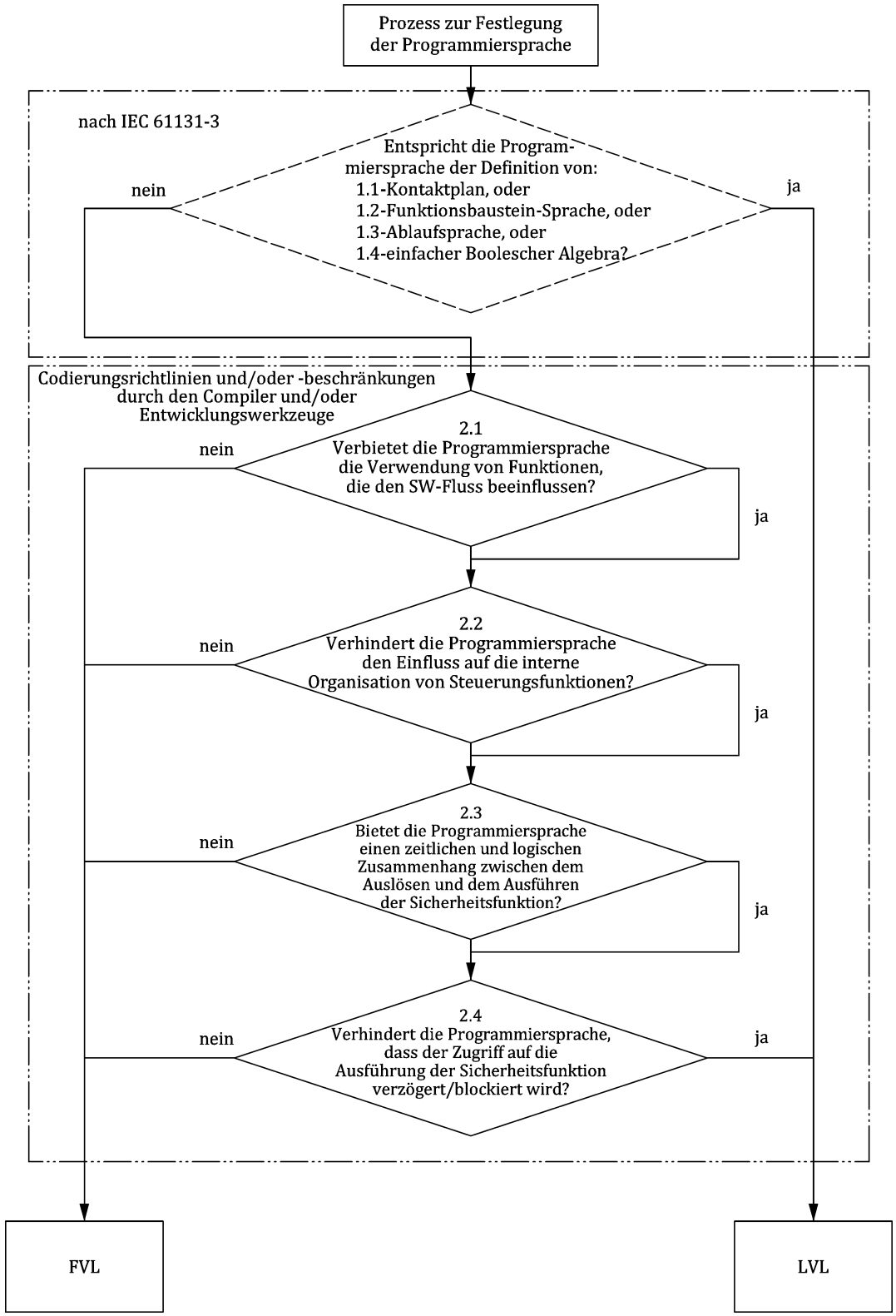


Bild 15 —Entscheidungshilfe bezüglich FVL bzw. LVL

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

BEISPIEL 2 Wenn eine Art strukturierter Text oder eine Teilmenge von C mit Beschränkungen der Compiler- und/oder Entwicklungswerkzeuge und mit restriktiven Codierungsrichtlinien verwendet wird, die 7.3 a) und b) erfüllen, und wenn eine der Fragen 2.1 bis 2.4 mit „ja“ beantwortet werden kann, 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 mit „nein“ beantwortet, ist das Ergebnis FVL.

BEISPIEL 4 Wenn eine Funktionsbausteinsprache mit selbst deklarierten Funktionsbausteinen in strukturiertem Text nach IEC 61131-3 verwendet wird und die Einschränkungen von 7.3 a) und b) erfüllt sind, ist das Ergebnis LVL.

ANMERKUNG 1 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.

ANMERKUNG 2 Anhang N gibt einen Überblick darüber, welche Maßnahmen für SRASW und SRESW gelten, die entweder mithilfe von LVL oder FVL ausgeführt werden.

7.3 Sicherheitsbezogene Embedded-Software

Für sicherheitsbezogene Embedded-Software (SRESW) in Bauteilen 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 Entwurfs, z. B. Spezifikation des Softwareentwurfs, Spezifikation des Softwaresystementwurfs, Spezifikation des Modulentwurfs, Codelisten einschließlich Bemerkungen;

c) modularer und strukturierter Entwurf und Codierung, z. B. Hierarchie und Einschränkung der Funktionalität, klare Programmstruktur, Definition von Schnittstellen, gut strukturierter Aufrufgraph, Vermeidung von Unterbrechungen, Verwendung von Codierungsrichtlinien;

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

e) wenn softwarebasierte Maßnahmen zur Steuerung zufälliger Hardwarefehler verwendet werden, wird die korrekte Ausführung überprüft, z. B. korrekte Ausführung von Diagnosemaßnahmen, RAM/ROM/CPU-Tests, Hardwaretests, Plausibilitätsprüfungen;

f) Funktionstests, z. B. 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 Bauteilen mit einem PL_r c oder d müssen die folgenden zusätzlichen Maßnahmen angewendet werden:

h) Projektmanagement und Qualitätsmanagement vergleichbar mit beispielsweise IEC 61508, z. B. Definition des Arbeitsablaufs, der Verantwortlichkeiten, Konfigurationsmanagement;

i) Dokumentation aller maßgebenden Aktivitäten im Lebenszyklus der Softwaresicherheit, z. B. Dokumentation von Prüfungen, Tests, Validierung und Verifizierung;

j) Konfigurationsmanagement zur Identifizierung aller Konfigurationspunkte und -dokumente in Zusammenhang mit einer SRESW-Version, z. B. Versionskontrolle von Codelisten, Modulen, Entwurfsdokumenten, Testplänen, Freigabekontrolle, Archivierung;

k) strukturierte Spezifikation mit Sicherheitsanforderungen und strukturiertem Aufbau;

l) sicherer Umgang mit geeigneten Programmiersprachen und rechnergestützten Werkzeugen;

m) modulare und strukturierte Programmierung, Abgrenzung von nicht sicherheitsbezogener Software, beschränkte Modulgrößen mit vollständig definierten Schnittstellen, Verwendung von Entwurfs- und Codierungsrichtlinien;

n) Verifizierung des Codes durch Walk-through/Überprüfung mit einer Kontrollflussanalyse, z. B. zur Überprüfung auf Fehler, Qualität der Bemerkungen, 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.

Die SRESW für Bauteile 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 Maßnahmen für PL_r c oder d erreicht werden.

ANMERKUNG Für SRESW mit Diversität in Entwurf und Codierung für Bauteile von Teilsystemen der Kategorie 3 oder Kategorie 4 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.

Bauteile, für die die SRESW-Anforderungen nicht erfüllt sind, z. B. SPS ohne Sicherheitsbewertung durch den Hersteller, dürfen unter 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 begrenzt mit Kategorie 2 oder PL d mit Kategorie 3 und es ist notwendig, die Diversitätsanforderungen der CCF zu erfüllen, wobei beide Kanäle voneinander verschiedene Technologien/Konstruktionen oder physikalische Prinzipien nutzen.

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

7.4 Sicherheitsbezogene Anwendungssoftware

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

SRASW, in LVL geschrieben und mit den folgenden Anforderungen übereinstimmend, kann einen PL a bis PL e erreichen. Wenn SRASW in FVL geschrieben ist, müssen die Anforderungen für SRESW angewendet werden, und PL a bis PL e ist erreichbar. Entscheidungshilfen bezüglich FVL bzw. LVL sind in 7.4 angegeben.

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

Bei SRASW für Bauteile 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 a;

— 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).

a) Die Spezifikation des Softwareentwurfs muss überprüft (siehe auch Anhang J) und jeder Person, die am Lebenszyklus beteiligt ist, 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 Steuerung von Hardware-Ausfällen, um den erforderlichen Diagnosedeckungsgrad und die Reaktion auf einen Fehler zu erreichen.

b) Auswahl der Werkzeuge, Bibliotheken, Sprachen:

   1) Werkzeuge müssen für die jeweilige Anwendung geeignet sein. Bei einem PL e, der mit einem Bauteil und dessen Werkzeug erreicht wird, muss das Werkzeug der einschlägigen Bauteilnorm entsprechen. Falls zwei verschiedene Bauteile mit unterschiedlichen Werkzeugen verwendet werden, können Erfahrungen aus dem erfolgreichen Betrieb in früheren Projekten ausreichend sein. Technische Fähigkeiten, die Bedingungen erkennen, die zu systematischen Fehlern führen könnten (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. Werkzeuge sollten Sprachenteilmengen und Programmierrichtlinien erzwingen oder mindestens den Entwickler leiten oder führen.

   2) Wann immer vernünftigerweise durchführbar, sollten validierte Funktionsbausteinbibliotheken (FB, en: function block) verwendet werden — entweder vom Werkzeughersteller gelieferte sicherheitsbezogene FB-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, z. B. eine anerkannte Teilmenge der IEC 61131-3-Sprachen.

c) Der Softwareentwurf 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 Funktionsbausteinbibliotheken oder anderer Modulstrukturen zum Erreichen einer einfachen Code-Lesbarkeit und -Testfähigkeit;

3) Funktionsbausteine mit begrenzter Codelänge;

4) innerhalb des Funktionsbausteins sollte die Ausführung des Codes mit einem Eingangspunkt und einem Ausgangspunkt erfolgen;

5) Architektur des Modells in drei Stufen: Eingänge ⇒ Verarbeitung ⇒ Ausgänge (siehe Bild 16 und Anhang J);

6) Zuordnung des Sicherheitsausgangs zu nur einem Programmteil; und

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

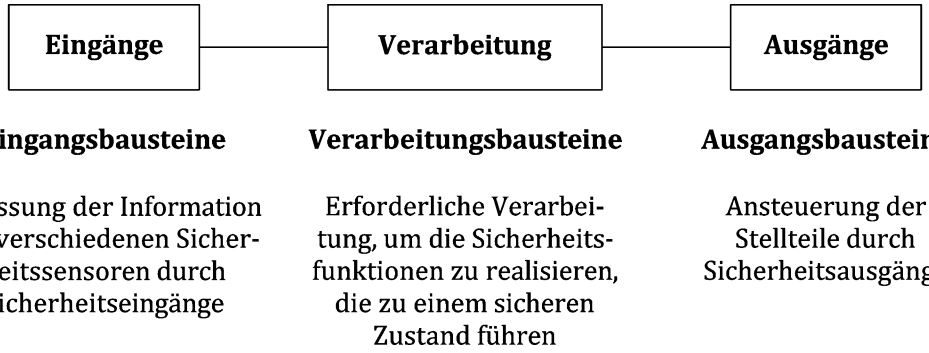


Bild 16 — Allgemeines Architekturmodell für Software

d) Wo SRASW und nicht-SRASW in einem Bauteil 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 könnte, 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 wird empfohlen und sollte Testfälle mit Abschlussbedingungen und erforderlichen Werkzeugen 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 Funktionsbausteinbibliothek und ausreichender Kommentierung der Netzwerke/Anweisung und Deklarationszeilen.

h) Verifizierung:

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

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

i) Konfigurationsmanagement:

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

j) Änderungen:

Bevor eine Änderung der SRASW vorgenommen wird, muss eine Auswirkungsanalyse durchgeführt werden, um die Übereinstimmung mit dem Softwareentwurf sicherzustellen. Nach Änderungen müssen angemessene Lebenszyklusaktivitäten stattfinden. Zugriffsrechte auf die Änderungen müssen geprüft und die Änderungshistorie muss dokumentiert werden.

7.5 Softwarebasierte manuelle Parametrisierung

7.5.1 Allgemeines

Der Anwendungsbereich dieses Unterabschnitts ist ausschließlich auf manuelle, softwarebasierte Parametrisierung beschränkt, die von einer befugten Person durchgeführt und kontrolliert wird. Siehe auch 5.2.3.6 sowie Tabelle M.2.

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

BEISPIELE Ein Wandler mit integrierten Teilfunktionen kann über ein PC-gestütztes Konfigurationswerkzeug parametrisiert 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 Parametrisierung ist es, sicherzustellen, dass die sicherheitsbezogenen Parameter, die für eine Sicherheitsfunktion oder eine Teilfunktion festgelegt sind, ordnungsgemäß in die Hardware eingegeben werden, welche die Sicherheitsfunktion bzw. die Teilfunktion ausführt. Es können verschiedene Verfahren angewendet werden, um derartige Parameter einzustellen; selbst die auf DIP-Schaltern basierende Parametrisierung kann angewendet werden, um sicherheitsbezogene Parameter einzustellen oder zu ändern. PC-gestützte Werkzeuge mit geeigneter Parametrisierungssoftware, allgemein bekannt als Konfigurations- oder Parametrisierungswerkzeuge, werden jedoch immer gebräuchlicher.

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

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

Falls das Konfigurations- oder Parametrisierungswerkzeug in Übereinstimmung mit diesem Dokument oder IEC 61508 voreingestellt ist, z. B. im Hinblick auf sein dazugehöriges Teilsystem, dann wird davon ausgegangen, dass keine gefahrbringenden Ausfälle durch die in 7.5.2 angegebenen Einflüsse oder irgendeinen anderen vernünftigerweise vorhersehbaren Einfluss eintreten werden. Es gelten die Anforderungen von 7.5.5, wenn eine softwarebasierte manuelle Parametrisierung mit dem voreingestellten Werkzeug durchgeführt wird.

Falls ein sicherheitsbezogenes Teilsystem oder SRP/CS nicht wie vorstehend beschrieben durch softwarebasierte manuelle Parametrisierung parametrisiert werden kann, gilt 8.5 nicht.

7.5.2 Einflüsse auf sicherheitsbezogene Parameter

Während der softwarebasierten manuellen Parametrisierung können die Parameter auf unterschiedliche Weise beeinflusst werden, wie beispielsweise durch:

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

b) Softwarefehler des Parametrisierungswerkzeugs;

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

d) Hardwarefehler des Parametrisierungswerkzeugs;

e) Fehler während der Übertragung von Parametern vom Parametrisierungswerkzeug 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 Parametrisierungsvorgangs, z. B. durch elektromagnetische Störung oder Energieverlust;

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

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

— die Parameter werden durch den Parametrisierungsprozess weder vollständig noch teilweise aktualisiert, ohne die für die Parametrisierung verantwortliche Person darüber zu benachrichtigen;

— die Parameter sind weder vollständig noch teilweise korrekt;

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

7.5.3 Anforderungen an die softwarebasierte manuelle Parametrisierung

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

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

Es ist möglich, die Anforderungen zu erfüllen, indem ein vorgefertigtes Teilsystem verwendet wird; anderenfalls muss der Entwurf den nachstehend in diesem Dokument aufgeführten Anforderungen entsprechen.

Bei Verwendung eines vorgefertigten SRP/CS oder Teilsystems, das für die softwarebasierte manuelle Parametrisierung geeignet ist, ist es das Ziel, gefahrbringende Ausfälle durch die in 7.5.2 angegebenen Einflüsse oder andere vernünftigerweise vorhersehbare Einflüsse zu verhindern. Die Validierung des vorgefertigten Teilsystems muss den Aspekt der Parametrisierung enthalten.

Wenn ein SRP/CS oder Teilsystem, das für die softwarebasierte manuelle Parametrisierung 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 Parametrisierung muss als sicherheitsbezogener Aspekt des SRP/CS-Entwurfs betrachtet werden, der in der Spezifikation der Sicherheitsanforderungen 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 Parametrisierung 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 Parametrisierungs-Hardware und -Software;

6) Beherrschung der Auswirkung der Unterbrechung der Energieversorgung;

d) das Parametrisierungswerkzeug muss alle Anforderungen an ein SRP/CS nach diesem Dokument oder nach 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 Parametrisierungswerkzeug; 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 Parametrisierungswerkzeug. 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 Softwarewerkzeug zur Parametrisierung ein Gerät nutzt, das nicht speziell für diesen Zweck vorgesehen ist (z. B. Personalcomputer 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 eine Diversität in der/den Funktion(en) aufweisen, um systematische Ausfälle zu verhindern.

7.5.4 Verifizierung des Parametrisierungswerkzeugs

Die folgenden Verifizierungsaktivitäten müssen durchgeführt werden, um die grundlegende Funktionalität des Parametrisierungswerkzeugs 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 Parametrisierung unter Verwendung eines Geräts ausgeführt wird, das nicht speziell für diesen Zweck vorgesehen ist (z. B. Personal Computer oder Ähnliches).

7.5.5 Dokumentation der softwarebasierten manuellen Parametrisierung

Softwarebasierte manuelle Parametrisierung muss mithilfe des dafür vorgesehenen Parametrisierungswerkzeugs 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-Parametrisierung sowie anschließende Änderungen an der Parametrisierung müssen dokumentiert werden. Die Dokumentation muss Folgendes umfassen:

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

b) das Datum oder die Versionsnummer des Datensatzes;

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

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

e) eindeutige Identifizierung der sicherheitsbezogenen Parameter.

8 Verifizierung, ob der erreichte Performance Level dem erforderlichen Performance Level entspricht

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 (siehe Bild 4). Wenn das nicht der Fall ist, wird eine Wiederholung des Prozesses, wie in Bild 4 beschrieben, notwendig.

Die PL verschiedener Teilsysteme, die Teil einer Sicherheitsfunktion sind, müssen größer oder gleich dem erforderlichen Performance Level dieser Sicherheitsfunktion sein (siehe 5.3 und 6.1.1).

9 Ergonomische Entwurfsaspekte

Die Schnittstelle zwischen den Bedienern und den SRP/CS muss so gestaltet und konstruiert sein, dass die Gefährdungen während des bestimmungsgemäßen Gebrauchs und der vernünftigerweise vorhersehbaren Fehlanwendung der Maschine durch Nichtbeachtung ergonomischer Grundsätze minimiert werden.

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 Übergehen 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 Gesamtspezifikation der Sicherheitsanforderungen 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 Funktionstests (siehe 10.4) unter vorhersehbaren Bedingungen in Übereinstimmung mit dem Validierungsplan.

ANMERKUNG 1 Die Validierung beschränkt sich auf das entworfene SRP/CS oder einen Teil davon, der die Sicherheitsfunktionen unterstützt, die erforderlich sind, um die beabsichtigte Risikominderung auf Maschinenebene nach ISO 12100 zu erreichen. Die Validierung des SRP/CS soll Teil des gesamten Validierungsprozesses für die Maschine sein.

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 Spezifikation der Sicherheitsanforderungen (nach Abschnitt 6) angegebenen Anforderungen erfüllt.

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

a) den festgelegten funktionalen Anforderungen der Sicherheitsfunktionen, die von diesem Teil ausgeführt werden, wie in der Spezifikation der Sicherheitsanforderungen festgelegt;

b) die Anforderungen des festgelegten PL müssen 7.1.1 entsprechen:

   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. 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“. Es kann notwendig sein, dass einige Teile der Analyse später als geplant erfolgen, wenn der Entwurf weiterentwickelt ist.

Wenn es aufgrund der Größe des Systems, der Komplexität des Systems 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 sicherheitsbezogenen Teilen auf die verbleibende Steuerung in Zusammenhang mit ihrer Verwendung in der Maschine.

Das Gleichgewicht zwischen der Analyse und den Tests hängt von der Technologie ab, die für die sicherheitsbezogenen Teile zum Einsatz kommt, sowie von dem erforderlichen Performance Level. Für die Kategorien 2, 3 und 4 muss die Validierung der Sicherheitsfunktion außerdem einen Test durch geeignete Fehlereinspeisung umfassen, um dies zu belegen. Unter anderem wird die Reaktion auf einen Fehler durch die enthaltene Diagnosefunktion ausgelöst.

„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.

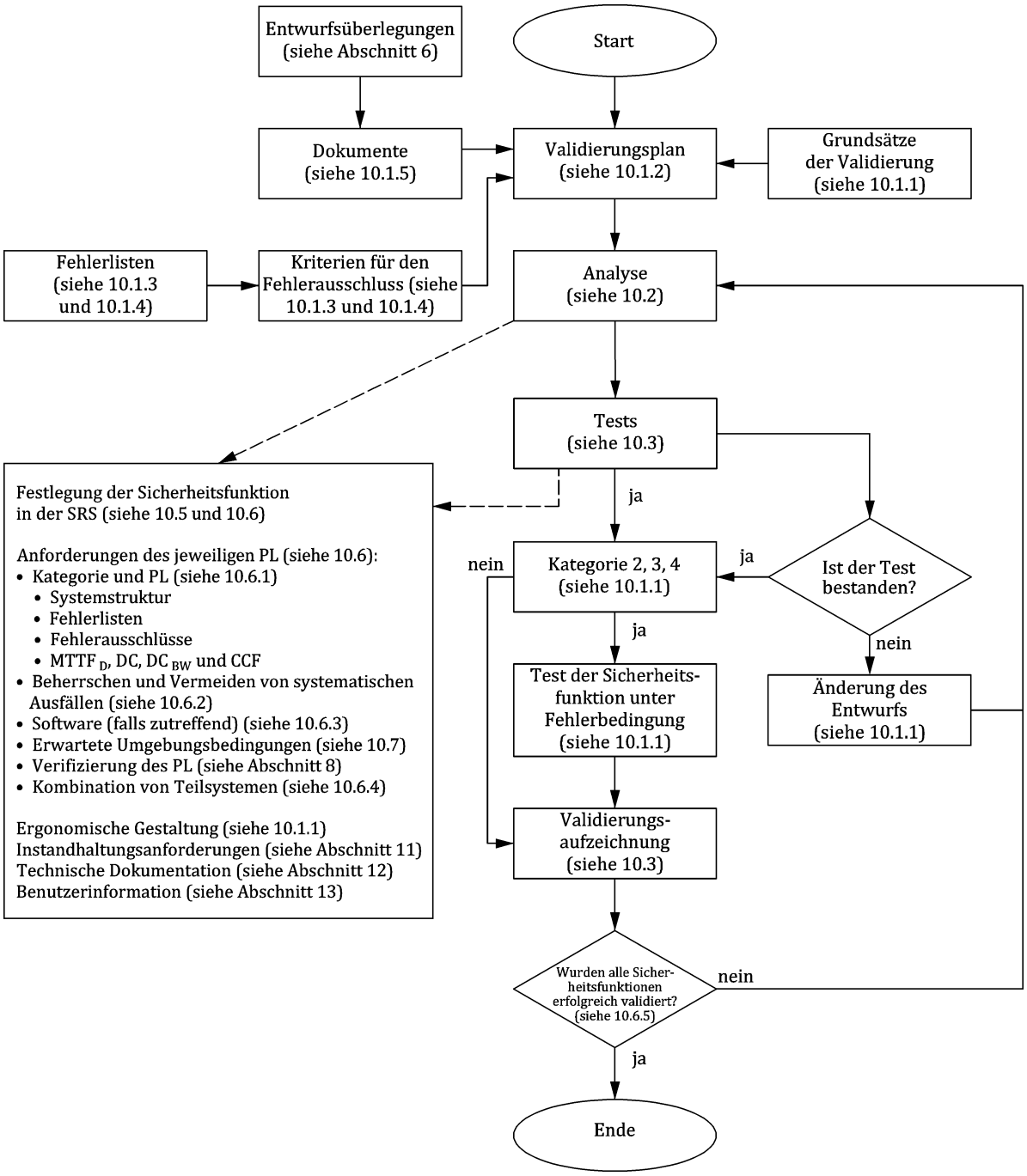


Bild 17 — Übersicht über den Validierungsprozess

10.1.2 Validierungsplan

Der Validierungsplan muss die Anforderungen an die Durchführung des Validierungsprozesses festlegen und beschreiben und muss allen 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 der Prüfung;

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) ausnahmsweise alle weiteren Fehler, für die die allgemeine(n) Liste(n) einen Ausschluss nicht zulässt/zulassen, für die jedoch eine Begründung und sinnvolle Erklärung für ihren Ausschluss gegeben 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 Spezifikation der Sicherheitsanforderungen und des Beitrags des SRP/CS zur Risikominderung. Dokumente, die in ausreichendem Umfang die Angaben aus der nachfolgenden Liste enthalten, müssen in die Validierung aufgenommen werden, um nachzuweisen, dass die

sicherheitsbezogenen Teile die festgelegten Sicherheitsfunktionen mit dem erforderlichen PL und/oder der erforderlichen Kategorie ausführen:

a) Spezifikation der Sicherheitsanforderungen einschließlich der geforderten Eigenschaften jeder Sicherheitsfunktion, z. B. Ansprechzeit (z. B. 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, Aufstellung;

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) aufgelisteten sicherheitsbezogenen Teile 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 übertragen 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, aufgelistet 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 Angaben darüber erforderlich, wie der PL und die durchschnittliche Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde (PFH_D) bestimmt werden. Die Dokumentation der quantifizierbaren Aspekte muss Folgendes enthalten:

— das sicherheitsbezogene Blockdiagramm (siehe Anhang B) oder die vorgesehene Architektur nach 6.1.3.2;

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

— die Bestimmung der Kategorie.

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 Performance Level erreicht.

ANMERKUNG 2 Soweit möglich, ist eine deutliche und rückverfolgbare Verweisung auf bestehende Dokumente ausreichend.

10.2 Validierung der Spezifikation der Sicherheitsanforderungen

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).

Die Anforderungen an alle Sicherheitsfunktionen der Maschinensteuerung müssen dokumentiert werden.

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

Die Validierung darf anhand von Prüfungen und Inspektionen der Spezifikation der Sicherheitsanforderungen durchgeführt werden, insbesondere, um nachzuweisen, dass sämtliche Aspekte berücksichtigt wurden von:

— den vorgesehenen Anwendungsanforderungen und Sicherheitserfordernissen (d. h. Risikobeurteilung); und

— den Betriebs- und Umgebungsbedingungen sowie möglichem menschlichen Versagen (z. B. Missbrauch.

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, Anhang F 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 Argumente;

— 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 Ausgangsereignissen und zur Berechnung der Wahrscheinlichkeit von Ausgangsereignissen aus der Wahrscheinlichkeit der auslösenden Ereignisse führen können. Sie können auch angewendet werden bei der Untersuchung der Folgen von erkannten Mehrfachfehlern.

   BEISPIEL 1 Fehlerbaum-Analyse (FTA, siehe IEC 61025), Ereignisbaumanalyse (ETA, siehe IEC 62502).

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

   BEISPIEL 2 Fehlzustandsart- und -auswirkungsanalyse (FMEA, siehe IEC 60812) und Ausfalleffekt- und Kritizitätsanalyse (FMECA, siehe IEC 60812).

10.4 Validierung durch Prüfung

10.4.1 Allgemeines

Die Prüfungen müssen Teil der Validierung sein, es sein denn, es handelt sich um Kategorie B oder Kategorie 1 und eine Analyse allein wird als unzureichend angesehen.

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 Übereinstimmung 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 die SRP/CS eingegeben werden. Die sich ergebende 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, Arbeitsablauf, 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 5 K bei Temperaturmessungen liegen und bei 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 das 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 sicherheitsbezogenen Teile 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 Auswirkung im schlimmsten Fall (en: worst case effect) bei einer Fehlereingabe ist mittels Analyse zu bestimmen und der Fehler ist zu diesem geeigneten entscheidenden Zeitpunkt einzugeben. Übliche Prüfverfahren sind:

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

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, könnten jedoch auch einige Fälle enthalten, die aus der Analyse der Schaltpläne oder der Software abgeleitet sind;

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

e) Prüfungen durch Fehlereinspeisung in den tatsächlich vorhandenen 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. Herstellung, Art, Bauart) zu bestätigen;

d) Funktionsprüfung der Sicherheitsfunktionen in allen Betriebsarten der Maschine, um festzustellen, ob sie mit den festgelegten Eigenschaften übereinstimmen (siehe Abschnitt 6). 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, könnten jedoch auch einige Fälle enthalten, die aus der Analyse der Schaltpläne oder der Software abgeleitet sind;

e) erweiterte Funktionsprüfung, um vorhersehbare ungewöhnliche Signale oder Kombinationen von Signalen aus einer beliebigen Eingangsquelle zu überprüfen, einschließlich Energieunterbrechung und -wiederkehr und fehlerhafte Betätigungen;

f) 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
Prüfverfahren für die Sicherheitsfunktion(en)	—	—	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

Anforderungen	Kategorie				
	B	1	2	3	4
Maßnahmen gegen systematische Ausfälle	X	X	X	X	X
Maßnahmen gegen Softwarefehler	X	—	X	X	X
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 Systemintegrität (siehe Anhang G, Software, CCF).

In diesem Zusammenhang erfolgt die Validierung von $MTTF_D$, DC_{avg} und CCF üblicherweise durch eine Analyse und Sichtprüfung.

Die $MTTF_D$-Werte für Bauteile (einschließlich der B_{10D}-, T_{10D}- und n_{op}-Werte) müssen einer Plausibilitätsprüfung unterzogen werden. Wenn Forderungen nach einem Fehlerausschluss bedeuten, dass bestimmte Bauteile nicht zur $MTTF_D$ des Kanals beitragen, ist die Plausibilität des Fehlerausschlusses zu überprüfen.

ANMERKUNG 1 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 von Bauteilen (Elementen des Teilsystems) und/oder logischen Blöcken 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 Hardwareanalyse und Funktionsprüfungen unter Umgebungsbedingungen.

ANMERKUNG 2 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 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:

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

   — weiteren Maßnahmen zur Vermeidung systematischer Ausfälle nach Anhang G; und

   — 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 durch das Qualitätsmanagement die Ursachen für systematische Fehler im Fertigungsprozess vermieden werden.

ANMERKUNG 1 Systematische Ausfälle können durch Fehler während des Entwurfs und der Integration verursacht worden sein (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 PLr 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, Unterlassungen 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 Steuersignalflusses und Prozeduren mithilfe der Softwaredokumentation (Steuersignal-Flussdiagramm, 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.

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 PFHD und PL/SIL der Teilsysteme (siehe 7.2);

— Überprüfung/Verifizierung der korrekten Bewertung des PL auf der Grundlage der Kategorie, von DCavg und MTTFD, CCF und Maßnahmen gegen systematische Ausfälle;

— Überprüfung/Verifizierung, ob der vom SRP/CS erreichte PL den PLr erfüllt, der in der Spezifikation der Sicherheitsanforderungen für die Maschine festgelegt ist: PL ≥ PLr.

10.7 Validierung der Umgebungsanforderungen

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

Die Validierung muss durch Analyse und, sofern notwendig, 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 Dauerhaftigkeit;

— elektrische Nennwerte und Energieversorgung;

— klimatische Bedingungen (Temperatur und Luftfeuchte); und

— elektromagnetische Verträglichkeit (Störfestigkeit).

Wenn Prüfungen erforderlich sind, um die Einhaltung der Umweltanforderungen festzustellen, sind die in den einschlägigen 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 ein Element des Validierungsprozesses nicht bestanden hat, muss in der Validierungsaufzeichnung beschrieben werden, welche Elemente der Analyse/Prüfung für die Validierung nicht bestanden wurden. Es muss sichergestellt sein, dass alle sicherheitsbezogenen Teile 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 Folgenden 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, gibt es Bestimmungen, 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 die festgelegte Leistung des SRP/CS aufrechtzuerhalten.

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

Bei der Konstruktion eines SRP/CS müssen folgende Faktoren 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 menschlichen Fähigkeiten;

— Begrenzung der Anzahl von Spezialwerkzeugen und -ausrüstungen für solche speziellen Anwendungen;

— Anzeichen, 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);

— erforderlicher 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) Spezifikation der Sicherheitsanforderungen einschließlich der Spezifikation jeder Sicherheitsfunktion (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_D-Wert;

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

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

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) Aufzeichnungen über die Prüfung, Verifizierung und Validierung, soweit zutreffend.

ANMERKUNG Im Allgemeinen ist diese Dokumentation für die herstellerinterne Verwendung gedacht und wird nicht an den Benutzer weitergegeben.

13 Benutzerinformation

13.1 Allgemeines

Die Benutzerinformation des SRP/CS muss alle maßgebenden Anleitungen für die vorgesehene Zielgruppe 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) Grenzen (z. B. Umgebungsbedingungen), geeignete Informationen, um die weitere Rechtfertigung der Fehlerausschlüsse sicherzustellen, z. B. hinsichtlich Änderung, Instandhaltung und Reparatur;

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

c) Ansprechzeit;

d) Betriebsgrenzen (z. B. Anforderungshäufigkeit);

e) Anzeigen und Alarme;

f) Überbrückungsfunktion und zeitweiliges Aufheben der Sicherheitsfunktionen;

g) Steuerungs- und Rückstellarten;

h) Instandhaltung (siehe Abschnitt 11);

i) Checklisten für die Instandhaltung;

j) Zugang zu und Austausch von SRP/CS;

k) Mittel zur leichten und sicheren Fehlersuche;

l) Prüfintervalle, soweit maßgebend;

m) Gebrauchsdauer (z. B. ISO 13855:2010).

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):

— datierte Verweisung auf dieses Dokument (d. h. „ISO 13849-1:2022“);

— die Kategorien der Teilsysteme, aus denen sich das SRP/CS zusammensetzt;

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

— der PFH_D-Wert für das SRP/CS, 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 Benutzer bereitgestellt werden.

Dazu können unter anderem die relevanten Aspekte von 13.1 und 13.2 zählen. Außerdem müssen maßgebende Informationen über die Prüfung der Sicherheitsfunktionen 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 und Sicherheitsfunktionen;

i) Anweisungen zu Instandhaltungsarbeiten, die Fachwissen und/oder besondere Fähigkeiten 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 Benutzern (z. B. Bedienpersonen) durchgeführt werden dürfen. Das Instandhaltungspersonal sollte darauf hingewiesen werden, welche Teile für die Sicherheit entscheidend sind und nur durch „vergleichbare“ Teile oder ähnliches ersetzt werden dürfen. In Fällen, in denen sicherheitskritische Teile durch nicht vergleichbare Teile ersetzt werden, ist voraussichtlich eine erneute Validierung der Sicherheitsfunktion erforderlich;

k) Kontrolle der Leitlinien, Schilder und Vorrichtungen für gefahrbringende Energiemengen (manuelle Maßnahmen/andere Vorrichtungen);

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 Erreichen von T_{10D} oder vor Ablauf des T_{10D}-Zeitraums (siehe auch C.4.2).

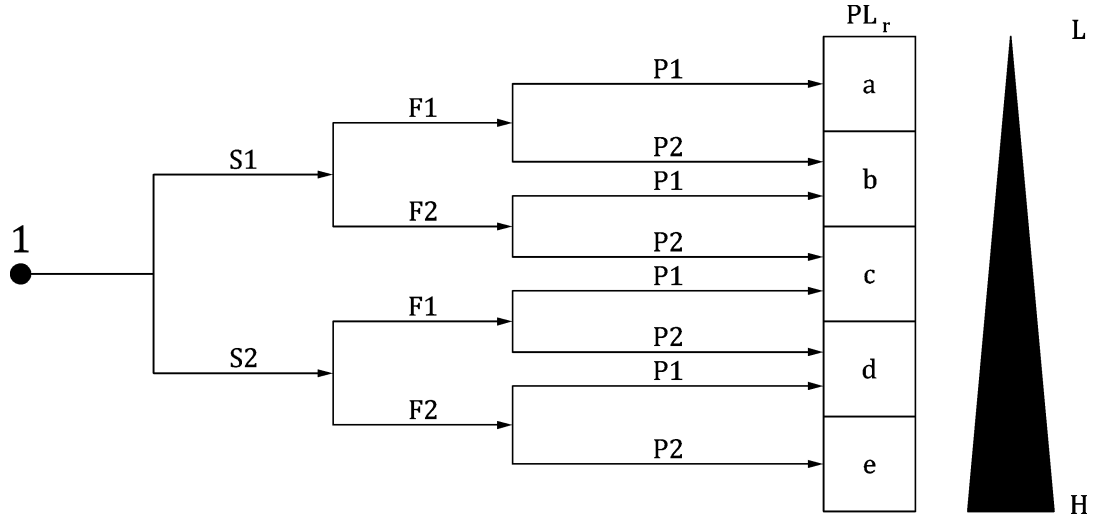
ANMERKUNG Für ergänzende Informationen siehe ISO 20607:2019 und IEC 60204-1:2016, 17.2, f.

Wenn eine Instandhaltungsaktivität eine Änderung des SRP/CS voraussetzt, ergibt sich daraus die Notwendigkeit einer Funktionsprüfung der maßgebenden Sicherheitsfunktionen.

Anhang A
(informativ)

Leitlinien für die Bestimmung des erforderlichen Performance Levels

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 der Gefährdung oder Begrenzung des Schadens
P1 möglich unter bestimmten Bedingungen
P2 kaum möglich

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

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

A.2 Auswahl des erforderlichen Performance Levels

Anhang A beschäftigt sich mit dem Beitrag zur Risikominderung, der durch die sicherheitsbezogenen Teile der betrachteten Steuerung 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.

ANMERKUNG 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 niedrig eingestuft werden kann, ist die Herabstufung um einen Performance Level möglich. 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.

Der Graph in Bild A.1 basiert auf der Situation vor Festlegung der beabsichtigten Sicherheitsfunktion (siehe 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 4).

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

— Schwere der Verletzung (S);

— Häufigkeit und Dauer der Gefährdungsexposition (F);

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

Die Erfahrung hat gezeigt, dass diese Parameter kombiniert werden können, wie in Bild A.1 gezeigt, um eine Abstufung des Beitrags zur erforderlichen Risikominderung von niedrig bis hoch zu erhalten. Es wird betont, dass dies ein qualitatives Verfahren ist, das nur eine Abschätzung eines erforderlichen Performance Levels liefert.

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. Allerdings könnte die folgende Erklärung die Entscheidungsfindung in Zweifelsfällen 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 Durchschnittwerts bewertet werden, der im Verhältnis zur Gesamtzeit gesehen werden kann, über die die Einrichtung verwendet wird. Ist es z. B. notwendig, im zyklischen Betrieb 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.

A.3.3 Möglichkeit zur Vermeidung der Gefährdung oder Begrenzung des Schadens

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 Gefährdung auftritt (z. B. schnell oder langsam);

b) Möglichkeit zur Vermeidung der Gefährdung, (z. B. durch Flucht);

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

d) Betrieb durch ausgebildete und geeignete Bedienungspersonen;

e) Betrieb mit oder ohne Beaufsichtigung.

Wenn ein Gefährdungsereignis eintritt, sollte P1 nur dann ausgewählt werden, wenn eine realistische Möglichkeit besteht, dass eine Gefährdung vermieden wird, oder dass deren Auswirkung deutlich verringert wird; ansonsten sollte P2 ausgewählt werden.

Der Parameter P kann mithilfe des folgenden Ansatzes bestimmt werden:

— 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.

Es ist nur eine Auswahl für jeden Faktor von Tabelle A.1 möglich.

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

Faktor	C	B	A
1. Benutzung der Maschine durch		Laie	Fachkraft

Faktor	C	B	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 (heiße/kalte Oberfläche, Strahlung usw.))	Ereignis mit hoher Geschwindigkeit keine Zeit zum Entkommen, z. B. aufgrund hoher Geschwindigkeit z. B. über 1 000 mm/s, Zeit bis zur Gefährdung < 1 s	Ereignis mit mittlerer Geschwindigkeit begrenzte Zeit zum Entkommen, z. B. aufgrund mittlerer Geschwindigkeit z. B. 251 mm/s bis 1 000 mm/s, Zeit bis zur Gefährdung < 3 s	Ereignis mit niedriger oder sehr niedriger Geschwindigkeit ausreichend Zeit zum Entkommen, z. B. aufgrund niedriger Geschwindigkeit z. B. maximal 250 mm/s, Zeit bis zur Gefährdung ≥ 3 s
3. Räumliche Möglichkeit, sich der Gefährdung zu entziehen	nicht möglich	möglich in weniger als 50 % der Fälle	möglich in mindestens 50 % der Fälle
4. Möglichkeit der Erkennung/Wahrnehmung der Gefährdung	nicht möglich z. B. Notwendigkeit von Geräten, Unfähigkeit die Gefährdung mit den Sinnen wahrzunehmen, Verhindern der Wahrnehmung aufgrund von Umgebungsbedingungen	nur möglich in weniger als 50 % der Fälle	möglich in mindestens 50 % der Fälle
5. Komplexität der Betätigungen (menschliche Interaktion in Bezug auf die Anzahl der Betätigungen und/oder Zeitvorgaben, die für diese Betätigungen vorliegen)		hohe Komplexität z. B. Fehlersuche oder mittlere Komplexität z. B. Verwendung einer Steuerung mit selbsttätiger Rückstellung zum Aufstellen 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.			

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

Gesamtbewertung		Parameter „P“
Einmal oder mehrmals „C“		P2
Keinmal „C“, drei- oder mehrmals „B“		P2
Keinmal „C“, zweimal „B“, der Rest „A“		P1 oder P2, je nach spezifischer Gefährdung
Keinmal „C“, einmal oder keinmal „B“, der Rest „A“		P1

P1 sollte nur dann ausgewählt werden, wenn eine realistische Chance besteht, dass eine Gefährdung vermieden wird, oder dass deren Auswirkung deutlich verringert wird; ansonsten sollte P2 ausgewählt werden.

A.4 Überlagerte Gefährdungen

Bei Anwendung von ISO 13849-1 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 Fehlzustandsart- und -auswirkungsanalyse oder das „Parts-Count"-Verfahren (siehe D.1).

B.2 Sicherheitsbezogenes Blockdiagramm

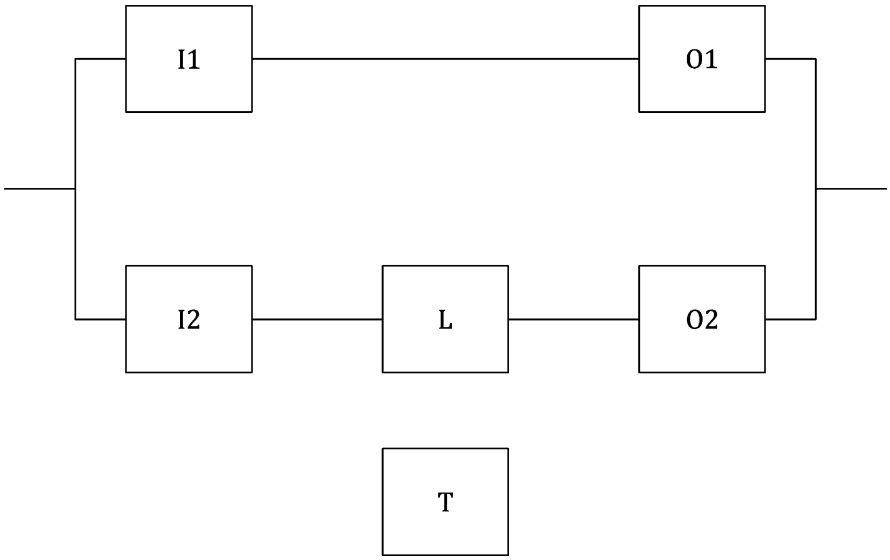
Die durch die Blockmethode definierten Blöcke dürfen verwendet werden, um die logische Struktur des Teilsystems in einem sicherheitsbezogenen Blockdiagramm graphisch darzustellen. Für eine solche graphische Darstellung kann Folgendes hilfreich sein:

— 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); Ausfälle infolge gemeinsamer Ursache können diesen Zustand herbeiführen (siehe 7.1.6 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 Abschätzung von $MTTF_D$-Werten für einzelne Bauteile

C.1 Allgemeines

Anhang C gibt verschiedene Verfahren an, um $MTTF_D$-Werte für einzelne Bauteile zu berechnen oder abzuschätzen; 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 hergestellt oder nach der einschlägigen Norm (siehe Tabelle C.1) für die Konstruktion des Bauteils.

   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	**Einschlägige 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}[a] $< 250\,000$ Zyklen je Jahr	Tabelle C.1 und Tabelle C.2	ISO 4413	$MTTF_D = 1\,200$

	Grundlegende und bewährte Sicherheitsprinzipien nach ISO 13849-2:2012	Einschlägige Normen	Typische Werte: $MTTF_D$ (Jahre), B_{10D} (Zyklen)
Pneumatische Bauteile	Tabelle B.1 und Tabelle B.2	ISO 4414	$B_{10D} = 20\,000\,000$[c]
Relais und Hilfsschütze mit geringer Last	Tabelle D.1 und Tabelle D.2	IEC 61810-3 IEC 60947	$B_{10D} = 20\,000\,000$
Relais und Hilfsschütze mit nominaler Last	Tabelle D.1 und Tabelle D.2	IEC 61810-3 IEC 60947	$B_{10D} = 400\,000$
Näherungsschalter mit geringer Last	Tabelle D.1 und Tabelle D.2	IEC 60947 ISO 14119	$B_{10D} = 20\,000\,000$
Näherungsschalter mit nominaler Last	Tabelle D.1 und Tabelle D.2	IEC 60947 ISO 14119	$B_{10D} = 400\,000$
Schütze mit geringer Last	Tabelle D.1 und Tabelle D.2	IEC 60947	$B_{10D} = 20\,000\,000$
Schütze mit nominaler Last	Tabelle D.1 und Tabelle D.2	IEC 60947	$B_{10D} = 1\,300\,000$
Positionsschalter[b]	Tabelle D.1 und Tabelle D.2	IEC 60947 ISO 14119	$B_{10D} = 20\,000\,000$
Positionsschalter (mit separatem Betätiger, Zuhaltung)[b]	Tabelle D.1 und Tabelle D.2	IEC 60947 ISO 14119	$B_{10D} = 2\,000\,000$
Not-Halt-Geräte[b]	Tabelle D.1 und Tabelle D.2	IEC 60947 ISO 13850	$B_{10D} = 100\,000$
Drucktaster (z. B. Zustimmungsschalter)[b]	Tabelle D.1 und Tabelle D.2	IEC 60947	$B_{10D} = 100\,000$

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

ANMERKUNG 1 B_{10D} wird abgeschätzt als zweimal B_{10} (50 % gefahrbringender Ausfall), wenn keine anderen Angaben vorliegen (z. B. Produktnorm).

„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 %.

ANMERKUNG 2 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 3 Das Reduzieren von Schaltzyklen kann zu einer zunehmenden Wahrscheinlichkeit des Festklebens der Schaltelemente in Steuerventilen führen (siehe ISO 4413).

ANMERKUNG 4 Die $MTTF_D$ für mechanische Bauteile bezieht sich ausschließlich auf mechanisch bewegbare 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.

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 angenommen 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, wie 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, 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 aber weder a) noch b) erreicht 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 $MTTF_D$ von pneumatischen, mechanischen und elektromechanischen Bauteilen und auch von hydraulischen Bauteilen 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 mittlere Dauer bis zum gefahrbringenden Ausfall ($MTTF_D$ 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 Hersteller des 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 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

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

Mit folgenden Annahmen, die in Bezug zur Anwendung des Bauteils getroffen worden sind:

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

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

t_{cycle} 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:

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

Falls die vom Bauteilhersteller angegebene gefährliche Ausfallrate (RDF) 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.

---

1 Wenn die gefährliche Ausfallrate (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.

Durch die Begrenzung der Verwendung des Bauteils auf T_{10D} wird die Aufrechterhaltung des erwarteten Performance Levels der Sicherheitsfunktion ermöglicht.

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: $F(t) = 1 - e^{-\lambda_D t}$. 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_{10D}) begrenzt wird, kann eine konstante gefährliche Ausfallrate (λ_D) während dieser Gebrauchsdauer wie folgt abgeschätzt werden:

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

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

$$F(T_{10D}) = 1 - e^{-\lambda_D T_{10D}} = 10\ \% \qquad \text{d. h.} \qquad \lambda_D = -\frac{\ln(0{,}9)}{T_{10D}} = \frac{0{,}105\ 36}{T_{10D}} \approx \frac{0{,}1}{T_{10D}} \tag{C.6}$$

Mit $\mathrm{MTTF_D} = 1/\lambda_D$ für eine exponentielle Verteilung ergibt dies:

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

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 $\mathrm{MTTF_D} = 1/\lambda_D$ kann die Umwandlung von „Jahren“ in „Stunden“ erfordern, wobei für 1 Jahr = 8 760 Stunden verwendet werden.

C.4.4 Beispiel

Für ein Pneumatikventil gibt ein Hersteller eine mittlere Anzahl von 60 Millionen Zyklen als B_{10D} an. Das Ventil wird an zwei Schichten je Tag mit 220 Arbeitstagen je Jahr verwendet. Die mittlere Zeit zwischen dem Beginn zweier aufeinanderfolgender Zyklen des Ventils wird auf 5 s geschätzt. Dies ergibt die folgenden Werte:

— d_{op} von 220 d je Jahr;

— h_{op} von 16 h je Tag;

— t_{cycle} von 5 s je Zyklus;

— B_{10D} von 60 000 000 Zyklen.

Mit diesen Eingangsdaten können die folgenden Werte berechnet werden:

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

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

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

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

C.5 $\mathrm{MTTF_D}$-Daten für elektrische Bauteile

C.5.1 Allgemeines

Tabelle C.2 bis Tabelle C.7 zeigen einige typische Durchschnittswerte der $\mathrm{MTTF_D}$ für elektronische Bauteile. Die Daten wurden aus der Datenbank der Reihe SN 29500 [46] entnommen. Alle Daten sind allgemeiner Art. Verschiedene Datenbanken sind verfügbar (siehe die unvollständige Liste in den Literaturhinweisen), die $\mathrm{MTTF_D}$-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 dringend 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 $\mathrm{MTTF_D}$ sollte ein Korrekturfaktor angewendet werden, wenn die elektronischen Bauteile außerhalb der angegebenen Werte für Temperatur und Last arbeiten (siehe auch SN 29500).

In der MTTF-Spalte der Tabellen sind die Werte aus SN 29500 für allgemeine Bauteile für alle möglichen Ausfallarten gezeigt, die nicht notwendigerweise gefahrbringende Ausfälle sind. In der $\mathrm{MTTF_D}$-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“ $\mathrm{MTTF_D}$ für Bauteile ist die Durchführung einer FMEA. Einige Bauteile, z. B. Transistoren als Schalter verwendet, können Kurzschlüsse oder Unterbrechungen als Ausfall haben. Nur eine der beiden Arten kann gefährlich sein; deshalb nimmt die Spalte „Bemerkungen“ nur 50 % als gefahrbringende Ausfälle an, was bedeutet, dass die $\mathrm{MTTF_D}$ 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 (verwendet als Schalter)

Transistor	**Beispiel**	**MTTF für Bauteile** Jahre	**$\mathrm{MTTF_D}$ für Bauteile** Jahre **Üblicherweise**	**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 Üblicherweise	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
Gleichrichter-dioden	—	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 pro-grammierbar)	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 Üblicherweise	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
Aluminium-elektrolyt	flüssiger Elektrolyt	22 831	45 662	50 % gefahrbringende Ausfälle
Aluminium-elektrolyt	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 **Üblicherweise**	**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 — Induktoren

Induktor	**Beispiel**	**MTTF für Bauteile** Jahre	**$MTTF_D$ für Bauteile** Jahre **Üblicherweise**	**Bemerkungen**
Für MC-Anwendung	—	38 052	76 104	50 % gefahrbringende Ausfälle
Niederfrequenz-Induktoren 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 **Üblicherweise**	**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 Annäherung, deren Abweichung immer zur sicheren Seite geht.

Die allgemeine Gleichung (D.1) ist:

$$\frac{1}{\mathrm{MTTF_D}} = \sum_{i=1}^{N} \frac{1}{\mathrm{MTTF_{Di}}} = \sum_{j=1}^{\tilde{N}} \frac{nj}{\mathrm{MTTF_{Dj}}} \qquad \text{(D.1)}$$

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 alle Bauteile 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 7, entspricht.

Tabelle D.1 — Beispiel für die Teileliste einer Platine

j	**Bauteil**	**Einheiten** n_j	**$MTTF_{D\,j}$** üblicherweise Jahre	**$1/MTTF_{D\,j}$** üblicherweise 1/Jahr	**$n_j/MTTF_{D\,j}$** üblicherweise 1/Jahr
1	Transistoren, bipolar, Kleinleistung (siehe Tabelle C.2)	2	11 416	0,000 087 6	0, 0,000 175 2
2	Widerstand, Kohlefilm (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 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

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

$MTTF_{D\,C2}$ die Werte für zwei unterschiedliche redundante Kanäle, die jeweils auf einen Höchstwert 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 für Funktionen und Teilsysteme

E.1 Beispiele für den Diagnosedeckungsgrad

Siehe Tabelle E.1.

Tabelle E.1 — Abschätzungen des Diagnosedeckungsgrads

Maßnahme	DC
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 5)
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 Maschinenstellteilen) Gilt nur, wenn der gefahrbringende Ausfall des einzelnen Kanals für redundante Kanäle festgestellt werden kann.	90 % bis 99 %, abhängig von der Anwendung (siehe ANMERKUNG 3)
Direkte Überwachung (z. B. elektrische Überwachung der Steuerungsventile, Überwachung elektromechanischer Einheiten durch Zwangsführung)	99 %
Fehlererkennung durch den Prozess	prozentualer Anteil, der in Abhängigkeit von der jeweiligen Anwendung festzulegen ist, z. B. abhängig von der Anwendung; diese Maßnahme ist allein nicht ausreichend für den erforderlichen Performance Level e (siehe ANMERKUNG 3 und ANMERKUNG 4)
Überwachung einiger Merkmale des Sensors (Ansprechzeit, der Bereich analoger Signale, z. B. elektrischer Widerstand, Kapazität)	60 %

Maßnahme	DC
Logik	
Indirekte Überwachung (z. B. Überwachung durch Druckschalter, elektrische Positionsüberwachung von Maschinenstellteilen, Plausibilitätsprüfung von Endergebnissen) Gilt nur, wenn der gefahrbringende Ausfall des einzelnen Kanals für redundante Kanäle festgestellt werden kann.	90 % bis 99 %, abhängig von der Anwendung (siehe ANMERKUNG 3)
Direkte Überwachung (z. B. elektrische Stellungsüberwachung der Steuerungsventile, Überwachung elektromechanischer Einheiten durch Zwangsführung, Plausibilitätsprüfung von Zwischenergebnissen)	99 %
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 Plausibilitätstests 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)	90 % (abhängig von der Testausführung)
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 %
Verarbeitungseinheit: codierte Verarbeitung (siehe IEC 61508-7:2010, A.3)	90 % bis 99 % (siehe ANMERKUNG 3)
Fehlererkennung durch den Prozess	prozentualer Anteil, der in Abhängigkeit von der jeweiligen Anwendung festzulegen ist, z. B. abhängig von der Anwendung; diese Maßnahme ist allein nicht ausreichend für den erforderlichen Performance Level e (siehe ANMERKUNG 3 und ANMERKUNG 4)

Maßnahme	DC
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 5)
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 5)
Kreuzvergleich von Ausgangssignalen mit dynamischem Test, ohne Erkennung von Kurzschlüssen (bei Mehrfach-Ein-/Ausgängen)	90 %
Kreuzvergleich von Ausgangssignalen und Zwischenergebnissen in der Logik (L) und zeitliche und logische Softwareüberwachung des Programmablaufs und Erkennen statischer Fehler und Kurzschlüsse (bei Mehrfach-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 Maschinenstellteilen) Gilt nur, wenn der gefahrbringende Ausfall des einzelnen Kanals für redundante Kanäle festgestellt werden kann.	90 % bis 99 %, abhängig von der Anwendung (siehe ANMERKUNG 3)
Fehlererkennung durch den Prozess	prozentualer Anteil, der in Abhängigkeit von der jeweiligen Anwendung festzulegen ist, z. B. abhängig von der Anwendung; diese Maßnahme ist allein nicht ausreichend für den erforderlichen Performance Level e! (siehe ANMERKUNG 3 und ANMERKUNG 4)
Direkte Überwachung (z. B. elektrische Überwachung der Steuerungs-ventile, Überwachung elektromechanischer Einheiten durch Zwangsführung)	99 %

Maßnahme	DC
ANMERKUNG 1 Für weitere Abschätzungen des DC siehe z. B. IEC 61508-2:2010, Tabelle A.2 bis Tabelle A.14. ANMERKUNG 2 Wenn mittel oder hoch als DC für die Logik gefordert wird, ist mindestens eine Maßnahme für variablen Speicher, invarianten Speicher und Verarbeitungseinheit mit mindestens je 60 % zu wählen. Es können auch andere Maßnahmen als die in dieser Tabelle aufgelisteten verwendet werden. Für Maßnahmen, für die ein Bereich des Diagnosedeckungsgrades 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“ könnten die Anforderungsrate der Sicherheitsfunktion (r_d) und die Prozessdiagnoserate (Testrate) (r_t) zusammen mit einer Begrenzung des effektiven DC der geprüften Komponente berücksichtigt werden: 1) $r_t/r_d = 1$ DC ist auf 60 % begrenzt; 2) $r_t/r_d = 10$ DC ist auf 90 % begrenzt; 3) $r_t/r_d = 100$ DC ist auf 99 % begrenzt. ANMERKUNG 4 Der Effekt der Testrate (wie oft eine Signaländerung von der Anwendung durchgeführt wird) kann 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 %; — $r_t \geq 1$/Jahr DC ist auf 90 % begrenzt; — $r_t \geq 1$/Monat DC ist auf 99 % begrenzt.	

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.

BEISPIEL 2 ISO/TR 24119 beschreibt mithilfe von Tabellen ein anwendungsbezogenes Schritt-für-Schritt-Verfahren zur Bewertung des Diagnosedeckungsgrades für in Reihe geschaltete Verriegelungseinrichtungen.

BEISPIEL 3 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 den Sensor, der eine sicher begrenzte Geschwindigkeit überwacht, zwischen 90 % und 99 % abgeschätzt werden.

E.2 Abschätzung des durchschnittlichen Diagnosedeckungsgrads

In vielen Systemen können mehrere Maßnahmen zur Fehlererkennung angewendet werden. Diese Maßnahmen könnten unterschiedliche Teile des SRP/CS testen und unterschiedliche Diagnosedeckungsgrade 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:

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

Hierbei sollten alle Bauteile des SRP/CS ohne Fehlerausschluss 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)

Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache

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. Dieser kann mithilfe des Verfahrens von F.2 erzielt 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 eines CCF betrachtet werden.

In Tabelle F.1 sind die Maßnahmen aufgeführt, die auf ingenieurmäßigen Beurteilungen basieren und den Beitrag darstellen, den jede Maßnahme zur Reduzierung von Ausfällen infolge gemeinsamer Ursache leistet.

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, ist eine Punktzahl von null anzunehmen.

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

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

[a] Wenn technische Maßnahmen nicht relevant sind, können die Punkte der rechten Spalte bei der ausführlichen Berechnung berücksichtigt werden.

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

F.3.1 Allgemeines

Die in Tabelle F.1 aufgeführten Maßnahmen sollten hinsichtlich ihrer Wirksamkeit zur Vermeidung oder Beherrschung von Ausfällen infolge gemeinsamer Ursache 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 der Kategorie 2 oder redundante Funktionskanäle der Kategorien 3 und 4.

ANMERKUNG 3 Typische Ursachen sind Überspannung, Überdruck, Überstrom, Überhitzung, Luftfeuchte, Schlag, Vibration, elektromagnetische Störung, 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.3.2 Trennung/Abtrennung

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

a) Trennung der Verdrahtung (z. B. Mehrfachleiterkabel 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, außerdem unter Berücksichtigung von z. B. Zinn-Whiskers (siehe ISO 13849-2:2012, D.2.2).

F.3.3 Diversität

Betrachtungen der Diversität betreffen Folgendes:

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 ein Öffner mit Zwangsöffnung nach IEC 60947-5-1:2020, Anhang K, zum Einsatz kommt; der zweite Positionsschalter wird betätigt, wenn das Schutzgitter geschlossen wird und ein Schließer zum Einsatz kommt;

b) Fühlerelemente 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 neu gekennzeichnet);

d) unterschiedliche Lasten, z. B. der erste Kontakt/das erste Ventil schaltet ohne Last, der zweite Kontakt/das zweite Ventil schaltet unter Last.

F.3.4 Gestaltung/Anwendung/Erfahrung

F.3.4.1 Schutz vor oder Kontrolle von Überspannung, Überdruck, Überstrom, Überhitzung, z. B.:

a) Eingänge und Ausgänge des SRP/CS und die Energieversorgung der Logikeinheit sind vor potentiellen Überspannungs- und/oder Überstrom-Niveaus geschützt (siehe auch IEC 60204-1);

ANMERKUNG Teile des SRP/CS können potentiellen Überspannungs- und/oder Überstrom-Niveaus 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).

F.3.4.2 Die verwendeten Bauteile sind bewährte Bauteile.

Alle in den Kanälen der Sicherheitsfunktion verwendeten Bauteile sind bewährte Bauteile (siehe auch ISO 13849-2:2012).

F.3.5 Beurteilung/Analyse

Für jedes Teil von sicherheitsbezogenen Teilen der Steuerung wurde eine Fehlzustandsart- und -auswirkungsanalyse oder eine Fehlerbaumanalyse durchgeführt, um die möglichen Ursachen für den CCF zu ermitteln, und es wurden deren Ergebnisse berücksichtigt, um Ausfälle infolge gemeinsamer Ursache im Entwurf zu vermeiden.

F.3.6 Ausbildung

Die Konstrukteure wurden ausgebildet (einschließlich eines Ausbildungsnachweises, z. B. ein Ausbildungszertifikat), damit sie die Gründe und Auswirkungen von Ausfällen gemeinsamer Ursache nachvollziehen können.

F.3.7 Umgebung

F.3.7.1 Verhindern von elektromagnetischen Störungen oder Verunreinigungen des Druckmediums

Für elektrische/elektronische Systeme werden Verunreinigungen und elektromagnetische Störungen zum Schutz vor Ausfällen infolge gemeinsamer Ursache entsprechend den einschlägigen Normen (z. B. IEC 61326-3-1, IEC 61000-6-7:2014, IEC 61000-1-2:2016, IEC 61800-5-2) verhindert.

ANMERKUNG 1 Diese EMV-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.3.7.2 Andere Einflüsse

Das SRP/CS besitzt eine Störfestigkeit gegenüber allen maßgebenden Umgebungseinflüssen wie Temperatur, Stoß, mechanische Beanspruchungen, Vibration, Luftfeuchte, wie in den einschlägigen Normen angegeben, z. B. in der Normenreihe IEC 60068, in der die strengeren Anforderungen an die sicherheitsbezogene Anwendung berücksichtigt werden.

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 Abdeckungen auf Systemebene erreicht werden.

F.4 Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache und weitere einschlägige 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 Systemkapazitäten (z. B. Detektionsvermögen von Messfühlern) begrenzt ist.

ANMERKUNG Einige einschlägige Normen (z. B. 62024:2018 für die Anwendung von Schutzeinrichtungen zum Erkennen von anwesenden Personen oder ISO 14119:2014 für die Auswahl und Anwendung von Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen) können Anwendungsgrenzen in Zusammenhang mit den Fähigkeiten des Systems 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 Steuerung 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) Energieabschaltung (siehe ISO 13849-2:2012): die sicherheitsbezogenen Teile der Steuerung (SRP/CS) sollten so gestaltet sein, dass die Maschine bei Trennung von der Energieversorgung einen sicheren Zustand erreicht oder aufrechterhält.

c) 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 und IEC 61508-7:2010, A.8);

e) Maßnahmen zur Beherrschung oder Vermeidung von Auswirkungen der physikalischen Umgebungsbedingungen (z. B. Temperatur, Luftfeuchte, Wasser, Vibration, Staub, korrosive Substanzen, elektromagnetische Störung und deren Wirkungen): das Verhalten des SRP/CS als Reaktion auf die Auswirkungen 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);

g) 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);

i) 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;

— ausfallorientierter Betrieb;

— Überdimensionierung durch einen geeigneten Faktor, womit der Hersteller nachweisen kann, dass eine Herabsetzung die Zuverlässigkeit erhöht.

ANMERKUNG Beispiele für Überdimensionierung sind in ISO 13849-2:2012, Tabelle D.2, enthalten.

G.3 Maßnahmen zur Vermeidung systematischer Ausfälle

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 elektromagnetische Störung (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.

Vermindern 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. 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 Funktionssicherheitsplan erstellt und dokumentiert werden, der bei Bedarf aktualisiert werden sollte. Der Funktionssicherheitsplan ist dafür vorgesehen, Maßnahmen für das Verhindern einer fehlerhaften Spezifikation, einer fehlerhaften Umsetzung oder eines fehlerhaften Änderungsvorhabens bereitzustellen.

Der Funktionssicherheitsplan sollte die maßgebenden Aktivitäten festlegen (siehe Bild 4, Iterativer Prozess für den Entwurf von SRP/CS) und sollte an das Projekt angepasst werden.

ANMERKUNG 1 Der Funktionssicherheitsplan kann Bestandteil anderer Entwurfsunterlagen sein.

ANMERKUNG 2 Der Inhalt des Funktionssichherheitsplans hängt von den jeweiligen Umständen ab, zu denen Folgende zählen können:

— Umfang des Projekts;

— Grad der Komplexität;

— Aktualität des Entwurfs und der Technologie;

— Stand der Normung von Entwurfsmerkmalen;

— mögliche Folge(n) bei Ausfall.

Insbesondere Folgendes sollte der Funktionssicherheitsplan:

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.

Zusätzlich sollte der Black-Box-Test unter Berücksichtigung der Komplexität des SRP/CS und dessen PL angewendet werden.

ANMERKUNG 3 Das Verlangen nach einer Änderung kann beispielsweise auf Folgendes zurückzuführen sein:

— eine Änderung der Spezifikation der Sicherheitsanforderungen;

— 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 verlangten 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 ein Maschinenstellteil anzusteuern. Dies ist kein Funktionsdiagramm/Arbeitsdiagramm und wird nur gezeigt, um das Prinzip der Zusammenschaltung der Kategorien und Technologien in dieser einen Funktion zu zeigen.

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-Stellteils verhindert, wenn der Lichtstrahl unterbrochen ist.

Die Teilsysteme eines SRP/CS, welche die Sicherheitsfunktion ausführen, sind: AOPD, elektronische Steuerlogik, hydraulisches Wegeventil und deren Verbindungsmittel.

Diese kombinierten Teilsysteme liefern eine Stopp-Funktion als Sicherheitsfunktion. 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-Stellteils.

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.

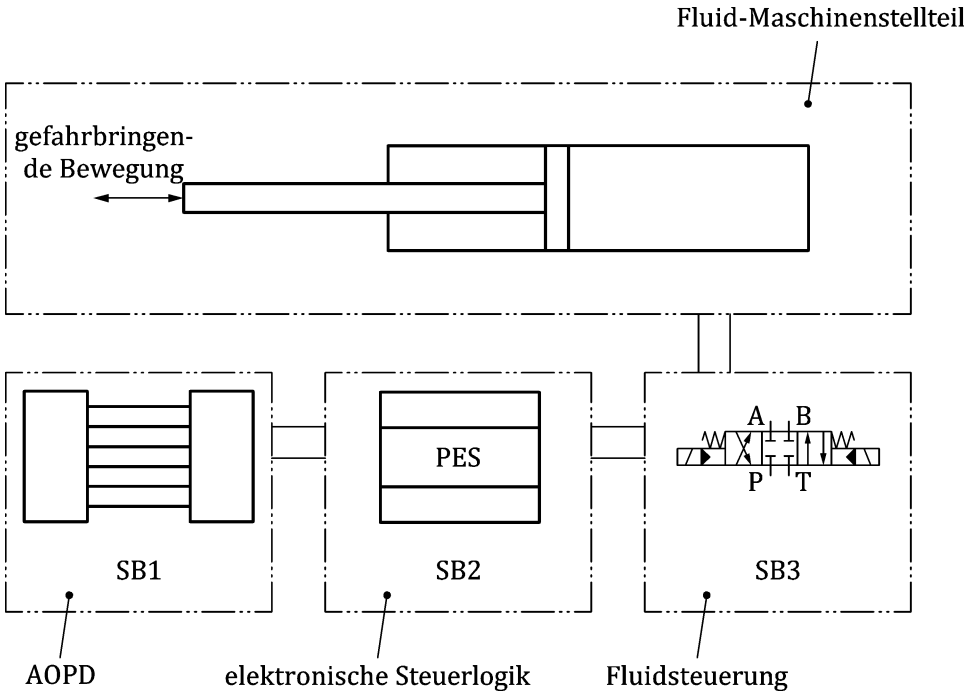
— Kategorie 2, PL c für die berührungslos wirkende Schutzeinrichtung (Lichtschranke). Um die Wahrscheinlichkeit von Fehlern zu vermindern, nutzt diese Einrichtung bewährte Sicherheitsprinzipien;

— Kategorie 3, PL d für die elektronische Steuerlogik. Um den Beitrag der elektronischen Steuerlogik zur Sicherheit zu erhöhen, ist die Struktur dieser Teilsysteme redundant und enthält einige Fehlererkennungsmechanismen, sodass die meisten Einzelfehler erkannt werden;

— Kategorie 1, PL c 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 in diesem Bauteil zu vermindern, besteht dieses aus bewährten Bauteilen, verwendet mit bewährten Sicherheitsprinzipien, und alle Einsatzbedingungen wurden berücksichtigt (siehe 6.1.3.2.4).

ANMERKUNG 1 Die Lage, Größe und Anordnung der Verbindungsmittel wurden ebenfalls berücksichtigt. Diese Kombination führt mit einem $PL_{niedrig}$ c und $N_{niedrig} = 2$ zu einem Gesamt-Performance-Level von PL c (siehe 6.2).

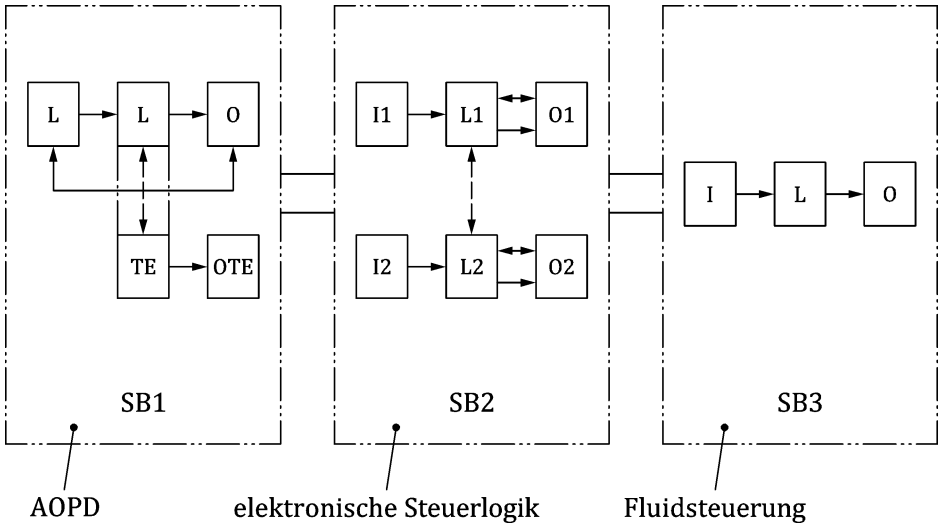
ANMERKUNG 2 Ein einzelner Fehler im Teilsystem der Kategorie 1 oder Kategorie 2 nach Bild H.2 kann zum Verlust der Sicherheitsfunktion führen.



Legende

AOPD aktive optoelektronische Schutzeinrichtung (z. B. Lichtschranke)
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. Lichtschranke)
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

I.1 Allgemeines

Anhang I 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 Steuerungskreise gezeigt. Für das schrittweise Vorgehen siehe Bild I.3.

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 Steuerungskreise 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

Für beide Beispiele können die Anforderungen der Sicherheitsfunktion in Verbindung mit der Verriegelung der Tür der trennenden Schutzeinrichtung wie folgt festgelegt werden.

Die gefahrbringende Bewegung hält an (durch Abbremsen oder Abschalten des Elektromotors), wenn die verriegelte trennende Schutzeinrichtung geöffnet ist.

ANMERKUNG Für das Beispiel B wurde bei der Risikobeurteilung festgestellt, dass ein Verlust des kontrollierten Abbremsens des Motors infolge einer Fehlfunktion (SW2, CC oder SPS) annehmbar war.

Der Mindestabstand zwischen der verriegelten trennenden Schutzeinrichtung und den beweglichen Teilen der Maschine wurde nach ISO 13855:2010 ermittelt, basierend auf dem Anhaltevermögen 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 der Gefährdung, P = P1, möglich unter bestimmten Voraussetzungen.

Diese Auswahl an Risikoparametern führt zu einem erforderlichen Performance Level 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.

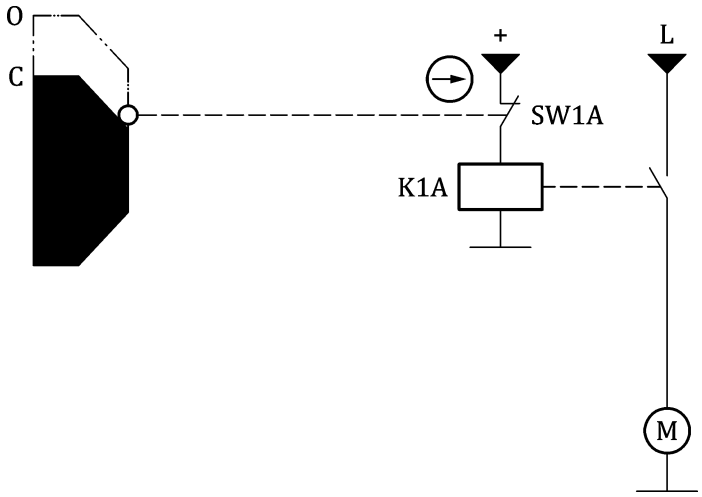
Diese Entscheidungen führen zu einem erforderlichen Performance Level PL_r von d.

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 Identifikation 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	Verriegelung der trennenden Schutzeinrichtung ist offen
C	Verriegelung der trennenden Schutzeinrichtung ist geschlossen
M	Motor
K1A	Hilfsschütz
SW1A	Positionsschalter (NC)
L	Energieversorgung
⊖	Zwangsöffnung

Bild I.1 — Steuerungskreis A zur Ausführung der Sicherheitsfunktion

In diesem Beispiel wird ein Positionsschalter SW1A mit Zwangsöffnung und zwangläufiger Betätigung verwendet, jedoch ohne begründeten Fehlerausschluss für den mechanischen Teil. Der Positionsschalter ist mit einem Hilfsschütz K1A verbunden, der in der Lage ist, die Energiezufuhr zum Motor zu trennen. Die wesentlichen Merkmale dieser sicherheitsbezogenen Teile sind daher:

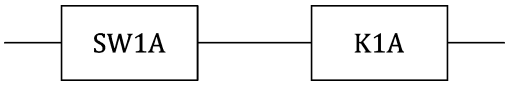
— ein Kanal aus elektromechanischen Bauteilen;

— 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.

Die sicherheitsbezogenen Teile können 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 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:

$$\frac{1}{MTTF_D} = \frac{1}{MTTF_{D,SW1A}} + \frac{1}{MTTF_{D,K1A}} = \frac{1}{113\,636\ \text{Jahre}} + \frac{1}{2\,273\ \text{Jahre}} = \frac{0{,}000\,45}{\text{Jahr}} \quad \text{(I.1)}$$

woraus sich eine $MTTF_D = 2\,222$ Jahre (begrenzt auf 100 Jahre) für den Kanal ergibt, der „hoch“ nach 6.1.4, Tabelle 5, ist.

ANMERKUNG Wenn keine B_{10D}-Informationen zu SW1A oder K1A zur Verfügung stehen, könnte 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 Steuerungskreis 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.

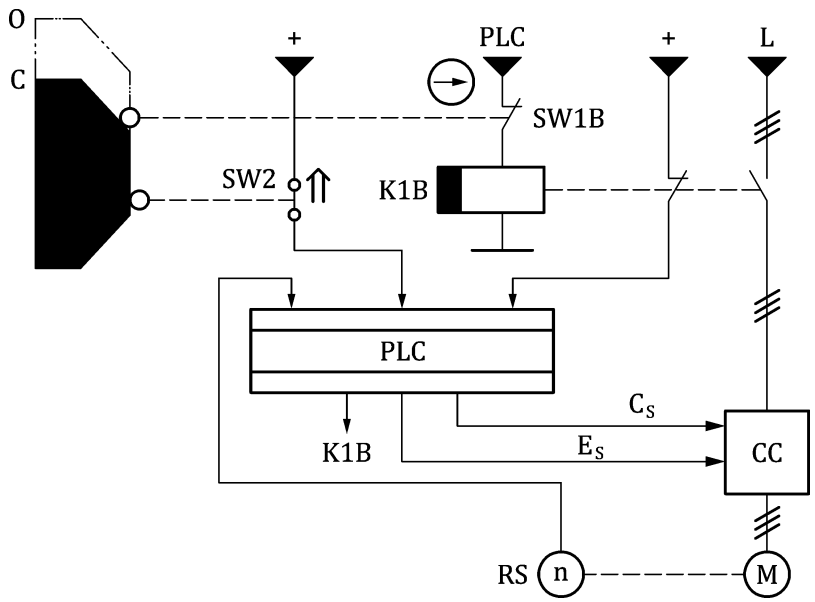
Die Anwendung von Anhang K ergibt eine durchschnittliche Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde (PFH_D) von $1{,}14 \times 10^{-6}$/h und PL c.

Das Ergebnis entspricht dem erforderlichen Performance Level 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 Identifikation 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

PLC	speicherprogrammierbare Steuerung (SPS)	C_S	Stopp-Signal (normal)
CC	Stromrichter	E_S	Freigabe (normal)
M	Motor	K1B	Hilfsschütz
RS	Drehgeber	SW1B	Positionsschalter (NC)
O	Verriegelung der trennenden Schutzeinrichtung ist offen	SW2	Positionsschalter (NO)
C	Verriegelung der trennenden Schutzeinrichtung ist geschlossen	⊖	Zwangsöffnung
L	Energieversorgung	⇑	betätigte Stellung

Bild I.3 — Steuerungskreis 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 auszuschalten. Die wesentlichen Merkmale dieser sicherheitsbezogenen Teile sind daher:

— redundante Kanäle, ein elektromechanischer und ein programmierbar elektronischer;

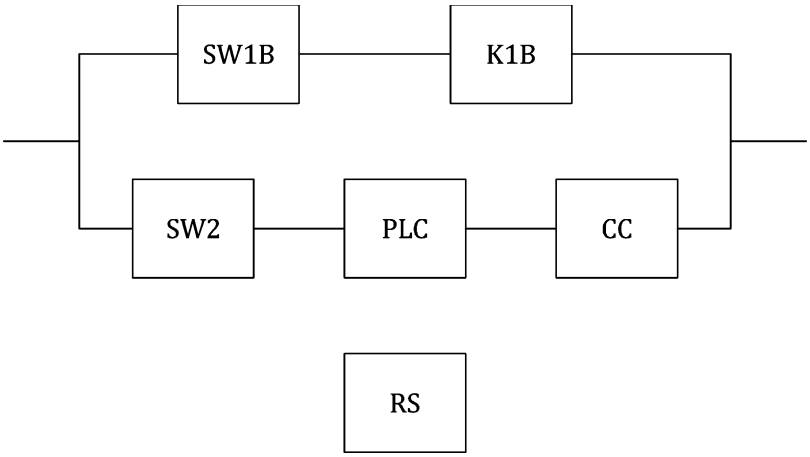
— nur der Positionsschalter SW1B (NC) verfügt über zwangsöffnende Kontakte, aber beide Positionsschalter SW1B und SW2 haben einen hohen B_{10D};

— die $MTTF_D$ des Hilfsschützes K1B ist hoch;

— die $MTTF_D$ der elektronischen Bauteile SPS und CC ist mittel;

— die sicherheitsbezogene Anwendungssoftware der SPS (SRASW), 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.

Die sicherheitsbezogenen Teile und ihre Aufteilung in Kanäle können 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	PLC	speicherprogrammierbare Steuerung (SPS)
K1B	Hilfsschütz	CC	Stromrichter
SW2	Positionsschalter	RS	Drehgeber

Bild I.4 — Blockdiagramme, die die sicherheitsbezogenen Teile 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 Ausfälle infolge gemeinsamer Ursache 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 begründet.

— $MTTF_D$

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 $MTTF_D = 55$ Jahre für den Kanal ergibt, der „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:

$$\frac{1}{MTTF_{D,C2}} = \frac{1}{MTTF_{D,SW2}} + \frac{1}{MTTF_{D,SPS}} + \frac{1}{MTTF_{D,CC}} = \frac{1}{139\ \text{Jahre}} + \frac{1}{20\ \text{Jahre}} + \frac{1}{20\ \text{Jahre}} = \frac{0{,}107\ 2}{\text{Jahr}} \qquad \text{(I.3)}$$

woraus sich $MTTF_D = 9{,}3$ Jahre für den Kanal ergibt, der „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, der „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 Steuerungskreis B werden fünf der sicherheitsbezogenen Teile durch die SPS geprüft. Diese Prüfung besteht aus SW1B, SW2 und K1B, die durch die SPS zurückgelesen werden, CC wird durch SPS über RS zurückgelesen und SPS führt Selbsttests durch. Die zugehörigen DC-Werte zu jedem dieser geprüften Teile sind:

1) $DC_{SW1B} = DC_{SW2} = 99$ %, „hoch“, aufgrund der Plausibilitätsprüfung, siehe Tabelle E.1 (zweite Zeile des Teils Eingabeeinheit);

2) $DC_{K1B} = 99$ %, „hoch“, aufgrund der zwangsgeführten Öffner-/Schließer-Kombination, siehe Tabelle E.1 (zweite Zeile des Teils Eingabeeinheit);

3) $DC_{SPS} = 30$ %, „keiner“, aufgrund der geringen Wirksamkeit der Selbsttests (dieser Wert ergibt sich aus der spezifischen Anwendung); und

4) $DC_{CC} = 90$ %, „mittel“, aufgrund indirekter Überwachung der Maschinenstellteile 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 mittlerer DC-Wert benötigt:

$$DC_{avg} = \frac{\frac{DC_{SW1B}}{MTTF_{D,SW1B}} + \frac{DC_{K1B}}{MTTF_{D,K1B}} + \frac{DC_{SW2}}{MTTF_{D,SW2}} + \frac{DC_{PLC}}{MTTF_{D,PLC}} + \frac{DC_{CC}}{MTTF_{D,CC}}}{\frac{1}{MTTF_{D,SW1B}} + \frac{1}{MTTF_{D,K1B}} + \frac{1}{MTTF_{D,SW2}} + \frac{1}{MTTF_{D,PLC}} + \frac{1}{MTTF_{D,CC}}} = \quad \text{(I.4)}$$

$$= \frac{\frac{0,99}{2\,778} + \frac{0,99}{56} + \frac{0,99}{139} + \frac{0,3}{20} + \frac{0,9}{20}}{\frac{1}{2\,778} + \frac{1}{56} + \frac{1}{139} + \frac{1}{20} + \frac{1}{20}} = \frac{0,09}{0,13} = 67,9\,\%$$

Demnach ist der sich daraus ergebende DC_{avg} „niedrig“.

— CCF

Für eine Abschätzung der Maßnahmen gegen CCF nach F.2 sind die Ergebnisse für Steuerungskreis B in Tabelle I.1 angegeben.

Tabelle I.1 — Abschätzung der Maßnahmen gegen CCF für das Beispiel B

Nr.	Betrachtungseinheit	Punktzahl für den Steuerungskreis	Maximal mögliche Punktzahl
1	**Trennung/Abtrennung**		
	Physische Trennung zwischen den Signalpfaden	15	15
2	**Diversität**		
	Unterschiedliche Technologien/Gestaltung oder physikalische Prinzipien werden verwendet	20	20
3	**Gestaltung/Anwendung/Erfahrung**		
3.1	Schutz gegen Überspannung, Überdruck, Überstrom, Übertemperatur	15	15
3.2	Verwendung bewährter Bauteile	keine (nur teilweise erfüllt, siehe F.2)	5
4	**Beurteilung/Analyse**		
	Für jedes Teil von sicherheitsbezogenen Teilen einer Steuerung wurde eine Fehlzustandsart- und -auswirkungsanalyse durchgeführt und deren Ergebnisse berücksichtigt, um Ausfälle infolge gemeinsamer Ursache im Entwurf zu vermeiden.	keiner	5
5	**Ausbildung**		
	Ausbildung der Konstrukteure, um die Gründe und Auswirkungen von Ausfällen infolge gemeinsamer Ursache zu verstehen.	keiner	5
6	**Umgebung**		
6.1	Für elektrische/elektronische Systeme, Verhindern von Verunreinigungen und elektromagnetischen Störungen (EMI) zum Schutz vor Ausfällen infolge gemeinsamer Ursache entsprechend den einschlägigen Normen (z. B. IEC 61326-3-1)	25	25

Nr.	Betrachtungseinheit	Punktzahl für den Steuerungskreis	Maximal mögliche Punktzahl
6.2	Andere Einflüsse Berücksichtigung der Anforderungen hinsichtlich Unempfindlichkeit gegenüber allen relevanten Umgebungsbedingungen wie Temperatur, Schock, Vibration, Feuchte (z. B. wie in den zutreffenden Normen festgelegt).	10	10
	Gesamt	85	Maximal 100

ANMERKUNG Externe Maßnahmen, z. B. zum Schutz gegen Überspannung und elektromagnetische Störungen, sind integriert, aber nicht in Bild I.3 dargestellt.

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 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: $MTTF_D$ für den Kanal ist „hoch“ (37 Jahre), DC_{avg} ist „niedrig“ und die Kategorie ist 3.

Durch Anwendung von Bild 12 kann dies als Performance Level d gewertet werden.

Die Anwendung von Anhang K (bei 36 Jahren) ergibt eine durchschnittliche Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde (PFH_D) von $5{,}16 \times 10^{-7}$/h und PL d.

Dieses Ergebnis entspricht dem erforderlichen Performance Level d nach I.2. Somit erfüllt der Steuerungskreis 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 Anhang J 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 leistungssteuernden Elemente unter Berücksichtigung der Sicherheitsanforderungen; und

— das Ansteuern der leistungssteuernden Elemente.

Das Funktionsdiagramm der SRESW bei dieser Anwendung entspricht Bild J.1.

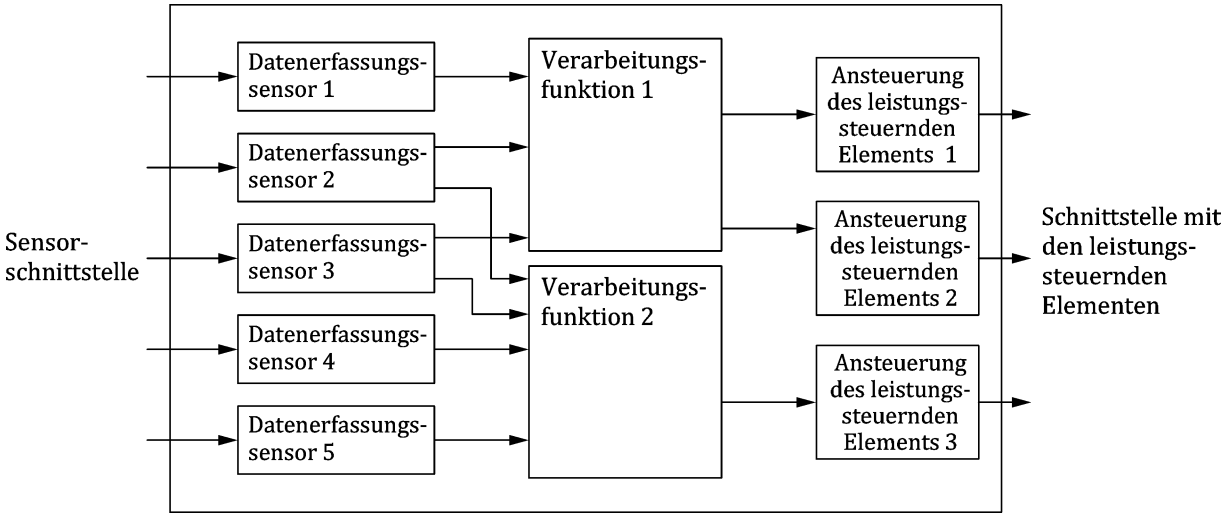


Bild J.1 — Entwurf eines Softwarebeispiels mit Funktionsbausteinsprache

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): Identifikation der mit dem SRP/CS verbundenen Funktionen	— Identifikation der Sicherheitsfunktionen	Ausgang: — Spezifikation der Sicherheits-anforderungen (SRS)

Entwicklungsaktivität	Lebenszyklusaktivität	Zugehörige Dokumentation
Architekturaspekt (Hardware und Software): Definition der Steuerungsarchitektur mit Sensoren und leistungssteuernden Elementen	— 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 J.3) — Planung des Tests der SRSS anhand der SRS	Eingang: — Spezifikation der Sicherheitsanforderungen (SRS) Ausgang: — Spezifikation des Softwareentwurfs (SDS) einschließlich Softwarebeschreibungen — Testplan für die SDS — Dokumentation der Überprüfungsaktivitäten
Aspekt der Softwarearchitektur: Softwaresystementwurf, einschließlich der einzelnen Aufführung der Funktionen nach Funktionsblöcken	— Überprüfung des Systementwurfs anhand der SDS, einschließlich der Definition von kritischen Blöcken, die eine ausführlichere Überprüfung und Validierung benötigen — Planung des Tests des Softwaresystementwurfs	Eingang: — SDS Ausgang: — Spezifikation des Softwaresystementwurfs (SSDS), einschließlich eines Funktionsblockmodells — Testplan für die SSDS — Dokumentation der Überprüfungsaktivitäten
Entwurf der Softwaremodule	— Überprüfung des Softwaremodulentwurfs anhand der SSDS — Planung des Tests der Softwaremodule	Eingang: — SSDS Ausgang: — Spezifikation des Modulentwurfs (MDS) — Testplan für die MDS — Dokumentation der Überprüfungsaktivitäten
Aspekt der Codierung: Codierung von nicht vorhandenen Softwaremodulen entsprechend den Programmierregeln (siehe 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: — Modultest	Test der Softwaremodule 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 Softwaremodule — Dokumentation der Testaktivitäten

Entwicklungsaktivität	Lebenszyklusaktivität	Zugehörige Dokumentation
Validierungsaspekt: — Test der Softwareintegration	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 Softwaremodule — 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: — 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 Parametrisierung;

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, dass ein konsistentes und verständliches allgemeines Gerüst erstellt wird, 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) Kommentierung jedes Programmabschnitts des Quellcodes, um eine Aktualisierung der Kommentierung im Fall einer Änderung zu erleichtern;

4) 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

— Die Ansteuerung oder Absteuerung jedes Ausgangs sollte nur einmalig erfolgen (zentralisierte Bedingungen).

— Das Programm sollte so strukturiert sein, dass die Gleichungen zum Aktualisieren einer Variablen zentralisiert sind.

— Jede globale Variable, Eingabe oder Ausgabe sollte einen eindeutigen mnemonischen Namen erhalten und eine Beschreibung im Kommentar des Quelltextes.

c) Programmierregeln auf der Ebene eines Funktionsblocks

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 — maximal acht digitale und zwei Integer-Eingänge, ein Ausgang;

   — im funktionalen Code — maximal 10 lokale Variablen, maximal 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

Siehe Tabelle K.1.

Tabelle K.1 — Numerische Darstellung von Bild 12

$MTTF_D$ für jeden Kanal	Durchschnittliche Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde, PFH_D (1/h) und der zugehöriger 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		
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		

$MTTF_D$ für jeden Kanal	**Durchschnittliche Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde, PFH_D (1/h) und der zugehöriger 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	
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
180													$1{,}33 \times 10^{-8}$	e

$MTTF_D$ für jeden Kanal	**Durchschnittliche Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde, PFH_D (1/h) und der zugehöriger 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
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	**Durchschnittliche Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde, PFH_D (1/h) und der zugehöriger 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
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 6.1.8), dann können die PFH_D–Werte in Tabelle K.1 für Kategorie 2 multipliziert mit einem Faktor 1,1 für die Abschätzung des ungünstigsten Falles benutzt werden.

ANMERKUNG 2 Die Berechnung der PFH_D–Werte basiert 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

Die folgenden Strategien enthalten Leitlinien zur Umsetzung der Maßnahmen für die elektromagnetische Störfestigkeit eines SRP/CS oder von Teilsystemen. Es sollte mindestens eine der Strategien ausgewählt und angewendet werden:

— Strategie A: Einhaltung der EMV-Anforderungen der einschlägigen Produktnorm (siehe IEC 61000-6-7:2014, 4.1, erster Satz). Beispiele für Produktnormen sind IEC 61326-3-1 oder IEC 61800-5-2);

— Strategie B: für PL_r a und b, Einhaltung der EMV-Anforderungen nach IEC 61000-6-2;

— Strategie C: für PL_r c, d und e, Umsetzung von EMV-Maßnahmen, um eine Punktzahl von mindestens 280 (von möglichen 400) zu erreichen nach der Tabelle L.1 „EMV“ (siehe IEC 61000-6-7, 4.1, ANMERKUNG 1); für PL_r e kann diese Strategie nur angewendet werden, wenn zusätzlich die Anforderungen von Kategorie 4 erfüllt sind;

— Strategie D: Einhaltung von IEC 61000-6-7 oder anderen EMV-Fachgrundnormen für die funktionale Sicherheit.

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 EMV sollten umgesetzt werden. Falls Strategie 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 Strategien/Maßnahmen sollten eindeutig dokumentiert und mit einem entsprechenden Nachweis der Übereinstimmung mit der gewählten Strategie 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 EMV für sicherheitsbezogene Bauteile und sonstige elektrische/elektronische Teile

Maßnahmen zum Erreichen der EMV	Punktzahl[a]
Sicherheitsbezogene Sensoren und deren Kabelbaum	
Anwendung der in IEC 60204-1, Anhang H und/oder IEC 61800-3 beschriebenen Maßnahmen	10
Analoge Spannungssignale, Winkelcodierer Abgeschirmte und geerdete und/oder verdrillte Leitungen für Sensoren und sicherheitsbezogene Eingangs-/Ausgangs-Signale (Leitungsabschirmungen werden mit geringer Impedanz in der Nähe der Bauteile geerdet)	20
Kabelbaum und Verdrahtung für Niederspannungs-Gleichstrom zu den Bauteilen mit verdrilltem Leitungspaar	10

Maßnahmen zum Erreichen der EMV	Punktzahl[a]
Sicherheitsbezogenes I/O-System (zentral oder dezentral oder in die SPS integriert)	
Eingebaut in einen abgeschirmten und ummantelten Schrank oder Bauteile in einem abgeschirmten und ummantelten Gehäuse	20
Steuerung und/oder spezifische Bauteile sind in Zonen[b] einzuteilen, z. B.: a) Netzstromversorgung und Stromverteilung; b) starke Störer wie z. B. Netzsperre, Netzdrosseln, Heizungskomponenten, Hochleistungs-versorgungen und Motorleitungen; c) empfindliche Bauteile wie z. B. Niederspannungsversorgung, SPS, Datenbusse, Sensoren und Niederspannungsstellteile.	20
SPS als Teil des SRP/CS	
Eingebaut in einen abgeschirmten und ummantelten Schrank oder Bauteile in einem abgeschirmten und ummantelten Gehäuse	10
Kategorie 3/4 für PL_r d/e mit verschiedenen SPS im selben Gehäuse, getrennt durch einen ausreichenden Abstand zueinander	10
Kategorie 3/4 für PL_r d/e mit redundanter SPS in unterschiedlichen Gehäusen	20
Kategorie 3/4 für PL_r d/e mit diversen Kanälen (z. B. SPS und diskrete Logik) oder mit Sicherheits-SPS	20
Sicherheitsbezogene Stellteile und deren Kabelbaum	
Anwendung der in IEC 60204-1, Anhang H, beschriebenen Maßnahmen und/oder Anwendung von IEC 61800-3	10
Sonstige Bauteile und Verdrahtungen mit maßgebendem Störpegel	
Umhüllte Leiter für Motoren oder Sinuswellenfilter zwischen Motor und Wandler oder vergleichbare Maßnahmen	20
RF-Filter, Überspannungs- und Transientenschutz (z. B. Filter, Übergangsspannungsunterdrücker-diode, Optokoppler, Ferrite) für sicherheitsbezogene Signale	20
EMV-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, Anhang H, beschriebenen Maßnahmen und/oder Anwendung von IEC 61800-3	10
Konstruktion, Programmierung, Ausbildung, Beobachtungen während des Einsatzes	
Bauteile entsprechen mindestens IEC 61000-6-2 (in der Dokumentation des Herstellers angegeben)	10
Risikoanalyse hinsichtlich EMV (siehe Beispiel in Tabelle L.2) und Risikobeurteilung mit einem Abschlussbericht	20
Diverse redundante Kanäle (siehe ANMERKUNG)	20
Trennung von elektromagnetischen Störquellen und empfindlichen Bauteilen, z. B.: — getrennte Verlegung und Anordnung von Stromleitungen und Signalleitungen; — getrennte Metallschränke 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 Plausibilitäts-prüfungen, Daten-Kreuzvergleich im Fall von Redundanz, Selbsttests	20

Maßnahmen zum Erreichen der EMV	Punktzahl[a]
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 EMV-Probleme erwiesen hat	30
Stromversorgung des SRP/CS	
Stromversorgungen mit Niederspannungs-Wechselstrom oder -Gleichstrom mit isolierten Transformatoren nach IEC 61558, und/oder SELV-Versorgungen nach IEC 60950, und/oder SELV- oder PELV-Versorgungen nach IEC 50178	20
Redundante SPS mit separatem Schaltnetzteil für das SRP/CS mit Kanal 1/2	10

Gesamtpunktzahl 400	**Maßnahmen für die elektromagnetische Störfestigkeit[a]**
280 oder besser	Anforderungen erfüllt
Weniger als 280	Verfahren gescheitert ⇒ Auswahl zusätzlicher Maßnahmen oder Auswahl einer oder mehrerer der oben genannten Strategien

ANMERKUNG Redundante Kanäle bedeuten in Tabelle L.1 Funktionskanäle und Testkanäle der Kategorie 2 oder redundante Funktionskanäle der Kategorien 3 und 4.

[a] Wenn technische Maßnahmen nicht relevant sind, können die Punktzahlen der rechten Spalte bei der ausführlichen Berechnung berücksichtigt werden.

[b] Die Zonen können sich innerhalb eines Schranks befinden oder auf mehrere Schränke aufgeteilt sein.

Tabelle L.2 — Beispiel für eine Risikoanalyse einer elektromagnetischen Störung

Störungsquelle	Phänomen der elektromagnetischen Störung	Abstand Quelle/Senke	Empfindliches Bauteil	Folge des Risikos	Problemlösung
Energieversorgung	induktive Kopplung kapazitive Kopplung	< 20 cm	Signalleitungen Sensorleitungen	falsche Messwerte Fehlfunktion	größerer Abstand Abschirmung Filtern geschirmtes Kabel
Wechselrichter	kapazitive Kopplung	< 40 cm	alle Leitungen alle Sensoren speicherprogrammierbare Logik Analog-Digital-Wandler	sporadischer Ausfall Fehlfunktion Funktionsverlust	größerer Abstand Filtern Sinusfilter geschirmtes Kabel Ferritklemmen
Stromnetz	leitungsgeführte Kopplung kapazitive Kopplung Hochleistungstransienten	—	Sensor Speicherprogrammierbare Logik Motorantrieb	Störung Fehlfunktion Schaden undefinierter Zustand	Netzfilter Spannungsstoßfilter verdrillte Leitung Filtern Transientenschutz

Störungs-quelle	**Phänomen der elektro-magnetischen Störung**	**Abstand Quelle/Senke**	**Empfindliches Bauteil**	**Folge des Risikos**	**Problemlösung**
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

Tabelle M.1 und Tabelle M.2 führen einige 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 12100:2010	
Sicherheitsbezogene Stopp-Funktion	5.2.3.1	3.26, 6.2.11.3	IEC 60204-1:2016, 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	5.2.3.2	—	IEC 62046:2018 ISO 13850:2015
Start-/Wiederanlauffunktion	5.2.3.3	5.2.11.3, 5.2.11.4	IEC 60204-1:2016, 9.2.3.2, 9.2.3.3, 9.2.3.10 IEC 62046:2018
Lokale Steuerungsfunktion	5.2.3.4	5.2.11.8, 5.2.11.10	IEC 60204-1:2016, 10.1.5
Überbrückungsfunktion	5.2.3.5	—	IEC 62046:2018, 5.7
Einrichtung mit selbsttätiger Rückstellung		5.2.11.8 b)	IEC 60204-1:2016, 9.2.3.7
Zustimmfunktion		—	IEC 60204-1:2016, 9.2.3.9, 10.9
Verhindern des unerwarteten Anlaufs	—	5.2.11.4	ISO 14118:2017 IEC 60204-1:2016, 5.4 IEC 61800-5-2:2016
Befreiung und Rettung eingeschlossener Personen	—	5.3.5.3	ISO 14119:2013, 5.7.5.2
Isolations- und Energie-ableitungsfunktion	—	5.3.5.4	ISO 14118:2017 IEC 60204-1:2016, 5.3, 6.3.1
Betriebsartenwahl	5.2.3.8	5.2.11.8, 5.2.11.10	IEC 60204-1:2016, 9.2.3.5

Sicherheitsfunktion/ Eigenschaft	Anforderung(en)		Für ergänzende Informationen siehe
	Dieses Dokument	ISO 12100:2010	
Beeinflussung zwischen verschiedenen sicherheitsbezogenen Teilen der Steuerungen	—	5.2.11.1 (letzter Satz)	IEC 60204-1:2016 ISO 11161:2007 ISO 13850:2015
Überwachung der Parametrisierung der sicherheitsbezogenen Eingangswerte	7.5	—	—
Funktion zum Stillsetzen im Notfall[a]	—	5.3.5.2	ISO 13850:2015 IEC 60204-1:2016, 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] 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 12100:2010	
Ansprechzeit	5.2 13.2	—	ISO 13855:2010, 3.2, A.3, A.4 IEC 62046:2018, 4.4.2.2
Sicherheitsbezogener Parameter, z. B. Geschwindigkeit, Temperatur, Druck, Position oder Moment	5.2.3.6	5.2.11.7.3	IEC 60204-1:2016, 7.1, 9.3.2 IEC 61800-5-2:201610218-
Schwankungen, Verlust und Wiederkehr der Spannungsversorgung	5.2.3.7	5.2.11.4 5.2.11.5	IEC 60204-1:2016, 4.3, 7.1, 7.5 ISO 4413:2010 ISO 4414:2010
Anzeigen und Alarme	—	5.2.3.6 und 5.2.3.7	ISO 7731:2008 ISO 11428:1996 ISO 11429:1996 IEC 61310-1:2007 IEC 60204-1:2016, 10.3, 10.4 IEC 61131-3:2013 IEC 62061:2015

Anhang N
(informativ)

Vermeiden eines systematischen Ausfalls durch den Softwareentwurf

N.1 Auswahl von Maßnahmen zur Fehlervermeidung für den Softwareentwurf

Die folgenden Tabellen enthalten Leitlinien für die Auswahl von Maßnahmen zur Fehlervermeidung für sicherheitsbezogene Embedded-Software (SRESW) oder sicherheitsbezogene Anwendungssoftware (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	Teil	Fall
a und b	B	Funktionskanal	Fall 1
a, b und c	2	Testkanal	
a und b	2	Funktionskanal	
a und b	3	vorher beurteilte 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	vorher beurteilte 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	vorher beurteilte Plattform	
d	3 und 4	Kanal 1 UND 2	
e	3 und 4	Kanal 1 ODER 2	
e	3 und 4	vorher beurteilte 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 Werkzeugauswahl.

BEISPIEL Für ein Teilsystem mit PL_r c und Kategorie 2 wird Fall 2 für den Funktionskanal und Fall 1 für den Testkanal ausgewählt.

In Tabelle N.3 und Tabelle N.4 werden die folgenden Abkürzungen verwendet:

— r = empfohlen (en: recommended), bedeutet, dass die Anwendung dieser Maßnahme die Qualität der Softare verbessert, deren Anwendung aber nicht obligatorisch ist;

— m = obligatorisch (en: mandatory), bedeutet, dass diese Maßnahme immer angewendet werden sollte;

— „—“ bedeutet, dass diese Maßnahme nicht erforderlich ist.

— Kanal 1 UND 2 bedeutet, dass SRESW oder SRASW in beiden Funktionskanälen der Kategorie 3 oder 4 verwendet wird;

— Kanal 1 ODER 2 bedeutet, dass SRESW oder SRASW nur in einem der Funktionskanäle der Kategorie 3 oder 4 verwendet wird;

— vorher beurteilte Plattform bedeutet, dass die Hardware und die interne Software (SRESW) für die Sicherheitsanwendungen entworfen und bereits beurteilt wurden, sodass sie diesem Dokument oder IEC 61508/IEC 62061 für den erforderlichen Performance Level entsprechen.

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 Testeinrichtungsblock 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; in diesem Fall werden die Anforderungen um einen Performance Level reduziert.

d) SRASW in PL d und PL e darf außerdem mithilfe einer vorher beurteilten Plattform verwendet werden (sicherheitsbezogene Hardware in Kombination mit dem Betriebssystem und Programmierungswerkzeug). In diesem Fall wird nur eine Anwendungssoftware für beide Funktionskanäle verwendet.

Tabelle N.2 — Auswahl von Maßnahmen für SRASW in LVL

	Beschreibung: r = empfohlen, m = obligatorisch (mit niedriger, mittlerer oder hoher Wirksamkeit), „—“ = nicht erforderlich				
	Fall	**Fall 1**	**Fall 2**	**Fall 3**	**Fall 4**
1	Diese grundlegenden Maßnahmen sollten angewendet werden:				
a)	Entwicklungslebenszyklus mit Verifizierungs- und Validierungstätigkeiten, siehe Bild 14a und Bild 14b	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				

	Beschreibung: r = empfohlen, m = obligatorisch (mit niedriger, mittlerer oder hoher Wirksamkeit), „—“ = nicht erforderlich				
	Fall	**Fall 1**	**Fall 2**	**Fall 3**	**Fall 4**
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 Werkzeuge, Bibliotheken, Sprachen:				
a)	Werkzeuge sollten für die jeweilige Anwendung geeignet sein.	—	m	m	m
b)	Bei einem PL e, der mit einem Bauteil und dessen Werkzeug erreicht wird, sollte das Werkzeug der entsprechenden Sicherheitsnorm entsprechen. * Falls zwei verschiedene Bauteile mit unterschiedlichen Werkzeugen verwendet werden, darf der Vertrauenswert aus deren Anwendung als ausreichend angenommen werden (für PL e).	—	—	—	m[a]
c)	Technische Fähigkeiten, die Bedingungen erkennen können, die zu systematischen Fehlern führen könnten (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. Werkzeuge sollten Sprachenteilmengen und Programmierrichtlinien erzwingen oder mindestens den Entwickler leiten oder führen.				
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 diesem Teil von ISO 13849.	—	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	Der Softwareentwurf sollte folgende Merkmale aufweisen:				
a)	Semiformale Verfahren zum Beschreiben des Daten- und Steuerungssignalflusses, z. B. Zustandsdiagramm oder Programmablaufdiagramm	—	m	m	m
b)	Modulare und strukturierte Programmierung, überwiegend realisiert durch die Bereitstellung validierter sicherheitsbezogener Funktionsbausteinbibliotheken 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				

	Beschreibung: r = empfohlen, m = obligatorisch (mit niedriger, mittlerer oder hoher Wirksamkeit), „—“ = nicht erforderlich				
	Fall	**Fall 1**	**Fall 2**	**Fall 3**	**Fall 4**
e)	Architektur des Modells in drei Stufen: Eingänge ⇒ Verarbeitung ⇒ Ausgänge (siehe Bild 10 und Anhang J)				
f)	Zuordnung des Sicherheitsausgangs zu nur einem Programmteil 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;				
b)	Es sollte keine logische Verknüpfung von nicht sicherheitsbezogenen und sicherheitsbezogenen Daten geben, die zur Herabstufung der Integrität der sicherheitsbezogenen Signale führen könnte, z. B. Verknüpfen eines sicherheitsbezogenen und eines nicht sicherheitsbezogenen Signals durch ein logisches „ODER“, dessen Ausgang sicherheitsbezogene Signale steuert.	—	m	m	m
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 Funktionsverhaltens 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.				
c)	Eine Testplanung wird empfohlen und sollte Testfälle mit Abschlussbedingungen und erforderlichen Werkzeugen enthalten	—	r	r	r
d)	Für PL d oder e wird eine Testfallausführung auf der Basis von Grenzwertanalysen empfohlen;	—	—	r	r

	Beschreibung: r = empfohlen, m = obligatorisch (mit niedriger, mittlerer oder hoher Wirksamkeit), „—“ = nicht erforderlich				
	Fall	**Fall 1**	**Fall 2**	**Fall 3**	**Fall 4**
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, Walk-through 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 Werkzeugkonfiguration, die im Bezug zu einer bestimmten SRASW stehen, zu identifizieren und zu archivieren	—	m	m	m
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

Tabelle N.3 — Auswahl von Maßnahmen für SRESW und/oder SRASW in FVL

	Beschreibung: r = empfohlen, m = obligatorisch, „—“ = nicht erforderlich				
	Fall	**Fall 1**	**Fall 2**	**Fall 3**	**Fall 4**
1	Diese grundlegenden Maßnahmen sollten angewendet werden:				
a)	Software-Sicherheitslebenszyklus mit Verifizierung und Validierung, siehe Bild 14 a;	m	m	m	m[a]
b)	Dokumentation der Spezifikation und des Entwurfs, z. B. Spezifikation des Softwareentwurfs, Spezifikation des Softwaresystementwurfs, Spezifikation des Modulentwurfs, Codelisten einschließlich Bemerkungen;				
c)	Modularer und strukturierter Entwurf und Codierung, z. B. Hierarchie und Einschränkung der Funktionalität, klare Programmstruktur, Definition von Schnittstellen, gut strukturierter Aufrufgraph, Vermeidung von Unterbrechungen, Verwendung von Codierungsrichtlinien;				
d)	Steuerung systematischer Ausfälle, z. B. Programmablaufüberwachung, Steuerung von Fehlern im Datenkommunikationsprozess (siehe G.2);				
e)	Wenn softwarebasierte Maßnahmen zur Steuerung zufälliger Hardwareausfälle verwendet werden, wird die korrekte Ausführung überprüft, z. B. korrekte Ausführung von Diagnosemaßnahmen, RAM/ROM/CPU-Tests, Hardwaretests, Plausibilitätsprüfungen;				
f)	Funktionstests, z. B. Black-Box-Tests, z. B. 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 IEC 61508, z. B. Definition des Arbeitsablaufs, der Verantwortlichkeiten, Konfigurationsmanagement, Werkzeugeinsatz;	—	m (siehe ANMERKUNG 2)	m (siehe ANMERKUNG 2)	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 Konfigurationspunkte 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 Entwurfs;				
e)	Anwendung geeigneter Programmiersprachen und rechnergestützter Werkzeuge mit Vertrauen in deren Verwendung, z. B. werden Programmierer dahingehend geschult, diese Werkzeuge zu verwenden;				
f)	Modulare und strukturierte Programmierung, Abgrenzung von der nicht sicherheitsbezogenen Software, beschränkte Modulgrößen mit vollständig definierten Schnittstellen, Verwendung von Entwurfs- und Codierungsrichtlinien;				

	Beschreibung: r = empfohlen, m = obligatorisch, „—“ = nicht erforderlich				
	Fall	**Fall 1**	**Fall 2**	**Fall 3**	**Fall 4**
g)	Verifizierung der Codierung durch Walk-through/Überprüfen mit Steuerungssignalflussanalyse (zur Überprüfung auf Fehler, Qualität der Bemerkungen, 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-Sicherheits-lebenszyklus-Aktivitäten nach Änderungen.				
j)	Die SRESW für Bauteile 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, Entwurf 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 PL_r c oder d ein PL_r e erreicht werden.

ANMERKUNG 2 Für SRESW mit Diversität in Entwurf und Codierung kann für die Bauteile des SRP/CS in Kategorie 3 oder 4 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.

N.2 Beispiel für eine Software-Validierung

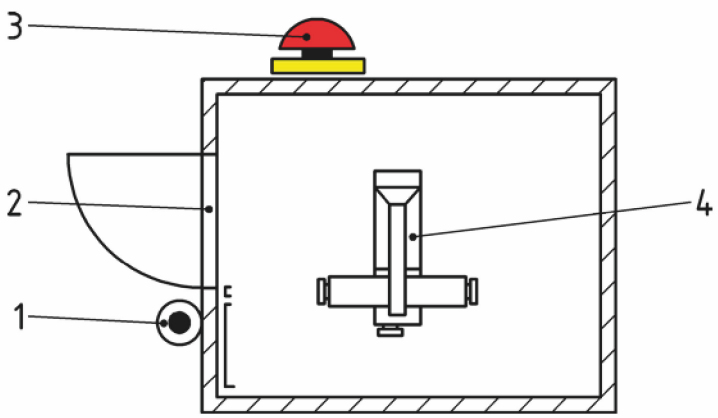
N.2.1 Beispiel für eine Software-Validierung

In diesem Beispiel für eine Validierung werden zuvor beurteilte Softwaremodule verwendet. Die Validierung erfolgt durch Testfälle an den Eingängen der zuvor beurteilten Softwaremodule, um deren Anwendung im Kontext der gesamten Anwendungssoftware zu überprüfen. Die Anzahl der Testfälle erhebt keinen Anspruch auf Vollständigkeit.

N.2.2 Codierungsrichtlinien

Die Codierung sollte nach den Codierungsrichtlinien des Herstellers der Softwareplattform erfolgen, sofern maßgebend, oder nach einer „hausinternen Richtlinie“, die allerdings nicht im Widerspruch zu den Codierungsrichtlinien der vom Benutzer angewendeten Softwareplattform steht.

N.2.3 Spezifikation der Sicherheitsfunktionen



Legende
1 ACK1 — Quittierungstaster für Tür 1 der verriegelten trennenden Schutzeinrichtung (zugänglich)
2 GD1 — Tür 1 der verriegelten trennenden Schutzeinrichtung
3 ES1 — Not-Halt 1
4 M1 — Motor 1, angehalten mit STO (sicher abgeschaltetes Drehmoment) in PL d (über Sicherheitsbus PL e)

Bild N.1 — Sicherheitsfunktionen

Die Sicherheitsfunktion und Ergänzungen arbeiten wie folgt:

— wenn Tür 1 der verriegelten trennenden Schutzeinrichtung (GD1) geöffnet wird (zugänglicher Bereich), dann wird M1 abgeschaltet (STO wird mit PL d ausgeführt). GD1 wird mit dem Taster ACK1 quittiert. Eine Quittierung ist nur möglich, wenn GD1 geschlossen ist.

— ein Not-Halt (ES1) löst ein STO von Motor M1 aus (PL_r = PL d).

Wenn alle sicherheitsbezogenen Anforderungen des Herstellers der Sicherheits-SPS erfüllt sind, reicht das vereinfachte V-Modell aus, siehe Tabelle N.4.

Tabelle N.4 — Allgemeines Architekturmodell für Software

<table>
<tr><th>Sensor</th><th colspan="3">Sicherheits-SPS</th><th>Stellteil</th></tr>
<tr><td rowspan="2">GD1
(redundante Abschaltung der verriegelten trennenden Schutzeinrichtung)
(RÜCKSTELLEN der verriegelten trennenden Schutzeinrichtung)
ES1
(Not-Halt)</td><td colspan="3">Eingang (Block) — Logik (Block) — Ausgang (Block)</td><td>M1
(Antrieb mit STO mit PL d)</td></tr>
<tr><td>Erfassen der Informationen für die verschiedenen Sicherheitssensoren durch die Eingänge</td><td>Verarbeiten der sicherheitsbezogenen Signale</td><td>Betätigen der Antriebselemente durch den Sicherheitsausgang</td><td></td></tr>
</table>

N.2.4 In SRAW umzusetzende Verifizierungsverfahren für DC-Maßnahmen

N.2.4.1 Allgemeines

Für den Nachweis des DC-Werts wird empfohlen, die Software in Blöcke aufzuteilen:

1) Bewertung der verriegelten trennenden Schutzeinrichtung;

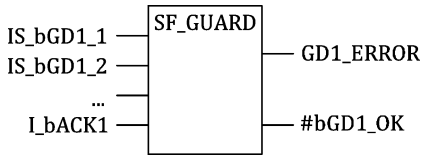
2) Bewertung des Not-Halts;

3) Bewertung der Freigabe/der Abschaltung von Motor M1.

N.2.4.2 Bewertung der verriegelten trennenden Schutzeinrichtung

Tabelle N.5 — FMEA der verriegelten trennenden Schutzeinrichtung

Maßgebende Eingänge				
Beschreibung	I/O	Typ	Information	Beschreibung
GD1 Ch1: IS_bGD1_1	E 1.1	boolesch	Zeitdifferenz zu Kanal 2 500 ms	Verriegelte trennende Schutzeinrichtung NC (zwangsläufiges Öffnen)
GD1 Ch2: IS_bGD1_2	E 1.2	boolesch	Zeitdifferenz zu Kanal 1 500 ms	Verriegelte trennende Schutzeinrichtung NC (zwangsläufiges Öffnen)
ACK1: I_bACK1	E 1.3	boolesch	NO	Quittieren der verriegelten trennenden Schutzeinrichtung GD1
Maßgebende Kennzeichen				
Beschreibung	O	Typ	Information	Beschreibung
#bGD1_OK	O 1.1	boolesch	NO	Dieses Freigabekennzeichen wird für die nachfolgende Verarbeitung verwendet.
GD1_ERROR	O 1.2	boolesch	NO	Dieses Fehlerkennzeichen wird für die nachfolgende Verarbeitung verwendet.

Verwendete Software-Blöcke			
Name	Zuvor beurteilter Block der Software-Plattform	Beschreibung	Information
SF_Guard	ja	Zuvor beurteilter Software-Block für die Überwachung der verriegelten trennenden Schutzeinrichtung mit PL d: Wird ein Fehler erkannt, ändert sich das GD1_ERROR-Kennzeichen in hoch.	

Nachweis von ausgeführten DC-Maßnahmen durch Testfälle (Fehlerursache- und -auswirkungsanalyse)			
Nr.	Fehlereinspeisung	Sicherer Zustand und Reaktion auf einen Fehler	Erwartetes Ergebnis

0	Keine Fehlereinspeisung und keine erwartete Reaktion auf einen Fehler:
	Wenn die Sicherheitsfunktion angefordert wird (durch Öffnen der Tür der verriegelten trennenden Schutzeinrichtung), dann ist
	IS_bGD1_1 = NIEDRIG und
	IS_bGD1_2 = NIEDRIG
		#bGD1_OK = NIEDRIG und
		GD1_ERROR = NIEDRIG
			ja/nein

ANMERKUNG 1 Fehlerfreier Zustand (Ausgangssituation/Normalzustand vor Durchführung der Prüfungen, die Tür der verriegelten trennenden Schutzeinrichtung ist geschlossen).			

1	Dauerhaftes Signal HOCH auf IS_bGD1_1 (E 1.1)
	Wenn die Sicherheitsfunktion angefordert wird (durch Öffnen der Tür der verriegelten trennenden Schutzeinrichtung), dann bewirkt IS_bGD1_2 eine Änderung des Signals
		Sicherer Zustand mit #bGD1_OK = NIEDRIG und eingeleitete Reaktion auf einen Fehler
		GD1_ERROR = NIEDRIG wird geändert in
		GD1_ERROR = HOCH
			ja/nein

ANMERKUNG 2 Übermittlungsfehler E 1.1, der Block kann nicht quittiert werden. Wird die Tür wieder geschlossen, kann der Block wieder quittiert werden.			

2	Dauerhaftes Signal HOCH auf IS_bGD1_2 (E 1.2).
	Wenn die Sicherheitsfunktion angefordert wird (durch Öffnen der verriegelten trennenden Schutzeinrichtung der Tür), dann bewirkt IS_bGD1_1 eine Änderung des Signals
		Sicherer Zustand mit #bGD1_OK = NIEDRIG und eingeleitete Reaktion auf einen Fehler
		GD1_ERROR = NIEDRIG wird geändert in
		GD1_ERROR = HOCH
			ja/nein

ANMERKUNG 3 Übermittlungsfehler E 1.2, der Block kann nicht quittiert werden. Wird die Tür wieder geschlossen, kann der Block wieder quittiert werden.			

3	Signal NIEDRIG auf IS_bGD1_1 (E 1.1)	Sicherer Zustand mit #bGD1_OK = NIEDRIG und eingeleitete Reaktion auf einen Fehler
		GD1_ERROR = NIEDRIG wird geändert in
		GD1_ERROR = HOCH
			ja/nein

ANMERKUNG 4 Übermittlungsfehler E 1.1, das Modul kann aufgrund des Ruhestromprinzips nicht quittiert werden, auch dann nicht, wenn die Tür der verriegelten trennenden Schutzeinrichtung wieder geschlossen wird.			

4	Signal NIEDRIG auf IS_bGD1_2 (E 1.2)	Sicherer Zustand mit #bGD1_OK = NIEDRIG und eingeleitete Reaktion auf einen Fehler
		GD1_ERROR = NIEDRIG wird geändert in
		GD1_ERROR = HOCH
			ja/nein

ANMERKUNG 5 Übermittlungsfehler E 1.2, das Modul kann aufgrund des Ruhestromprinzips nicht quittiert werden, auch dann nicht, wenn die Tür der verriegelten trennenden Schutzeinrichtung wieder geschlossen wird.			

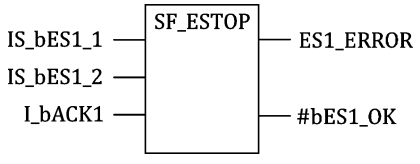
5	IS_bGD1_1 ändert den Signalstatus außerhalb der eingestellten Zeitdifferenz in IS_bGD1_2	Sicherer Zustand mit #bGD1_OK = NIEDRIG und eingeleitete Reaktion auf einen Fehler
		GD1_ERROR = NIEDRIG wird geändert in
		GD1_ERROR = HOCH
			ja/nein

ANMERKUNG 6 Diese Diagnosefunktion gilt für den Schutz vor Manipulation. Der Abweichungsfehler mit dem GD1-Modul kann nicht quittiert werden. Wird die Tür wieder geschlossen, kann das Modul quittiert werden.			

6	IS_bGD1_2 ändert den Signalstatus außerhalb der eingestellten Zeitdifferenz in IS_bGD1_1	Sicherer Zustand mit #bGD1_OK = NIEDRIG und eingeleitete Reaktion auf einen Fehler GD1_ERROR = NIEDRIG wird geändert in GD1_ERROR = HOCH	ja/nein
ANMERKUNG 7 Diese Diagnosefunktion gilt für den Schutz vor Manipulation. Der Abweichungsfehler mit dem GD1-Modul kann nicht quittiert werden. Wird die Tür wieder geschlossen, kann das Modul quittiert werden.			
7	ACK1 (E 1.3) dauerhaftes Signal hoch und GD1_ERROR = wahr	Selbst wenn der Fehler behoben wird, kann der Block nicht zurückgesetzt werden	ja/nein
ANMERKUNG 8 Eine Quittierung ist flankengesteuert und nicht pegelgesteuert. Diese Diagnosefunktion ist eine Vorbeugungsmaßnahme zum Schutz vor Manipulation.			
8	ACK1 (E 1.3) dauerhaftes Signal niedrig und GD1_ERROR = wahr	Selbst wenn der Fehler behoben wird, kann der Block nicht zurückgesetzt werden	ja/nein
ANMERKUNG 9 Eine Quittierung ist flankengesteuert und nicht pegelgesteuert. Diese Diagnosefunktion ist eine Vorbeugungsmaßnahme zum Schutz vor Manipulation.			

N.2.4.3 Bewertung des Not-Halts

Tabelle N.6 — FMEA des Not-Halts

Maßgebende Eingänge				
Beschreibung	I/O	Typ	Information	Beschreibung
ES1 Ch1: IS_bES1_1	E 1.4	boolesch	Zeitdifferenz zu Kanal 2: 500 ms	Not-Halt NC (zwangsläufiges Öffnen)
ES1 Ch2: IS_bES1_2	E 1.5	boolesch	Zeitdifferenz zu Kanal 1: 500 ms	Not-Halt NC (zwangsläufiges Öffnen)
ACK1: I_bACK1	E 1.3	boolesch	NO	Quittierung Not-Halt ES1
Maßgebende Ausgänge/Kennzeichen				
Beschreibung	O	Typ	Information	Beschreibung
#bES1_OK	O 1.3	boolesch	NO	Dieses Freigabekennzeichen wird für die nachfolgende Verarbeitung verwendet.
ES1_ERROR	O 1.4	boolesch	NO	Dieses Fehlerkennzeichen 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 Im Fall eines Fehlers wird ES1_ERROR auf hoch eingestellt		

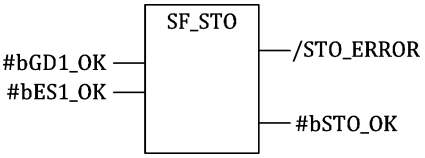
Nachweis von ausgeführten DC-Maßnahmen durch Testfälle (Fehlerursache- und -auswirkungsanalyse)			
Nr.	Fehlereinspeisung	Sicherer Zustand und Reaktion auf einen Fehler	Erwartetes Ergebnis
0	Keine Fehlereinspeisung und keine erwartete Reaktion auf einen Fehler: Wenn die Sicherheitsfunktion angefordert wird (Betätigen des Not-Halts), dann ist IS_bES1_1 = NIEDRIG und IS_bES1_2 = NIEDRIG.	#bES1_OK = NIEDRIG und ES1_ERROR = NIEDRIG	ja/nein
ANMERKUNG 1 Fehlerfreier Zustand (Ausgangssituation/Normalzustand vor Durchführung der Prüfungen, Not-Halt wird nicht angefordert).			
1	Dauerhaftes Signal HOCH auf IS_bES1_1 (E 1.4) Bei Anforderung der Sicherheitsfunktion (Betätigen des Not-Halts) und Änderung des Signals IS_bES1_2 ANMERKUNG 2 Übermittlungsfehler E 1.4, der Block kann nicht quittiert werden. Wird der Not-Halt wieder entriegelt, kann der Block wieder quittiert werden.	Sicherer Zustand mit #bES1_OK = NIEDRIG und eingeleitete Reaktion auf einen Fehler ES1_ERROR = NIEDRIG wird geändert in HOCH	ja/nein
ANMERKUNG 3 Übermittlungsfehler E 1.4, der Block kann nicht quittiert werden. Wird der Not-Halt wieder entriegelt, kann der Block wieder quittiert werden.			
2	Dauerhaftes Signal HOCH auf IS_bES1_2 (E 1.5). Bei Anforderung der Sicherheitsfunktion (Betätigen des Not-Halts) und Änderung des Signals IS_bES1_1	Sicherer Zustand mit #bES1_OK = NIEDRIG und eingeleitete Reaktion auf einen Fehler ES1_ERROR = NIEDRIG wird geändert in HOCH	ja/nein
ANMERKUNG 4 Übermittlungsfehler E 1.5, der Block kann nicht quittiert werden. Wird der Not-Halt wieder entriegelt, kann der Block wieder quittiert werden.			
3	Signal NIEDRIG auf IS_bES1_1 (E 1.4)	Sicherer Zustand mit #bES1_OK = NIEDRIG und eingeleitete Reaktion auf einen Fehler ES1_ERROR = NIEDRIG wird geändert in HOCH	ja/nein
ANMERKUNG 5 Übermittlungsfehler E 1.4, das Modul kann aufgrund des Ruhestromprinzips nicht quittiert werden, auch dann nicht, wenn der Not-Halt wieder entriegelt wird.			
4	Signal NIEDRIG auf IS_bES1_2 (E 1.5)	Sicherer Zustand mit #bES1_OK = NIEDRIG und eingeleitete Reaktion auf einen Fehler ES1_ERROR = NIEDRIG wird geändert in HOCH	ja/nein
ANMERKUNG 6 Übermittlungsfehler E 1.5, das Modul kann aufgrund des Ruhestromprinzips nicht quittiert werden, auch dann nicht, wenn der Not-Halt wieder entriegelt wird.			
5	IS_bES1_1 (E 1.4) ändert den Signalstatus außerhalb der eingestellten Zeitdifferenz in IS_bES1_2	Sicherer Zustand mit #bES1_OK = NIEDRIG und eingeleitete Reaktion auf einen Fehler ES1_ERROR = NIEDRIG wird geändert in HOCH	ja/nein
ANMERKUNG 7 Diese Diagnosefunktion wird angewendet, um das Betätigungselement für den Not-Halt zu überprüfen.			

6	IS_bES1_2 (E 1.5) ändert den Signalstatus außerhalb der eingestellten Zeitdifferenz in IS_bES1_1	Sicherer Zustand mit #bES1_OK = NIEDRIG und eingeleitete Reaktion auf einen Fehler ES1_ERROR = NIEDRIG wird geändert in HOCH	ja/nein
ANMERKUNG 8 Diese Diagnosefunktion wird angewendet, um das Betätigungselement für den Not-Halt zu überprüfen.			

N.2.4.4 Bewertung der Freigabe/Abschaltung von Motor M1

Tabelle N.7 — FMEA der Freigabe/Abschaltung von Motor M1

Maßgebende Eingänge/maßgebende Kennzeichen				
Beschreibung	I/O	Typ	Information	Beschreibung
#bGD1_OK	Kennzeichen GD1	boolesch	NO	Dieses Freigabekennzeichen wird für die nachfolgende Verarbeitung verwendet.
#bES1_OK	Kennzeichen ES1	boolesch	NO	Dieses Freigabekennzeichen wird für die nachfolgende Verarbeitung verwendet.

Verwendete Software-Blöcke			
Name	Zuvor beurteilter Block der Software-Plattform	Beschreibung	Information
SF_STO	ja	Dieser Block wurde zuvor beurteilt, um das STO über BOOL zu aktivieren. Die Rückmeldung erfolgt automatisch im Block. Tritt ein Fehler auf, wird /STO_ERROR niedrig eingestellt.	

Maßgebende Ausgänge/Kennzeichen				
Beschreibung	O	Typ	Information	Beschreibung
#bSTO_OK	O 1.5	BUS	zuvor beurteilt nach PL d	über Sicherheitsbus zum Wechselrichter 1, aktiviert STO
/STO_ERROR	O 1.6	boolesch	NO	Dieses Fehlerkennzeichen wird für die nachfolgende Verarbeitung verwendet.

Nachweis von ausgeführten DC-Maßnahmen durch Testfälle (Fehlerursache- und -auswirkungsanalyse)			
Nr.	Annahme	Wirkung	Erwartetes Ergebnis
1	GD1_ERROR = hoch	#bGD1_OK = niedrig #bSTO_OK = niedrig /STO_ERROR = niedrig	ja/nein
ANMERKUNG 1 Falls ein Fehler GD1_ ERROR vorliegt, dann sollte der Wechselrichter (FU) ebenfalls abschalten.			
2	ES1_ERROR = hoch	#bES1_OK = niedrig #bSTO_OK = niedrig /STO_ERROR = niedrig	ja/nein
ANMERKUNG 2 Falls ein Fehler ES1_ERROR vorliegt, dann sollte der Wechselrichter (FU) ebenfalls abschalten.			

3	#bGD1_OK = hoch und #bES1_OK = hoch	#bSTO_OK = hoch /STO_ERROR = hoch	ja/nein
Bemerkung: Dies ist der fehlerfreie Zustand.			
4	#bGD1_OK = hoch und #bES1_OK = niedrig	#bSTO_OK = niedrig /STO_ERROR = niedrig	ja/nein
Bemerkung:			
5	#bGD1_OK = niedrig und #bES1_OK = hoch	#bSTO_OK STO_IN = niedrig /STO_ERROR = niedrig	ja/nein
Bemerkung:			
6	#bGD1_OK = niedrig und #bES1_OK = niedrig	#bSTO_OK = niedrig /STO_ERROR = niedrig	ja/nein
Bemerkung:			
7	Fehlerbuskommunikation	#bSTO_OK = niedrig /STO_ERROR = hoch	ja/nein
ANMERKUNG 3 Ernster Fehler (z. B. sollte im Fall eines ernsten Fehlers die Steuerung neu gestartet werden).			

Zusätzlich zum Nachweis des DC sollte Folgendes dokumentiert werden:

— das Datum: JJJJ-MM-TT (derzeit gültige Version/Änderungen);

— der Name: (verantwortliche Person);

— die Softwaresignatur;

— die Hardwaresignatur;

— die signifikanten Reaktionszeiten der Sicherheitsfunktionen (mögliche Verzögerungszeiten).

ACHTUNG — Bei Sicherheitssoftware sollte der erforderliche PL (PL_r) nicht durch eine ODER-Funktion reduziert werden.

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.

Die Geräte können im Allgemeinen anhand folgender Merkmal unterschieden werden:

— 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);

— Gerät, das nur anhand des Entwurfsprozesses des Benutzers als ein SRP/CS oder Teilsystemelement definiert und beurteilt wird (Gerätetyp 2 und Gerätetyp 3).

ANMERKUNG Eine Sicherheitsfunktion nutzt üblicherweise verschiedene Gerätetypen.

Tabelle O.1 — Charakteristische Werte der Gerätetypen

<table>
<tr><th>Charakteristischer Wert</th><th colspan="4">Gerätetyp</th><th>Bemerkung</th></tr>
<tr><td></td><td>1</td><td>2</td><td>3</td><td>4</td><td></td></tr>
<tr><td>PL</td><td rowspan="2">X</td><td></td><td></td><td></td><td>ISO 13849-1</td></tr>
<tr><td>SIL</td><td></td><td></td><td></td><td>IEC 62061</td></tr>
<tr><td>PFH_D</td><td>X</td><td></td><td></td><td></td><td>ISO 13849-1 und IEC 62061</td></tr>
<tr><td>Kategorie</td><td rowspan="2">X</td><td rowspan="2">X</td><td rowspan="2">X</td><td></td><td rowspan="2">ISO 13849-1 und IEC 62061
Einer der charakteristischen Werte ist erforderlich.</td></tr>
<tr><td>HFT</td><td></td></tr>
<tr><td>$MTTF_D$</td><td></td><td rowspan="4">X</td><td></td><td></td><td rowspan="4">ISO 13849-1 und IEC 62061
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 und IEC 62061
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
SFF					IEC 62061[a]
T_{10d}	X	X		X	ISO 13849-1 und IEC 62061 Exakt einer der charakteristischen Werte ist erforderlich.
T_M					
X obligatorisch O optional					

[a] SFF (Anteil sicherer Ausfälle, en: safe failure fraction) wird in IEC 52061, 3.2.5.4, definiert als der Anteil an der Gesamtausfallrate eines Teilsystems, der nicht zu einem gefahrbringenden Ausfall führt.

[b] Wenn kein Sicherheitswert vom Hersteller festgelegt wurde ($MTTF_D$ oder B_{10d}).

O.1.2 Gerätetyp 1

Gerätetyp 1 besitzt den höchsten Integrationsgrad. Typisch sind vorgefertigte Sicherheitssysteme mit integrierter Diagnosefunktion. Dieser Typ wird je nach Verwendungszweck nach SIL oder PL eingestuft. Die Einstufung wird vom Gerätehersteller vorgenommen.

Geräte dieses Typs werden in Übereinstimmung mit Sicherheitsnormen (z. B. IEC 61508) entwickelt.

ANMERKUNG 1 Beispiele für Gerätetyp 1: Sicherheitslichtschranke, Sicherheitslichtgitter, Bauteile von sicherheitsbezogenen Steuerungen, sichere Antriebe/Antriebsfunktionen, 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, Diagnosedeckungsgrad (DC) und Betrachtung von Ausfällen infolge gemeinsamer Ursache (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: nicht-sicherheitsbezogene Elektronik, z. B. Funktionsverstärker, Annäherungsschalter, Drucksensor, Hydraulikventil.

O.1.4 Gerätetyp 3

Geräte vom Typ 3 sind Bauteile mit einer Ausfallart, die von den Betriebszyklen abhängig ist.

Ergänzende Anwendungsdaten (Anzahl der Schaltspiele, Anzahl der Aktivierungen, Struktur des Schaltkreises, Diagnosedeckungsgrad (DC) und Betrachtung von Ausfällen infolge gemeinsamer Ursache (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 eintritt, beträgt ungefähr $PFH_D = 0$. Für Bauteiles dieses Typs gilt einer der folgenden Punkte für jeden potentiellen 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. IEC 61508) beurteilt werden.

O.2 Software

O.2.1 Allgemeines

Wird im Bauteil eine Software verwendet, sollte der Gerätehersteller Angaben zur Eignung der Software entsprechend dem PL machen.

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

Veröffentlichungen zu programmierbaren elektronischen Systemen

[1] IEC 61496-1:2014, *Safety of machinery — Electro-sensitive protective equipment — Part 1: General requirements and tests*

[2] IEC 61496-2:2014, *Safety of machinery — Electro-sensitive protective equipment — Part 2: Particular requirements for equipment using active opto-electronic protective devices*

[3] IEC 61496-3:2019, *Safety of machinery — Electro-sensitive protective equipment — Part 3: Particular requirements for active opto-electronic protective devices responsive to diffuse reflection (AOPDDR)*

[4] IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements*

[5] 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*

[7] IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations*

[8] IEC 61508-5:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 5: Examples of methods for the determination of safety integrity levels*

[9] 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*

[10] IEC 61508-7:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures*

Weitere Veröffentlichungen

[11] ISO 11161:2007, *Safety of machinery — Integrated manufacturing systems — Basic requirements*

[12] ISO 13850:2015, *Safety of machinery — Emergency stop function — Principles for design*

[13] ISO 13851:2019, *Safety of machinery — Two-hand control devices — Principles for design and selection*

[14] ISO 13856-1:2013, *Safety of machinery — Pressure-sensitive protective devices — Part 1: General principles for design and testing of pressure-sensitive mats and pressure-sensitive floors*

[15] ISO 13856-2:2013, *Safety of machinery — Pressure-sensitive protective devices — Part 2: General principles for design and testing of pressure-sensitive edges and pressure-sensitive bars*

[16] ISO 11428:1996, *Ergonomics — Visual danger signals — General requirements, design and testing*

[17] ISO 9001:2013, *Quality management systems — Requirements*

[18] ISO 9355-1:1999, *Ergonomic requirements for the design of displays and control actuators — Part 1: Human interactions with displays and control actuators*

[19] ISO 9355-2:1999, *Ergonomic requirements for the design of displays and control actuators — Part 2: Displays*

[20] ISO 9355-3:2006, *Ergonomic requirements for the design of displays and control actuators — Part 3: Control actuators*

[21] ISO 11429:1996, *Ergonomics — System of auditory and visual danger and information signals*

[22] ISO 7731:2008, *Ergonomics — Danger signals for public and work areas — Auditory danger signals*

[23] ISO 4413:2010, *Hydraulic fluid power — General rules and safety requirements for systems and their components*

[24] ISO 4414:2010, *Pneumatic fluid power — General rules and safety requirements for systems and their components*

[25] ISO 14118:2017, *Safety of machinery — Prevention of unexpected start-up*

[26] ISO 14119:2013, *Safety of machinery — Interlocking devices associated with guards — Principles for design and selection*

[27] ISO 19973 (all parts), *Pneumatic fluid power — Assessment of component reliability by testing*

[28] ISO/TR 22100-2:2013, *Safety of machinery — Relationship with ISO 12100 — Part 2: How ISO 12100 relates to ISO 13849-1*

[29] ISO/TR 22100-4:2020, *Safety of machinery — Relationship with ISO 12100 — Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects*

[30] IEC 60204-1:2019, *Safety of machinery — Electrical equipment of machines — Part 1: General requirements*

[31] IEC 60447:2017, *Basic and safety principles for man-machine interface (MMI) — Actuating principles*

[32] IEC 60529:1989+AMD2:2013, *Degrees of protection provided by enclosures (IP code)*

[33] IEC 60812:2018, *Analysis techniques for system reliability — Procedure for failure mode and effects analysis (FMEA)*

[34] IEC 60947 (all parts), *Low-voltage switchgear and controlgear*

[35] IEC 61000-1-2:2016, *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*

[36] IEC 61000-6-2:2016, *Electromagnetic compatibility (EMC) — Part 6-2: Generic standards — Immunity for industrial environments*

[37] 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*

[38] IEC 61078:2016, *Reliability block diagrams*

[39] IEC 61326-3-1:2017, *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*

[40] IEC 61800-3:2017, *Adjustable speed electrical power drive systems — Part 3: EMC requirements and specific test methods*

[41] IEC 61800-5-2:2016, *Adjustable speed electrical power drive systems — Part 5-2: Safety requirements — Functional*

[42] IEC 61810 (all parts), *Electromagnetic elementary relays*

[43] IEC 61300 (all parts), *Fibre optic interconnecting devices and passive components — Basic test and measurement procedures*

[44] IEC 61310 (all parts), *Safety of machinery — Indication, marking and actuation*

[45] IEC 61131-3:2013, *Programmable controllers — Part 3: Programming languages*

[46] IEC 60050-192:2015, *International electrotechnical vocabulary — Chapter 191: Dependability and quality of service. Geändert durch IEC 60050-191-am1:1999 und IEC 60050-191-am2:2002:1999*

[47] EN 614-1:2006, *Sicherheit von Maschinen — Ergonomische Gestaltungsgrundsätze — Teil 1: Begriffe und allgemeine Leitsätze*

[48] EN 1005-3:2002, *Sicherheit von Maschinen — Menschliche körperliche Leistung — Teil 3: Empfohlene Kraftgrenzen bei Maschinenbetätigung*

[49] IEC 61810-3:2015, *Electromechanical elementary relays — Part 3: Relays with forcibly guided (mechanically linked) contacts*

[51] Goble W.M. *Control systems Safety Evaluation and Reliability*. 3rd Edition:2010 (ISBN-101934394807)

[52] IFA-Report 2/2017e, *Functional safety of machine controls — Application of ISO 13849*, German Social Accident Insurance (DGUV), Juni 2009, ISBN 978-3-88383-793-2, kostenlos abrufbar unter: www.dguv.de/ifa/13849e

[53] IEC 61506:1997, *Documentation of software for process control systems and facilities*

[54] ISO/IEC/IEEE 26512:2018, *Systems and software engineering — Requirements for acquirers and suppliers of information for users*

[55] ISO/TR 14121-2:2012, *Safety of machinery — Risk assessment — Part 2: Practical guidance and examples of methods*

[56] ISO 10218-1:2011, *Robots and robotic devices — Safety requirements for industrial robots — Part 1: Robots*

[57] ISO 10218-2:2011, *Robots and robotic devices — Safety requirements for industrial robots — Part 2: Robot systems and integration*

[58] CHINNIAH YUVIN, (2015) *Analysis and prevention of serious and fatal accidents related to moving parts of machinery*, Safety Science 75 (2015) 163–173

[59] 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

[60] ANSI B11.26 — 2018 *Functional Safety for Equipment: General Principles for the Design of Safety Control Systems Using ISO 13849-1*

[61] EN 50495:2010, *Sicherheitseinrichtungen für den sicheren Betrieb von Geräten im Hinblick auf Explosionsgefahren*

[62] VDMA 66413:2012, *Funktionale Sicherheit — Universelle Datenbasis für sicherheitsbezogene Kennwerte von Komponenten oder Teilen von Steuerungen*

[63] VDMA 24584:2020, *Sicherheitsfunktionen geregelter und nicht geregelter (fluid-)mechanischer Systeme*

[64] IFA. „*SISTEMA Cookbook 6: Definition of safety functions: what is important?*“ (https://www.dguv.de/medien/ifa/en/pra/softwa/sistema/kochbuch/sistema_cookbook6_en.pdf)

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

[66] ISO 60947-4-1:2018, *Low-voltage switchgear and controlgear — Part 4-1: Contactors and motor-starters — Electromechanical contactors and motor-starters*

[67] ISO 60947-5-1:2020, *Low-voltage switchgear and controlgear — Part 5-1: Control circuit devices and switching elements — Electromechanical control circuit devices*

[66] ISO 60947-5-5:2017, *Low-voltage switchgear and controlgear — Part 5-5: Control circuit devices and switching elements — Electrical emergency stop device with mechanical latching function*

[66] ISO 60947-5-8:2008, *Low-voltage switchgear and controlgear — Part 5-8: Control circuit devices and switching elements — Three-position enabling switches*

[67] ISO 61810-2-1:2017, *Electromechanical elementary relays — Part 2-1: Reliability — Procedure for the verification of B_{10} values*

[68] ISO 8573-1:2010, *Compressed air — Part 1: Contaminants and purity classes*

[69] IEC/TR 63074:2021, *Safety of machinery — Security aspects related to functional safety of safety-related control systems*

[70] ISO 16090-1:2017, *Machine tools safety — Machining centres, Milling machines, Transfer machines — Part 1: Safety requirements*

[71] ISO 23125:2015, *Machine tools — Safety — Turning machines*

[72] ISO/TS 10566:2017, *Robots and robotic devices — Collaborative robots*

[73] IEC 61310-1:2007, *Safety of machinery — Indication, marking and actuation — Part 1: Requirements for visual, acoustic and tactile signals*

Datenbanken

[74] IEC 61709:2017[2], *Electric components — Reliability — Reference conditions for failure rates and stress models for conversion*

[75] *Reliability Prediction of Electronic Equipment*, MIL-HDBK-217E, Notice-2, Department of Defense, Washington, DC, 1995

[76] *Reliability Prediction Procedure for Electronic Equipment*, Telcordia SR-332, Issue 04, 2016 (https://www.ericsson.com/en)

[77] *British Handbook for Reliability Data for Components used in Telecommunication Systems*, British Telecom (HRD5, last issue)

[78] Chinese Military Standard, GJB/Z 299C-2006 *Reliability prediction handbook for electronic equipment (Englische Fassung)*

[79] 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, Deutschland (www.ifm.com/obj/EMC-Pocket-Guide-ZVEI-english.pdf)

2 Identisch mit RDF 2000/*Reliability Data Handbook*, UTE C 80-810, Union Technique de l'Electricité et de la Communication.

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 199, *Safety of machinery*.

This fourth edition cancels and replaces the third edition (ISO 13849-1:2015), which has been technically revised.

The main changes compared to the previous edition are improvements and as follows:

— specification of the safety functions (clause 5);

— software (clause 7);

— validation (clause 10);

— combination of several subsystems ;

— management of the functional safety (Annex G.5) ;

— EMC immunity (annex L);

— additional information for safety requirements specification (annex M);

— avoiding of fault avoiding measures for the design of safety related software (annex N);

— safety-related values of components or parts of the control systems (Annex O).

A list of all parts in the ISO 13849 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document is a type-B1 standard as stated in ISO 12100.

The first edition of ISO 13849-1 was published in 1999 based on EN 954-1:1996.

The second edition of ISO 13849-1 was revised in 2006.

The third edition was amended and published in 2015.

This fourth edition cancels and replaces the third edition (ISO 13849-1:2015), which has been technically revised.

This document is of relevance, in particular, for the following stakeholder groups with regard to machinery safety:

— machine manufacturers (small, medium and large enterprises);

— health and safety bodies (regulators, accident prevention organisations, market surveillance).

Others can be affected by the level of machinery safety achieved with the means of the document by the above-mentioned stakeholder groups:

— machine users/employers (small, medium and large enterprises);

— machine users/employees (e.g. trade unions);

— service providers, e.g. for maintenance (small, medium and large enterprises);

— consumers (in case of machinery intended for use by consumers).

The above-mentioned stakeholder groups have been given the possibility to participate in the drafting process of this document.

In addition, this document is intended for standardization bodies elaborating type-C standards.

The requirements of this document can be supplemented or modified by a type-C standard.

For machines which are covered by the scope of a type-C standard and which have been designed and built according to the requirements of that standard, the requirements of that type-C standard take precedence.

NOTE 1 The examples and basis for most content is based on stationary machines in factory applications. However, other machines are not excluded. This document was written with the intent of being used across many machinery industries and as a basis for type-C standards developers.

This document is intended to give guidance to those involved in the design and assessment of control systems, and those preparing type-B2 or type-C standards.

Risk reduction according to ISO 12100:2010, Clause 6, is accomplished by applying, in the following sequence, inherently safe design measures, safeguarding and/or complementary risk reduction measures and information for use. A designer may reduce risks by risk reduction measures that can have safety functions. Parts of machinery control systems that are assigned to provide safety functions are called safety-related parts of control systems (SRP/CS). These can consist of hardware and/or software, and can either be separate from the machine control system or an integral part of it. In addition to implementing safety functions, SRP/CS can also implement operational functions.

ISO 12100 is used for risk assessment of the machine. Annex A of this document can be used for the determination of the required performance level of a safety function performed by the SRP/CS, where PL_r is not specified in the applicable type-C standard.

This document is relevant for the SRP/CS safety functions that are used to address risks for cases where a risk assessment conducted according to ISO 12100 is needed. ISO 12100 determines that a risk reduction measure is needed that relies on a safety function (e.g. interlocking guard). In those cases, the safety-related control system has to perform a safety function. This document should be used to design and evaluate the safety-related parts of the control system. Only the part of the control system that is safety-related falls under the scope of this document

Figure 1, taken from ISO 12100, illustrates the relationship between ISO 12100 and this document. For a detailed overview see Figure 2.

NOTE 2 See also ISO/TR 22100-2:2013 for further information.

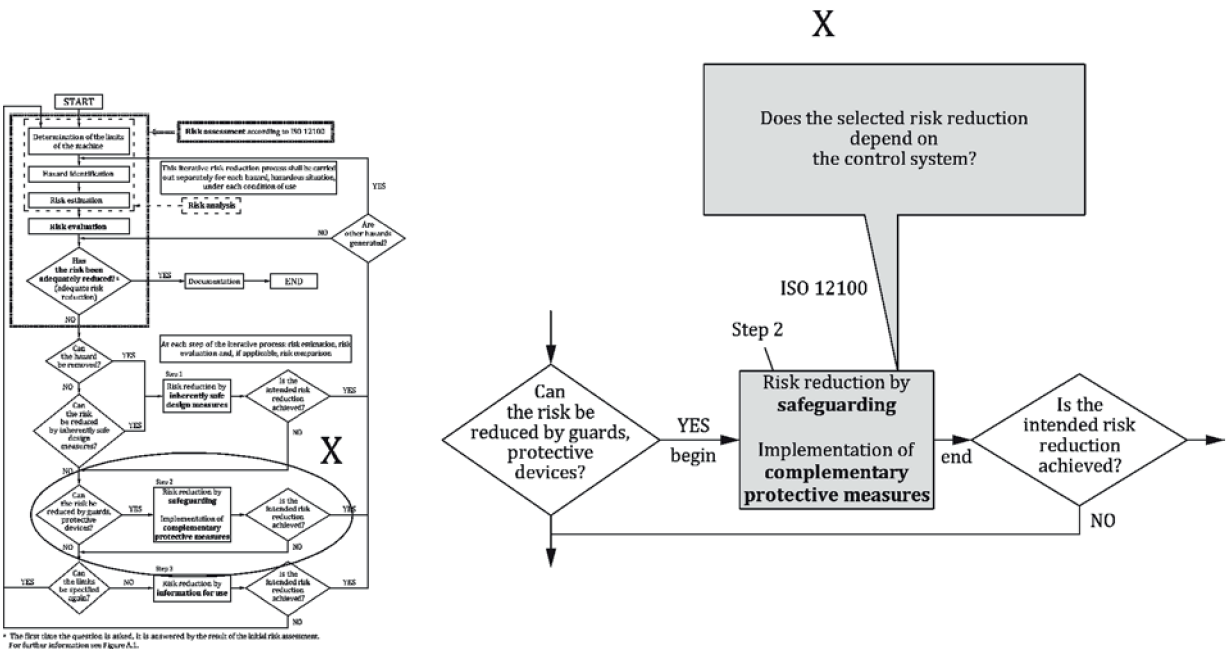


Figure 1 — Integration of ISO 13849-1 within the risk reduction process of ISO 12100

NOTE 3 Figure 1 shows where the SRP/CS contributes to the risk reduction process of ISO 12100:2010: Step 2. The SRP/CS supports the combined risk reduction measures by the implementation of safety functions.

The ability of safety-related parts of control systems to perform a safety function under foreseeable conditions is allocated one of five levels, called performance levels (PL). The required performance level (PLr) for a particular safety function will be determined by risk estimation.

The probability of dangerous failure of the safety function depends on several factors, including but not limited to hardware and software structure, the extent of fault detection mechanisms (diagnostic coverage (DC)), reliability of components (mean time to dangerous failure ($MTTF_D$), common cause failure (CCF)), design process, operating stress, environmental conditions and operation procedures.

In order to facilitate the design of SRP/CS and the assessment of achieved PL, this document employs a methodology based on the categorization of architectures with specific design criteria ($MTTF_D$, DC_{avg}, etc.) and specified behaviour under faults conditions. These architectures are allocated one of five levels termed Categories B, 1, 2, 3 and 4..

Functional safety considers the failure characteristics of elements/components performing a safety function. For each safety function, this failure characteristic is expressed as the probability of dangerous failure per hour (PFH_D).

Risk estimation will show a variance because of the subjective nature of the evaluation criteria. Type-C standards can have more specific risk estimation methods for specific machine applications. Therefore,

using the methodology in this document should be considered as valuable guidance for the design of the safety-related parts of the control system.

The performance levels and categories can be applied to safety-related parts of control systems, such as

— control units (e.g. a logic unit for control functions, data processing, monitoring) and

— electro-sensitive protective devices (e.g. photoelectric barriers), pressure sensitive devices.

The performance levels can be defined, and categories determined for subsystems of SRP/CS using safety parts (components) such as

— protective devices (e.g. two-hand control devices, interlocking devices);

— power control elements (e.g. relays, valves);

— sensors and HMI elements (position sensors, enable switches).

Machinery considered by this document can range from simple (e.g., small kitchen machines, or automatic doors and gates) to complex (e.g., packaging machines, printing machines, presses and integrated machinery into a system).

This document and IEC 62061, both documents specify a methodology and provide related guidance for the design and implementation of safety-related control systems of machinery.

The requirements of Clause 10 of this document supersede the requirements of ISO 13849-2:2012 with the exception of the informative annexes. An SRP/CS that meets the requirements of Clause 10 is considered to meet the requirements of ISO 13849-2:2012.

Safety of machinery — Safety-related parts of control systems —

Part 1: General principles for design

1 Scope

This document specifies a methodology and provides related recommendations and requirements for the design and integration of safety-related parts of control systems (SRP/CS), including the design of software. This document specifies a methodology and provides related guidance for the design and integration of safety-related parts of control systems (SRP/CS) that perform safety functions, including the design of software. This document applies to SRP/CS for high demand and continuous mode including their subsystems, regardless of the type of technology and energy (e.g. electrical, hydraulic, pneumatic, and mechanical). This document does not apply to low demand mode.

NOTE 1 See 3.1.43 and IEC 61508 for low demand mode. This document does not specify the safety functions or required performance levels that are to be used in particular applications.

This document does not give specific requirements for the design of products/components that are parts of SRP/CS. Specific requirements for the design of components of SPR/CS are covered by applicable ISO and IEC-standards.

This document does not provide specific measures for security (e.g. physical, IT-security, cyber security) aspects.

NOTE 2 Security issues can have an effect on safety functions. See ISO/TR 22100-4 and IEC/TR 63074 for further information.

NOTE 3 This document specifies a methodology for SRP/CS design without considering if certain machinery (e.g. mobile machinery) has specific requirements. These specific requirements can be considered in a Type-C standard.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 12100:2010, *Safety of machinery — General principles for design — Risk assessment and risk reduction*

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

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

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

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

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

3 Terms, definitions, symbols and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 12100:2010 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at https://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp

3.1.1
safety–related part of a control system
SRP/CS
part of a control system that performs a safety function, starting from a safety-related input(s) to generating a safety-related output(s)

Note 1 to entry: The safety-related parts of a control system start at the point where the safety-related inputs are initiated (including, for example, the actuating cam and the roller of the position switch) and end at the output of the power control elements (including, for example, the main contacts of a contactor).

3.1.2
machine control system
system which responds to input signals from parts of machine elements, operators, external control equipment or any combination of these and generates output signals causing the machine to behave in the intended manner

Note 1 to entry: The machine control system can use any technology or any combination of different technologies (e.g. electrical/electronic, hydraulic, pneumatic and mechanical).

3.1.3
safety requirements specification
SRS
specification containing the requirements for the safety functions that have to be met by the safety-related control system in terms of characteristics of the safety functions (functional requirements) and required performance levels

[SOURCE: IEC 61508-4:2010, 3.5.11, modified, information from 3.5.12 included]

3.1.4
category
classification of the subsystem in respect of the resistance to faults and the subsequent behaviour in the fault condition which is achieved by the structural arrangement of the parts, fault detection and/or by their reliability

3.1.5
performance level
PL
discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions

Note 1 to entry: See 6.1.

3.1.6
required performance level
PL_r
performance level required in order to achieve the required risk reduction for each safety function

Note 1 to entry: See 5.3 and Figure A.1.

3.1.7
safety integrity level
SIL
discrete level (one out of a possible four) for specifying the safety integrity requirements of safety functions to be allocated to the safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

Note 1 to entry: In this document only SIL 1 to SIL 3 are considered.

[SOURCE: IEC 61508-4:2010, 3.5.8, modified – NOTES deleted and “allocated to safety-related systems” added]

3.1.8
fault
state of a device characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, Note 1 to entry: A fault is often the result of a failure of the item itself, but can exist without prior failure.

Note 1 to entry: In this document “fault” means random fault or fault caused by a systematic failure.

[SOURCE: IEC 60050-192:2015, modified — NOTE 2 to entry amended.]

3.1.9
fault exclusion
exclusion of certain faults within a SRP/CS, if this can be justified due to their improbability and their negligible contribution to the reliability of the SRP/CS

3.1.10
failure
termination of the ability of a device to perform a required function

Note 1 to entry: After a failure, the device has a fault.

Note 2 to entry: “Failure” is an event, as distinguished from “fault”, which is a state.

Note 3 to entry: Failures which only affect the availability of the process under control are outside of the scope of this document.

[SOURCE: IEC 60050-192:2015, modified — NOTE 3 to entry had been amended.]

3.1.11
permanent fault
fault of an item that persists until an action of corrective maintenance is performed

[SOURCE: IEC 60050-192:2015]

3.1.12
dangerous failure
failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:

a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the SRP/CS is put into a hazardous or potentially hazardous state; or

b) decreases the probability that the safety function operates correctly when required

[SOURCE: IEC 61508 4:2010, 3.6.7, modified, "EUC" replaced by " SRP/CS"]

3.1.13
common cause failure
CCF
failure, that is the result of one or more events, causing concurrent failures of two or more separate channels in a multiple channel subsystem, leading to failure of a safety function

Note 1 to entry: Common cause failures are not identical with common mode failures (see ISO 12100:2010, 3.36).

[SOURCE: IEC 61508-4:2010, 3.6.10, NOTE 1 added]

3.1.14
systematic failure
failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

Note 1 to entry: Corrective maintenance without modification will usually not eliminate the failure cause.

Note 2 to entry: A systematic failure can be induced by simulating the failure cause.

Note 3 to entry: Examples of causes of systematic failures include human error in

— the safety requirements specification,

— the design, manufacture, installation, operation of the hardware, and

— the design, implementation, of the software.

[SOURCE: IEC 60050-192:2015]

3.1.15
muting
temporary automatic suspension of a safety function(s) by the SRP/CS

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

3.1.16
manual reset
safety function within the SRP/CS used to restore manually one or more safety functions before re-starting a machine

3.1.17
harm
physical injury or damage to health

[SOURCE: ISO 12100:2010, 3.5]

3.1.18
hazard
potential source of harm

Note 1 to entry: A hazard can be qualified in order to define its origin (e.g. mechanical hazard, electrical hazard) or the nature of the potential harm (e.g. electric shock hazard, cutting hazard, toxic hazard and fire hazard).

Note 2 to entry: The hazard envisaged in this definition:

— either is permanently present during the intended use of the machine (e.g. motion of hazardous moving elements, electric arc during a welding phase, unhealthy posture, noise emission, high temperature);

— or can appear unexpectedly (e.g. explosion, crushing hazard as a consequence of an unintended/unexpected start-up, ejection as a consequence of a breakage, fall as a consequence of acceleration/deceleration).

[SOURCE: ISO 12100:2010, 3.6, modified — NOTE 3 to entry has been deleted.]

3.1.19
hazardous situation
circumstance in which a person is exposed to at least one hazard

Note 1 to entry: The exposure can result in harm immediately or over a period of time.

[SOURCE: ISO 12100:2010, 3.10]

3.1.20
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO 12100:2010, 3.12]

3.1.21
residual risk
risk remaining after risk reduction measures (protective measures) have been taken

Note 1 to entry: See Figure 3.

[SOURCE: ISO 12100:2010, 3.13, modified — Note 1 to entry has been modified.]

3.1.22
risk assessment
overall process comprising risk analysis and risk evaluation

[SOURCE: ISO 12100:2010, 3.17]

3.1.23
risk reduction measure
protective measure
action or means to eliminate hazards or reduce risks

EXAMPLE Inherently safe design; protective devices; personal protective equipment; information for use and installation; organization of work; training; application of equipment; supervision.

[SOURCE: ISO Guide 51:2014, 3.13]

3.1.24
risk analysis
combination of the specification of the limits of the machine, hazard identification and risk estimation

[SOURCE: ISO 12100:2010, 3.15]

3.1.25
risk evaluation
judgement, on the basis of risk analysis, of whether risk reduction objectives have been achieved

[SOURCE: ISO 12100:2010, 3.16]

3.1.26
intended use of a machine
use of a machine in accordance with the information provided in the instructions for use

[SOURCE: ISO 12100:2010, 3.23]

3.1.27
reasonably foreseeable misuse
use of a machine in a way not intended by the designer, but which can result from readily predictable human behaviour

[SOURCE: ISO 12100:2010, 3.24]

3.1.28
safety function
function of the machine whose failure can result in an immediate increase of the risk(s)

Note 1 to entry: A safety function is a function to be implemented by a safety-related part of a control system, which is needed to achieve or maintain a safe state for the machine, in respect of a specific hazardous event.

[SOURCE: ISO 12100:2010, 3.30]

3.1.29
sub-function
part of a safety function whose failure results in a failure of the safety function

Note 1 to entry: A sub-function is a function to be implemented by a subsystem of the SRP/CS. See also IEC 61800-5-2:2016.

EXAMPLE Sub-functions according to IEC 61800-5-2 are e.g. safe torque off (STO), safe stop 1 (SS1). See figure 6.

3.1.30
monitoring
diagnostic measure which detects a state and compares it to the expected value

Note 1 to entry: Monitoring is realised by following methods: plausibility check (direct. Indirect or cross monitoring, see 3.1.24), cyclic test stimulus or cross monitoring.

3.1.31
cross monitoring
diagnostic measure which checks plausibility of redundant signals in both channels of a redundant subsystem

3.1.32
programmable electronic system
PE system
system for control, protection or monitoring based on one or more programmable electronic devices, including all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices

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

3.1.33
mean time to dangerous failure
$MTTF_D$
expectation of the mean time to dangerous failure

Note 1 to entry: In the case of items with an exponential distribution of operating times to dangerous failure (i.e. a constant failure rate) the $MTTF_D$ is numerically equal to the reciprocal of the dangerous failure rate".

[SOURCE: IEC 62061:2019, 3.2.34, modified — NOTE 1 to entry has been modified]

3.1.34
mean time between failures
MTBF
expected value of the operating time between consecutive failures

3.1.35
ratio of dangerous failures
RDF
fraction of the overall failure rate of an element that can result in a dangerous failure

3.1.36
diagnostic coverage
DC
measure of the effectiveness of diagnostics, which is determined as the ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures

Note 1 to entry: Diagnostic coverage can exist for the whole or parts of a safety-related system. For example, diagnostic coverage could exist for sensors and/or logic system and/or power control elements.

3.1.37
mission time
T_M
period of time covering the intended use of an SRP/CS

3.1.38
test rate
r_t
frequency of tests to detect faults in an SRP/CS, reciprocal value of diagnostic test interval

3.1.39
demand rate
r_d
frequency of demands for a safety function to be performed by the SRP/CS

3.1.40
limited variability language
LVL
type of language that provides the capability to combine predefined, application specific, library functions to implement the safety requirements specifications

Note 1 to entry: A LVL provides a close functional correspondence with the functions required to achieve the application.

Note 2 to entry: Typical examples of LVL are given in IEC 61131-3. They include ladder diagram, function block diagram and sequential function chart. Instruction lists and structured text are not considered to be LVL.

Note 3 to entry: Typical example of systems using LVL: Programmable Logic Controller (PLC) configured for machine control

[SOURCE: IEC 62061, FDIS 2020, 3.2.62]

3.1.41
full variability language
FVL
type of language that provides the capability to implement a wide variety of functions and applications

Note 1 to entry: Typical example of systems using FVL are general-purpose computers.

Note 2 to entry: FVL is normally found in embedded software and is rarely used in application software.

Note 3 to entry: FVL examples include: Ada, C, Pascal, Instruction List, assembler languages, C++, Java, SQL.

[SOURCE: IEC 62061, FDIS 2020, 3.2.61]

3.1.42
safety-related application software
SRASW
software specific to the application and generally containing logic sequences, limits and expressions that control the appropriate inputs, outputs, calculations and decisions necessary to meet the SRP/CS requirements

3.1.43
safety-related embedded software
SRESW
firmware
software that is part of the system supplied by the manufacturer

Note 1 to entry: Embedded software is usually written in FVL.

[SOURCE: IEC 61511-1:2016, 3.2.76.2, modified – "and is not accessible for modification by the user of the machinery" deleted]

3.1.44
high demand or continuous mode
mode of operation in which the frequency of demands on an SRP/CS to perform its safety function is greater than one per year or the safety function retains the machine in a safe state as part of normal operation

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

3.1.45
low demand mode
mode of operation in which the frequency of demands on the SRP/CS to perform its safety function is not greater than once per year

Note 1 to entry: Low demand mode is not addressed in this document, see Clause 1.

[SOURCE: IEC 61508-4:2010, 3.5.16, modified — NOTE amended]

3.1.46
subsystem
entity which results from a first-level decomposition of an SRP/CS and whose dangerous failure results in a dangerous failure of a safety function

Note 1 to entry: The subsystem specification includes its role in the safety function and its interface with the other subsystems of the SRP/CS.

Note 2 to entry: One subsystem can be part of one or several SRP/CS, e.g. the same combination of contactors can be used to de-energise a motor in case of detection of a person in a danger zone and also in case of opening a safe guard.

3.1.47
subsystem element
part of a subsystem comprising a single component or any group of components

Note 1 to entry: A subsystem element can comprise hardware or a combination of hardware and software. For the purposes of this document, software-only components are not considered subsystem elements.

3.1.48
channel
element or group of elements that independently implement a safety function or a part of it

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

3.1.49
well-tried safety principle
principles that have proved effective in the design or integration of safety-related control systems in the past, to avoid or control critical faults or failures which can influence the performance of a safety function

Note 1 to entry: Newly developed safety principles can only be considered as equivalent to well-tried if they are verified using methods which demonstrate their suitability and reliability for safety-related applications.

Note 2 to entry: Well-tried safety principles are effective not only against random hardware failures, but also against systematic failures which can creep into the product at some point in the course of the product life cycle, e.g. faults arising during product design, integration, modification or deterioration.

Note 3 to entry: Table A.2, Table B.2, Table C.2 and Table D.2 of ISO 13849-2:2012 address well-tried safety principles for different technologies.

3.1.50
well-tried component
component-successfully used in safety-related applications

Note 1 to entry: See 6.1.11 for requirements and ISO 13849-2 for a list of recognized well-tried components.

3.1.51
operating mode
mode of operation in a machine (e.g. automatic, manual, maintenance) to select predefined machine functions and safety measures related to those functions

Note 1 to entry: For each specific operating mode, the relevant safety functions and/or risk reduction measures are implemented.

Note 2 to entry: Operating mode is not a machine function itself. The functions (including safety functions) summarized under an operating mode can only be used when that particular operating mode has been activated.

3.1.52
dynamic test
monitored diagnostic measure which at appropriate intervals executes a change of a signal for test purposes

Note 1 to entry: The test fails if monitoring did not detect the change as expected.

Note 2 to entry: The use of test pulses is a common technology of dynamic testing and is widely used to detect short circuits or interruptions in signal paths or malfunctions.

3.1.53
plausibility check
diagnostic measure which is monitoring that the state of an input (output) fits to the state of the system or other inputs (outputs)

3.1.54
verification
confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

Note 1 to entry: The objective evidence needed for a verification can be the result of an inspection or of other forms of determination such as performing alternative calculations or reviewing documents.

Note 2 to entry: The activities carried out for verification are sometimes called a qualification process.

Note 3 to entry: The word “verified” is used to designate the corresponding status.

[SOURCE: ISO 9000:2015, 3.8.12, .]

3.1.55
validation
confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled

Note 1 to entry: The objective evidence needed for a validation is the result of a test or other form of determination such as performing alternative calculations or reviewing documents.

Note 2 to entry: The word “validated” is used to designate the corresponding status.

Note 3 to entry: The use conditions for validation can be real or simulated.

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

3.1.56
skilled person
person with relevant training, education, and experience to enable him or her to perceive risks and to avoid hazards associated with the relevant equipment

Note 1 to entry: Several years of practice in the relevant technical field can be taken into consideration in assessment of professional training.

[SOURCE: ISO 14990-1:2016, 3.5.4, modified — "electricity" has been replaced by "the relevant equipment".]

3.1.57
Black box
device, system or object which can be viewed in terms of its inputs and outputs

3.1.58
grey box
device, system or object where some of the internal functions are known

Note 1 to entry: The third way for functional testing is "white box", where all internal functions are known.

3.2 Symbols and abbreviated terms

Table 1 gives an overview on used abbreviations and terms.

Table 1 — Symbols and abbreviated terms

Symbol or abbreviation	Description	Definition or occurrence
a, b, c, d, e	denotation of performance levels	Table K.1
AOPD	active optoelectronic protective device (e.g. light barrier)	Annex H
B, 1, 2, 3, 4	denotation of categories	Table 4
B_{10D}	number of cycles until 10 % of the components fail dangerously (for components with mechanical wear)	Annex C
Cat.	category	3.1.3
CC	current converter	Annex I
CCF	common cause failure	3.1.8
DC	diagnostic coverage	3.1.31
DC_{avg}	average diagnostic coverage	E.2
EMI	electromagnetic interference	6.2.2
ETA	event tree analysis	10.3.2
F, F1, F2	frequency and/or time of exposure to the hazard	A.2.2
FB	function block	Annex J
FVL	full variability language	3.1.40
FMEA	failure modes and effects analysis	6.1.5
FMECA	failure modes, effects and critically analysis	10.3.2
FTA	fault tree analysis	10.3.2
F(t)	cumulated distribution function	Annex C.4.3
HFT	hardware fault tolerance	6.1
I, I1, I2	input device, e.g. sensor	6.1
i, j	index for counting	Annex D
I/O	inputs/outputs	Table E.1 and E.2

Table 1 *(continued)*

Symbol or abbreviation	Description	Definition or occurrence
i_m	interconnecting means	Figure 7, 8, 9, 10
K1A, K1B	contactors	Annex I
L, L1, L2	logic	6.1
LVL	limited variability language	3.1.38
λ_D	dangerous failure rate of a component	Annex C
M	motor	Annex I
MTTF	mean time to failure	Annex C
$MTTF_D$	mean time to dangerous failure	3.1.28
n, N, Ñ	number of items	6.2, D.1
N_{low}	number of subsystems with PL_{low} in a combination of subsystems	6.2
n_{op}	mean number of annual operations	Annex C
O, O1, O2, OTE	output device, e.g. power control elements	6.1
P, P1, P2	possibility of avoiding the hazard	A.2.3
PES	programmable electronic system	3.1.26
PFH_D	average probability of dangerous failure per hour	Table 2 and Table K.1
PL	performance level	3.1.27
PLC	programmable logic controller	Annex I
PL_{low}	lowest performance level of a subsystem in a combination of subsystems	6.2
PL_r	required performance level	3.1.27
r_d	demand rate	3.1.35
r_t	test rate	3.1.34
RDF	ratio of dangerous failures	C.4.2
RS	rotation sensor	Annex I
S, S1, S2	severity of injury	A.2.1
SB	subsystem	Figure 13, H.1, H.2
SOS	safe operating stop	5.2.3.1
SS2	safe stop 2	5.2.3.1
SW1A, SW1B, SW2	position switches	Annex I
SIL	safety integrity level	3.1.38, Clause 6
SLS	Safely limited speed	Table 3
SRASW	safety-related application software	3.1.40
SRESW	safety-related embedded software	3.1.41
SRP	safety-related part	General
SRP/CS	safety-related part of a control system	3.1.1
SRS	safety requirements specification	3.1.2
STO	safe torque off	Table 3 and N.2
TE	test equipment	6.1
T_M	mission time	3.1.33
T_{10D}	mean time until 10 % of the components fail dangerously	Annex C

4 Overview

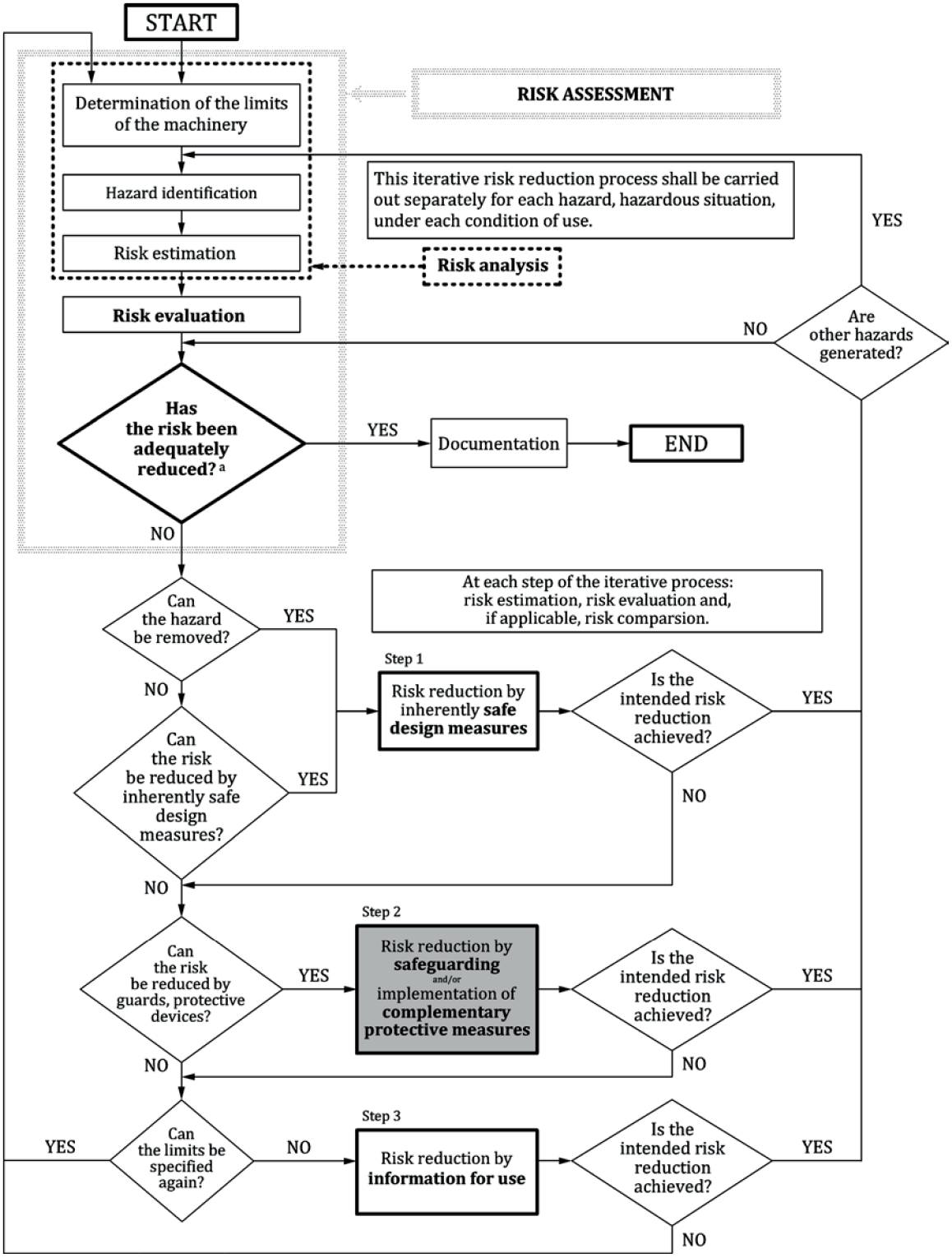
4.1 Risk assessment and risk reduction process at the machine

The risk assessment and risk reduction process is defined by ISO 12100:2010 as shown in Figure 2. ISO 13849-1 is included in the risk reduction process when a safety function and its corresponding SRP/CS are used to provide the risk reduction.

NOTE For further information see ISO/TR 22100-2: 2013.

The safety requirements specification and the design of the SRP/CS shall take into account the result of the risk assessment including the intended use and reasonably foreseeable misuse of the machine (see Figure 1 and Figure 2).

NOTE This document does not apply to non-safety-related parts of control systems of a machine (see Figure 6).



Key

a The first time the question is asked, it is answered by the result of the initial risk assessment.

▢ risk reduction by safeguarding may be realized by SRP/CS that execute safety functions. In this case this document

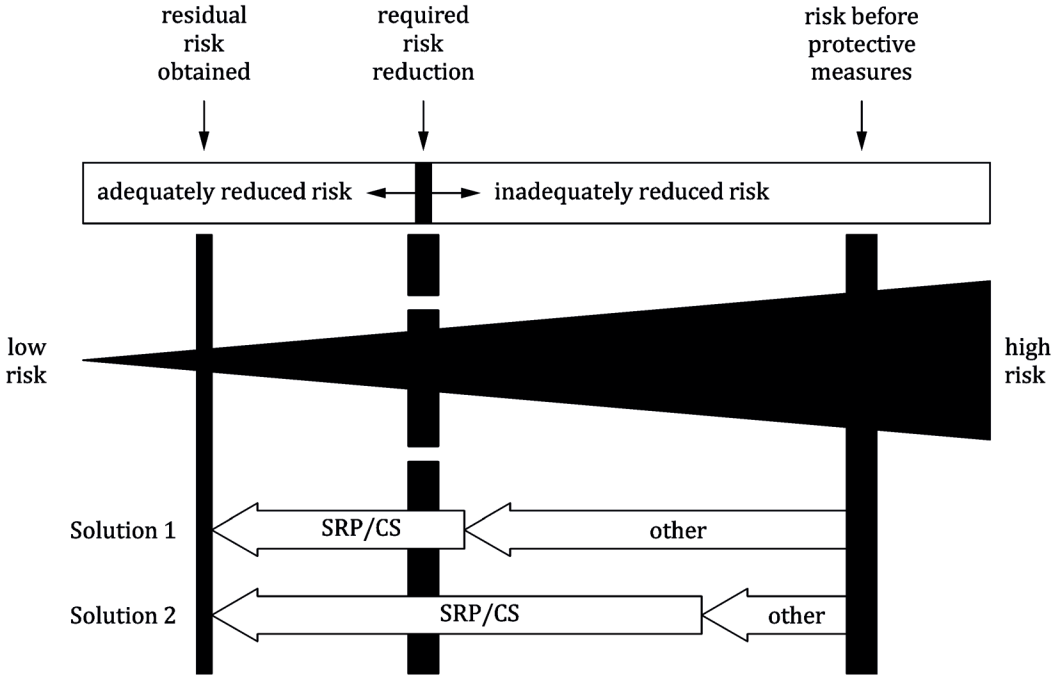
Figure 2 — Schematic representation of risk reduction process including iterative three-step method according to ISO 12100:2010

NOTE In special cases, this document applies also to step 3 of Figure 2. For examples see Annex M for indications and alarms.

4.2 Contribution to the risk reduction

From the risk assessment, the designer shall decide the contribution to the risk reduction provided by each relevant safety function carried out by the SRP/CS. This contribution covers the risk reduced by the application of each particular safety function (see Figure 3) that can be achieve by measures other than SRP/CS. It does not cover the overall risk of machinery under control.

EXAMPLE The stopping safety function on a press initiated by using an electro-sensitive protective device or the door-locking safety function of a washing machine, etc.



Key

Solution 1 important part of risk reduction due to protective measures other than SRP/CS (e.g. mechanical measures), small part of risk reduction due to SRP/CS (e.g. light curtain)

Solution 2 important part of risk reduction due to the SRP/CS, small part of risk reduction due to protective measures other than SRP/CS

NOTE See ISO 12100:2010 for further information on risk reduction.

Figure 3 — Overview of the risk reduction process for each hazardous situation

4.3 Design process of an SRP/CS

Figure 4 shows the design process of an SRP/CS and determining whether the SRP/CS achieves the intended risk reduction.

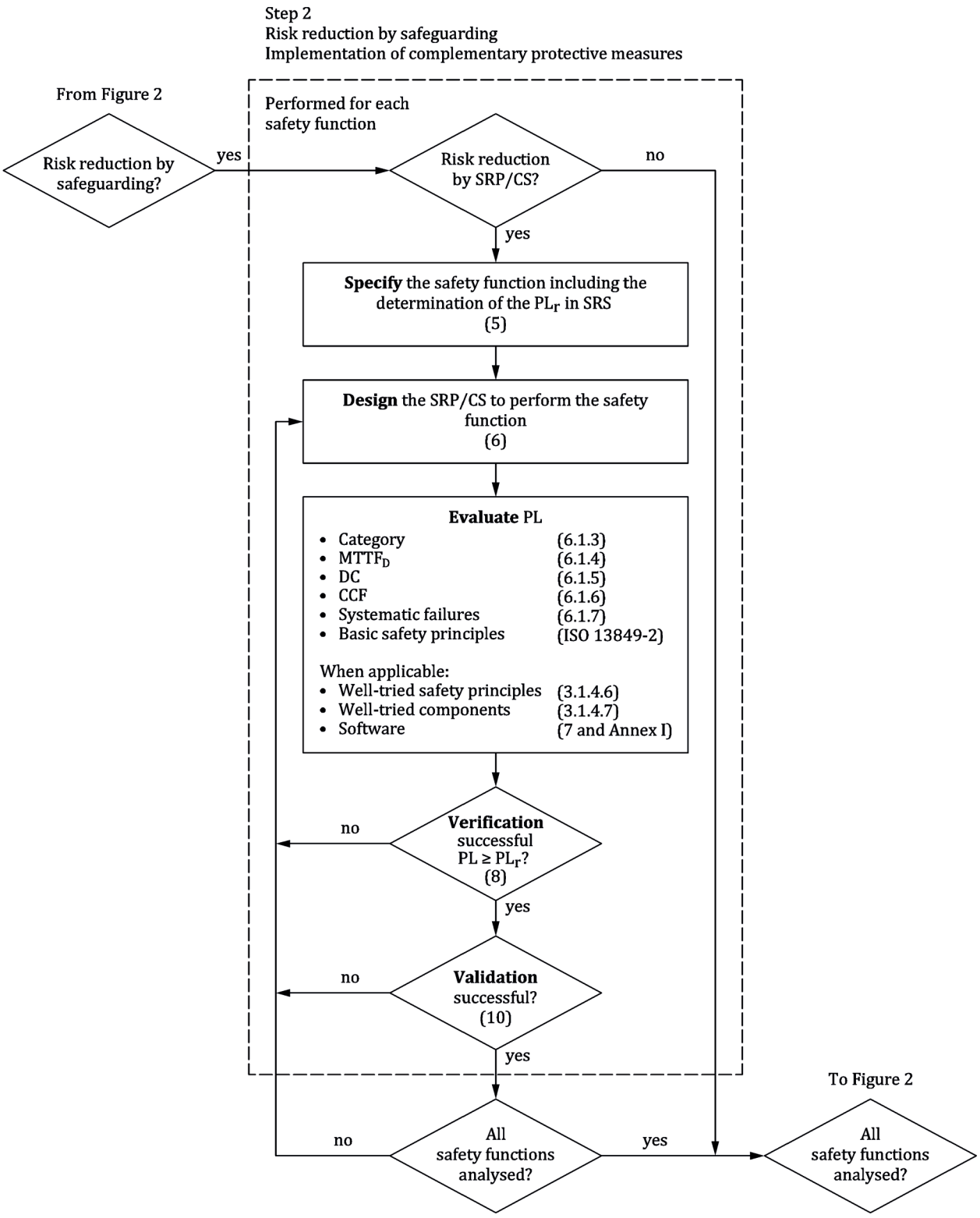


Figure 4 — Iterative process for design of safety-related parts of control systems

4.4 Methodology

This document uses the following methodology:

1) specification of safety functions (Clause 5)

2) design and technical realization of the safety functions including identification of the SRP/CSs and their subsystems which carry out each safety function;

   a) design considerations (Clause 6),

   b) software safety requirements (Clause 7);

3) verification that the achieved PL meets PL_r (Clause 8);

4) ergonomic aspects of the design (Clause 9);

5) validation (Clause 10 or ISO 13849-2);

6) maintenance (Clause 11);

7) technical documentation (Clause 12);

8) information for use (Clause 13).

The required performance level refers to the risk reduction to be provided by the safety function. The greater the contribution to the risk reduction needed, the higher the required safety performance shall be. The performance levels are defined in terms of average probability of dangerous failure of the safety function per hour. There are five performance levels, from providing a low contribution to risk reduction for PL a, to a high contribution to the risk reduction for PL e. The defined ranges of probability of a dangerous failure per hour are in Table 2.

Table 2 — Performance levels

PL	**Average probability of dangerous failure per hour** (PFH_D) 1/h
a	$10^{-5} \leq PFH_D < 10^{-4}$
b	$3 \times 10^{-6} \leq PFH_D < 10^{-5}$
c	$10^{-6} \leq PFH_D < 3 \times 10^{-6}$
d	$10^{-7} \leq PFH_D < 10^{-6}$
e	$PFH_D < 10^{-7}$

NOTE 1 The PFH_D value is considered to be identical to the PFH according to IEC 61508.

Subsystems (see 5.5) shall be evaluated using the same process as is used for SRP/CS systems, according to Clauses 5 through 13.For each safety function, the achieved performance level shall meet or exceed the required performance level (PL_r).

4.5 Required information

To fulfil the requirements of this document, the following information is necessary:

— results of the risk assessment of the machine or part of it;

— information for all safety functions (see Clause 5) determined to be necessary for the risk reduction process for each hazard including:

   — detailed description of each safety function (see 5.2);

   — determination of the required performance level (PL_r) for each safety function (see 6.3).

NOTE This information is already be given in applicable Type-C standards.

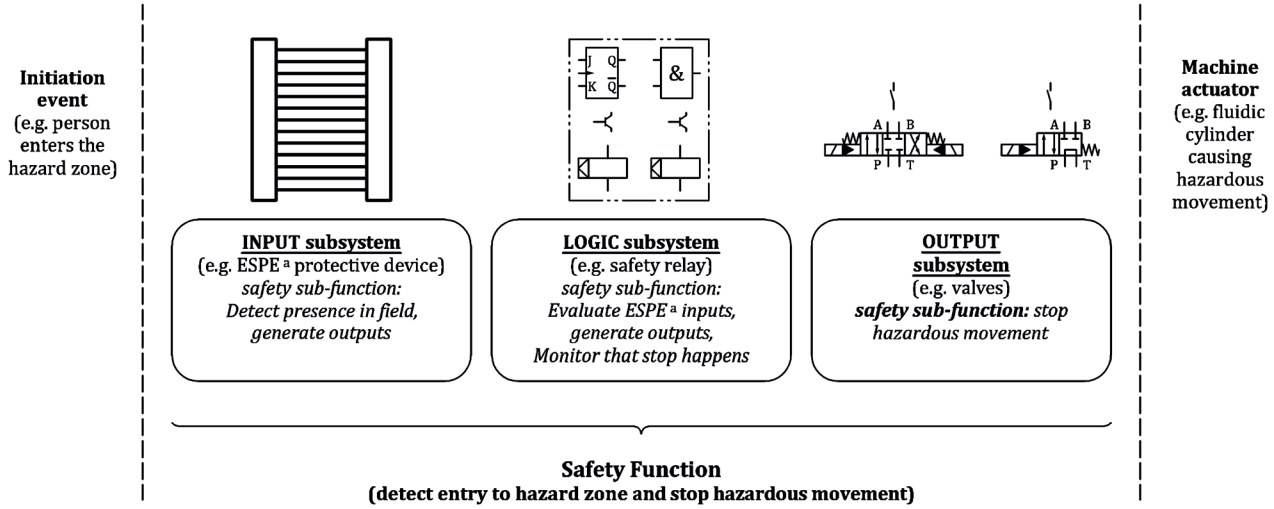
4.6 Safety function realization by using subsystems

The realisation of a safety function may be done by:

— using previously validated subsystems according to this document, IEC 62061, IEC 61508 or other relevant safety-related product standards (e.g. IEC 61496-1 and IEC 61800-5-2),

— designing new subsystems according to this document, or

— a combination of both alternatives above (see example in Figure 5).



[a] Electrosensitive protective equipment (ESPE).

Figure 5 — Example of combination of subsystems

5 Specification of safety functions

5.1 Identification and general description of the safety function

The objective of this subclause is to provide guidance on how to specify the requirements of each safety function to be implemented by the SRP/CS.

Part of the risk reduction process is to determine the safety functions of the machine e.g. prevention of unexpected start-up. A safety function may be implemented by one or more subsystems combined as an SRP/CS, and several safety functions may share one or more subsystems [e.g. a logic unit, power control element(s)].

Specification of the safety function can take place as described in ISO 12100, 6.2.11 and afterwards as a part of the design specification for the SRP/CS under this document.

Clause 5 addresses the following steps:

1) General description of the safety function (linking hazards to safety functions)

2) Detailed description of the safety requirements (see 5.2);

3) Determination of the PL_r for each safety function how reliable the safety function needs to be – see 5.3;

4) Review of the safety requirements specification (see 5.4).

A safety function shall have a general description to define how the SRP/CS contributes to risk reduction. The description shall be linked to hazards identified in the risk assessment and shall state how the function operates to achieve the required safety. The process for specifying safety functions requires detailed information from the risk assessment performed in accordance with ISO 12100:2010.

5.2 Safety requirements specification

5.2.1 General requirements

5.2.1.1 General

The safety requirements specification shall document details of each safety function to be performed.

The safety requirements specification is intended to prevent mistakes at the transition from the risk assessment and risk reduction process according to ISO 12100:2010 to the SRP/CS design and evaluation process according to this document, especially if these two processes are performed by different persons or organizations (see Table 3).

Table 3 — Transition from the risk assessment and risk reduction process according to ISO 12100 to the SRP/CS design and evaluation process according to ISO 13849-1

Necessary information to produce the SRS (see 5.2.1.2)	Transformation	Examples of specifications of safety functions in the SRS (see 5.2.1.3)
— results of risk assessment of the machine or part of it, including hazardous parts — machine operating characteristics, e.g. intended use — emergency operation — description of the interaction of different working processes and manual activities, e.g. repairing — ergonomic aspects — limits of use in relation to environmental conditions	⇨	required safety functions (examples): 1) interlocking function — operating mode (all) — triggering event: opening of a movable guard — safety-related reaction: safe torque off (STO) of all movements — PL_r d — response time — etc. 2) safely limited speed (SLS) — operating mode (manual) — triggering event: Speed is higher than the specified limit — safety-related reaction: safe torque off (STO) of all movements — PL_r c — response time — etc.

5.2.1.2 Necessary information to produce the safety requirements specification

NOTE The following information is used for technical documentation. For information for users see 13.3.

The following information shall be available to the designer of the safety-related control system to develop the safety requirements specifications where relevant:

a) Results of the risk assessment of the machine or part of it for each specific hazard where the associated risk reduction measure(s) rely on a safety-related control system to perform a safety function;

b) machine operating characteristics, including:

   1) intended use of the machine

   2) reasonably foreseeable misuse,

   3) effect of overlapping hazards

   4) operating modes (e.g. local mode, automatic mode, modes related to a zone or part of the machine),

   5) the mode(s) of operation during which the safety function is to be active

   6) cycle time, and

7) response time until a safe state is achieved (see also ISO 13855:2010, 5.1);

NOTE 1 The response time of the control system is part of the overall response time of the machine. The required overall response time of the machine can influence the design of the safety-related part, e.g. the need to provide a braking system.

NOTE 2 Operational functions (e.g. starting, normal stopping) can also be safety functions, but this can be ascertained only after a complete risk assessment on the machinery has been carried out.

c) emergency operation (IEC 60204-1:2016, Annex E);

d) description of the interaction of different working processes and manual activities (e.g. repairing, setting, cleaning, trouble shooting, modes of operation with the safeguards suspended);

e) ergonomic aspects to minimize incorrect operation or defeating;

f) limits of use in relation to environmental conditions;

g) effect of overlapping hazards (see Annex A.3).

5.2.1.3 Specification of all safety functions in the safety requirements specification

The SRS shall have the following information for each safety function in relation to the specific application:

a) the brief description / title of the safety function to have a clear reference;

b) the event that triggers the safety function;

c) the reaction to be initiated by the safety function output(s) to reach the intended safe state;

EXAMPLE 1 Stop hazardous movements.

d) the required performance level PL_r for each safety function (see 5.3);

e) the response time for the machine to achieve a safe state after the demand is made upon the safety function e.g., the overall system stopping performance (reaction time plus stopping time) according to ISO 13855:2010;

f) the operating mode(s) during which the safety function is to be active;

g) interfaces of the safety functions;

h) if needed, in case of a fault detection in a functional channel, procedures to bring the machine to a safe state including how the safe state is maintained until the fault is repaired;

EXAMPLE 2 If there is a fault in a functional channel and a stop category 1 is not possible, then a fault reaction can be initiated by using stop category 0. For stop categories, see IEC 60204-1.

i) the behaviour of the machine on the loss of power (see 5.2.3.7);

NOTE It can be necessary to hold a vertical axis in position to prevent a fall due to gravity forces. Where external forces can have an impact on functional safety, for instance on those gravity loaded axes, a reinforcement (e.g. for power elements) can be necessary because of systematic requirements. An appropriate design solution can be the integration of a non-return valve on cylinders or supplementary mechanical brakes. This can also require the design of two separate safety functions: One with power available and another without power available.

j) the demand rate of the safety function and/or the frequency of operation of the SRP/CS;

k) the priority of the safety functions that can be simultaneously active and that can cause conflicting action;

EXAMPLE 3 An emergency stop function has priority over all other functions.

EXAMPLE 4 The safely limited speed (SLS) function can be a precondition of a "hold to run" safety function.

l) safety-requirements of type C standards for the design of an SRP/CS or subsystem (e.g. ISO 23125:2015, ISO 16090-1:2017).

The above is a non-exhaustive list of details for safety functions that can be provided by the SRP/CS.

See also Annex M for typical safety functions and their characteristics and safety-related parameters.

5.2.2 Requirements for specific safety functions

5.2.2.1 Safety-related stop function

A safety-related stop function (e.g. initiated by a safeguard) shall as soon as necessary after actuation, put the machine in a safe state. Such a safety-related stop-function shall have priority over all relevant starts and non-safety-related stops. When a group of machines is working together in a coordinated manner, provision shall be made for signalling the supervisory control and/or the other machines that such a stop condition exists.

As a result of the risk assessment, safety-related stop functions can be realised according to the stop categories in IEC 60204-1:2016, 9.2.2.

NOTE IEC 61800-5-2:2016 provides information about safety-related power drive system including descriptions of safe-torque off (STO), safe stop 1 (SS1), safe stop 2 (SS2), safe operating stop (SOS).

After a stop command has been initiated by a safety function, the stop condition shall be maintained until safe conditions for restarting exist. See also Table M.1 in Annex M.

5.2.2.2 Manual reset function

The re-establishment of the safety function by resetting of the safeguard cancels the stop command. If indicated by the risk assessment, this cancellation of the stop command shall be confirmed by a manual, separate and intended action (manual reset).

The manual reset function shall:

— be provided through a separate and manually operated device that is separate from start command,

— only be achieved if all affected safety functions and safeguards are operational,

— not initiate a hazardous situation by itself,

— be initiated by intended action,

— enable the control system to accept a separate start command, and

— be accepted by monitored signal change, in order to avoid foreseeable misuse.

When the function “manual reset” is required to be a safety function (e.g., prevention of unexpected start), the required performance level shall be determined. The PL of the manual reset function can be different from the PL_r of the associated safety function.

NOTE It is not always necessary that the manual reset function has the same PL_r as the associated safety function.

The reset actuator shall be located outside the hazard zone and in a position from which there is sufficient visibility to ensure that no person is inside the hazard zone. It shall not be possible to activate the reset function from inside the hazard zone.

Where the visibility of the hazard zone is not sufficient, specific reset sequence or monitoring of the area that is not visible, shall be provided.

EXAMPLE One solution is the use of a sequenced resetting. The reset function is initiated within the hazard zone by the first actuator in combination with a second reset actuator located outside the hazard zone (near the safeguard). This reset procedure can be realized within a limited time before the control system accepts a separate start command. Monitoring of the area can be done by e.g. use of presence sensing devices that detect persons in hazard zones not visible from the reset position.

See also Table M.1.

5.2.2.3 Restart function

A restart shall take place automatically only if the safe condition is guaranteed. In particular, for interlocking guards with a start function, ISO 12100:2010, 6.3.3.2.5 applies.

EXAMPLE In automatic machine operations, sensor feedback signals to the control system are often used to control the process flow. If a work piece has come out of position, the process flow is stopped. If the monitoring of the interlocked safeguard does not have a higher priority to the automatic process control, there could be a danger of unexpected restarting of the machine while the operator readjusts the workpiece. Therefore, the automatic restart ought not to be allowed until the safeguard is closed again and the operator has left the hazard zone. The contribution of the prevention of unexpected start-up (see ISO 14118:2017) provided by the control system is dependent on the result of the risk assessment.

See also Table M.1.

5.2.2.4 Local control function

When a machine is controlled locally, e.g. by a portable control station that can be a portable device or pendant, the following requirements shall apply:

— the means for granting local control shall be situated outside the hazard zone;

— it shall only be possible to initiate command by a local control station in a zone defined by the risk assessment in order to avoid hazardous situations;

— switching between local and a different another control shall not create a hazardous situation;

— initiation of commands from multiple control stations (local or remote) shall not lead to a hazardous situation. It can be necessary to preclude use of other control stations when a local control station is selected or when certain commands are initiated.

See also Table M.1.

5.2.2.5 Muting function

Muting is a temporary automatic suspension of a safety function by the machine safety-related control system. It can be used to allow access by persons or by materials:

— during a non-hazardous portion of the machine cycle, or

— when safety is maintained by other means.

The muting function shall be initiated and terminated automatically. This shall be achieved by the use of appropriately selected and placed sensors or by signals from the machine control system. Incorrect signals, sequence, or timing of the muting sensors or signals shall not allow a mute condition.

The part or parts of the control system that performs the muting function shall have an appropriate safety-related performance (SIL according to IEC 62061 or PL according to this document) and shall not reduce the safety-related performance of the protective function below that required for the application.

At the end of muting, all affected safety functions shall be reinstated and active.

The implementation of muting shall meet the requirements of IEC 62046:2018. See also Table M.1.

5.2.2.6 Safety-related parameters

When safety-related parameters, e.g. position, speed, temperature, time, torque or pressure, deviate from present limits the safety-related control system shall initiate appropriate measures.

If errors in manual inputting of safety-related data in programmable or configurable electronic systems can lead to a hazardous situation, then a data checking system within the safety-related control system should be provided, e.g. check of limits, format and/or logic input values. For additional requirements, see 7.5 and see also Table M.2.

Annex O provides information on safety-related values of components or parts of control systems.

5.2.2.7 Fluctuations, loss and restoration of power sources

When fluctuations in energy levels outside the design operating range occur, including loss of energy supply, the SRP/CS shall continue to provide or initiate output signal(s) which will enable other parts of the machine system to maintain a safe state. See also Table M.2.

5.2.2.8 Requirements for operating mode selection

Selection of operating mode is a safety function when the selection enables or disables safety function(s). The following is required:

a) only one operating mode shall be active at a time; each selected operating mode shall be clearly identifiable or indicated;

   NOTE It is sufficient that a mode can be identified or indicated in the overall safety function.

b) mode selection by itself shall not initiate machine operation. A separate actuation of the start control shall be required.

c) when changing from one operating mode to another, safety functions and/or risk reduction measures necessary for the selected operating mode shall be activated without any loss of the intended risk reduction during the transition.

The operating mode selection function shall be implemented as a safety function, if it is required by the risk assessment, by considering the systematic requirements a) to c). The means of selecting the operating mode shall not degrade the PL of the safety functions active in that mode.

5.2.2.9 Safety function(s) for maintenance tasks

The design of the machine shall take into account maintenance tasks on the machine and provide safety functions for these tasks. The results of the risk assessment for each relevant safety function shall be considered in the specification of the SRP/CS.

NOTE 1 Maintenance tasks can include, but are not limited to:

— setting;

— teaching/programming;

— process/tool changeover;

— cleaning and housekeeping;

— sanitizing;

— planned or unplanned preventive or corrective maintenance;

— troubleshooting/fault finding;

— fault diagnosis..

Some maintenance task require a full isolation of the machine from all power sources and therefore do not rely on the SRP/CS. For maintenance tasks that require power and/or machine movements while maintenance personnel are inside the hazard zone, and where manual suspension or override of specific safety functions is needed it shall only be allowed by providing alternative and appropriate safety functions (e.g. enabling device safety function with a speed limiting safety function).

EXAMPLE Teaching/ programming, troubleshooting, process fine-tuning are tasks requiring power and machine movement.

The following safety functions are examples of what is often provided for maintenance tasks:

a) hold-to-run;

b) enabling control;

c) monitoring or limiting of speed, torque, power, position, location, temperature, level, etc.;

d) prevention of unexpected start-up;

e) isolation and energy dissipation;

f) mechanical restraint or containment.

NOTE 2 See Annex M for additional information.

The motivation to defeat or circumvent risk reduction measures provided by the SRP/CS during maintenance of the machine shall be considered when specifying, designing and selecting the SRP/CS (see 5.2.2.10).

The SRP/CS shall include consideration that additional personnel other than the intended operator(s) perform a task, e.g.:

— an operator performs reset and restart functions while maintenance personnel are inside the hazard zone;

— risk reduction measures intended to protect an individual are inappropriately used for multiple personnel;

In maintenance mode, the design of the SRP/CS shall prevent a remote access (see 5.2.2.11) to the machine control system without appropriate notification or indication to persons that are at or near the machine.

5.2.2.10 Motivation to defeat safety functions

The motivation to defeat or circumvent a safety function depends on the process, the intended use of the machine (or part of the machine) and the design details of the risk reduction measure(s). The motivation to defeat a safety function shall be minimized in the design of the SRP/CS.

NOTE 1 Providing means to perform tasks easily whilst protecting operators can lessen the motivation to defeat or circumvent safety function(s) and/or safeguard(s).

NOTE 2 ISO 14119 gives a method and shows examples how to minimize possibilities to defeat an interlocking device.

NOTE 3 Safety research has shown that many injuries occur due to defeat of safety function and/or safeguards. See Bibliography for more information.

EXAMPLE Motivations to defeat or circumvent a risk reduction measure (including safety function(s)) can be that:

— the risk reduction measure prevents the task from being performed; there is a need to perform a task that was not identified and assessed for hazards and risks;

— the risk reduction measure slows down production or interferes with any other activities or preferences of the user;

— the risk reduction measure is difficult to use;

— the risk reduction measure and/or its associated hazard is not recognized as such by personnel;

— the risk reduction measure is not accepted as suitable, necessary or appropriate for its function.

The use and access to programmable systems introduces an additional possibility to defeat or circumvent safety functions if not properly applied or supervised.

5.2.2.11 Remote access

When a machine is capable of remote access, the SRP/CS shall remain operational. Alternative risk reduction measures can be used when provided in the information of use.

The design of the SRP/CS shall not allow remote access of a machine without specific measures to prevent dangerous situations that can arise due to the presence of persons being inside or near to the machine.

NOTE A remote start that is unexpected to persons working at the machine can lead to injury.

5.3 Determination of required performance level for each safety function

For each selected safety function a required performance level (PL_r) shall be determined and documented. The determination of the PL_r shall be based on the result of the risk assessment of the machine or part of it and shall correlate to the needed risk reduction (see Figure 3). Annex A provides guidance for the determination of the PL_r for the safety function. Overlapping hazards if relevant also need to be considered when defining the safety functions. See A.3 for further guidance.

NOTE 1 Other methods like the method presented in IEC 62061 can be used instead.

NOTE 2 Type-C standard typically provide information on PL_r.

As the methodology for determining the required performance level includes subjective estimations, some variability is acceptable in the practical application of particular cases. This variability shall be taken into account when defining PL_r.

NOTE 3 The PL_r for a safety function determines the reliability of the control system to execute the safety function and to achieve the intended risk reduction. The PL_r is determined using several factors of risk. See also Annex A.

5.4 Review of the safety requirements specification

The safety requirements specification shall be verified against the risk assessment before starting the design, since every other activity is based on these requirements. The review shall ensure that all safety functions are specified to achieve the intended risk reduction at the machine. See also 10.4 for the validation of the SRS.

NOTE Depending on the specific safety functions it can be useful to have independence between who prepares the SRS and who reviews it.

5.5 Decomposition of SRP/CS into subsystems

The safety functions shall be decomposed into sub-functions that are allocated to subsystems. The description of each sub-function shall include

— the safety requirements for the sub-function (functional and integrity), and

— inputs and outputs of each sub-function.

An SRP/CS can comprise:

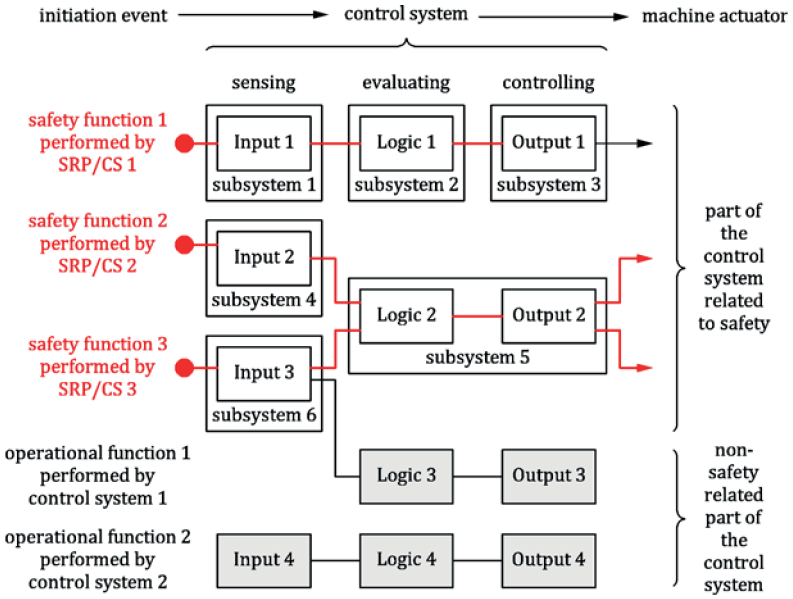
— one or several previously validated subsystem(s);

— one or several subsystem(s) based on subsystem element(s);

— a combination of both alternatives above.

By definition, a dangerous failure of any subsystem results in the loss of the whole safety function.

EXAMPLE Figure 6 provides an example of decomposition starting with a detection and evaluation of an 'initiating event' (e.g. manual actuation of a push button, opening of guard, interruption of beam of AOPD) and is ending with an output causing a safe reaction of a 'machine actuator' (e.g. motor, cylinder).



NOTE 1 Safety function 1 is decomposed into sub-function 1, sub-function 2 and sub-function 3. Sub-function 1 is performed by subsystem 1.

NOTE 2 Safety function 2 is decomposed into sub-function 4 and sub-function 5. Sub-function 4 is performed by subsystem 4.

NOTE 3 Safety function 3 is decomposed into sub-function 6 and sub-function 5. Sub-function 6 is performed by subsystem 6.

Figure 6 — Example of decomposition of safety functions and their allocation to subsystems

Figure 6 shows a diagrammatic presentation of subsystems combined as SRP/CS(s) for:

— initiation event (e.g. opening of a guard, interruption of beam of AOPD);

— input (e.g. limit switch, sensor, AOPD) (subsystems 1, 4 and 6),

— logic/processing (subsystems 2 and 5),

— output/power control elements (e.g. valve, contactor, current converter, brakes) (subsystems 3 and 5),

— machine actuator (e. g. motor, cylinder),

— interconnecting means (e.g. electrical, optical).

NOTE 1 The decomposition of an SRP/CS into subsystems represented in Figure 6 is typical but the whole SRP/CS may be also realized by a single subsystem or more than three subsystems.

NOTE 2 An SRP/CS can be implemented by one single subsystem having a sensor, logic and power control elements. Example for an SRP/CS implementation with a single subsystem is an "Intelligent" sensor unit (e.g. light curtain, laser scanner) with integrated output switching device (e.g. relay to switch-off a dangerous movement).

NOTE 3 It is also possible that one subsystem or SRP/CS implements safety functions and standard control functions. The designer can use any of the technologies available, singly or in combination. SRP/CS can also provide an operational function (e.g. an AOPD as a means of cycle initiation).

NOTE 4 The designer of a previously validated subsystem can be a system integrator, machine manufacturer or a component manufacturer.

The manufacturer of a previously validated subsystem shall provide the relevant information according to 13.2.

6 Design considerations

6.1 Evaluation of the achieved performance level

6.1.1 General overview of performance level

The ability to perform a safety function is determined by the evaluation of the performance level.

A performance level shall be determined for each subsystem and/or each combination of subsystems that provide a safety function. The PL of the subsystem shall be determined by the estimation of the following aspects:

1) the architecture (see 6.1.3);
   a) assign a category to the subsystem and evaluate the result;
   b) evaluate if the applicable qualitative (non-quantifiable) requirements of the category are met, including:
      — basic safety principles (see ISO 13849-2:2012, Tables A.1, Table B.1, Table C.1 and Table D.1);
      — well-tried safety principles (see ISO 13849-2:2012, Table A.2, B.2, C.2 and D.2);
      — well-tried components (see ISO 13849-2:2012, Table A.3 and Table D.3, Annex B and Annex C);
   c) evaluate that required behaviour under fault condition(s) is met;
2) the $MTTF_D$ value for single components (see 6.1.4, Annex C and Annex D);
3) the DC (see 6.1.5 and Annex E);
4) the CCF (see 6.1.6 and Annex F);
5) the effect of the safety-related software design on the operation of the hardware (see Clause 7 and Annex J);
6) the effect of measures against systematic failures (see 6.1.7 and Annex G);

NOTE 1 Other parameters, e.g. operational aspects, demand rate, test rate, can have certain influence.

These aspects can be grouped under two approaches in relation to the evaluation process:

a) quantifiable aspects ($MTTF_D$ value for single components, DC, CCF, architecture);

b) non-quantifiable, qualitative aspects which affect the behaviour of the subsystem (behaviour of the safety function under fault conditions, safety-related software, systematic failure, the application of basic and well-tried safety principles, the use of well-tried components, environmental conditions and fault exclusion).

NOTE 2 The contribution of reliability (e.g. $MTTF_{D,}$ architecture) can vary with the safety-related parts used.

NOTE 3 There are several methods for estimating the quantifiable aspects of the PL for any type of system (e.g. a complex structure), for example, Markov modelling, generalized stochastic petri nets (GSPN), reliability block diagrams (see, e.g. IEC 61508, IEC 61078, IEC 62021).

To make the assessment of the PL easier, this document provides a simplified method based on the definition of five designated architectures that fulfil specific design criteria and behaviour under a fault condition (see 6.1.3).

For PL evaluation of a subsystem the requirements are given in 6.1. A simplified approach for the PL evaluation of a subsystem is given in 6.1.8 (Figure 12), 6.1.9, using the procedure given in Annex B to Annex H, Annex J, Annex K and Annex L.

For PL evaluation of subsystem combinations see 6.2.

Qualitative aspects of the PL and the avoidance of systematic failures shall be achieved by fulfilling the requirements and guidance of this document, including Annex G.

Where product-specific standards such as the IEC 61496 series for electro-sensitive protective equipment (ESPE) or ISO 13856 for pressure-sensitive protective equipment specify requirements to avoid or control systematic or random failures, such subsystems shall meet the requirements of these product standards in addition to the requirements specified in this document.

Risk reduction measures shall be applied and the following shall be fulfilled:

— Reduce the probability of faults at the component level which affect the safety function. This can be done by increasing the reliability of components, e.g. by selection of well-tried components and/or applying well-tried safety principles, in order to minimize or exclude critical faults or failures (see ISO 13849-2:2012).

— Improve the structure of the subsystem to avoid the dangerous effect of a fault. Some faults could require detection, thereby necessitating a redundant and/or monitored structure.

Reducing the probability of faults and avoiding dangerous effects of faults can be applied separately or in combination. Depending on the technologies, this can be achieved by

— selecting reliable components and by fault exclusions; or

— the safety function having a redundant and/or monitored architecture system.

The structure including fault tolerance and fault detection are important parameters to determine the PL. Architectural constraints limit the maximum achievable PL of category B, 1 and 2. For these architectural constraints, see 6.1.3.2.2 to 6.1.3.2.4.

Common cause failures (CCF) requirements shall be fulfilled.

For subsystems that have PL or SIL and PFH_D-values from the manufacturer, further estimation (e.g. DC, MTTF, CCF, SRESW evaluation) is unnecessary.

6.1.2 Correlation between performance level and safety integrity level

When a safety function is designed using one or more subsystem, each subsystem shall be designed either using PLs according to this document, or using SILs according to IEC 62061 and IEC 61508. Subsystems designed according to IEC 61508 or IEC 62061 may be used but shall be restricted to those designed for high demand or continuous mode that use Route 1_H (see IEC 61508-2:2010, 7.4.4.2). Subsystems are to be combined according to 6.2. See Table 4 for correlations between PLs and SILs.

Table 4 — Correlation between performance level and safety integrity level

PL	SIL (see IEC 62061 for information) high/continuous operating mode
a	no correlation
b	1
c	1
d	2
e	3

NOTE 1 PL a has no correlation on the SIL scale and is mainly used to reduce the risk of slight, normally reversible, injury.

NOTE 2 PL e corresponds to SIL 3 which is defined as the highest level typically used for machinery.

6.1.3 Architecture — Categories and their relation to $MTTF_D$ of each channel, average diagnostic coverage and common cause failure

6.1.3.1 General

Subsystems designed according to this document shall be in accordance with the requirements of one of the categories specified in 6.1.3.2. The categories are fundamental to achieving a specific PL. They describe the required behaviour of the subsystem in respect of its resistance to faults based on the design considerations described in Clause 4.

Category B is the basic category. The occurrence of a fault can lead to the loss of the safety function. In category 1 improved resistance to faults is achieved predominantly by using high quality components. In categories 2, 3 and 4, improved performance is achieved predominantly by improving fault tolerance and/or diagnostic measures. In category 2 this is provided by periodically checking that the specified sub-function is being performed correctly (without faults). In categories 3 and 4 this is provided by ensuring that the single fault does not lead to the loss of the sub-function. In category 4, and whenever reasonably practicable in category 3, such faults are detected. Category 4 is resistant to the accumulation of faults. Table 5 gives an overview of categories of the subsystem, the requirements and the sub-function behaviour in case of faults.

Table 5 — Overview of requirements for categories

Category	Summary of requirements for subsystems	Sub-function behaviour	Principle used to achieve safety	$MTTF_D$ of each functional channel	DC_{avg}	CCF
B (see 6.1.3.2.2)	Subsystems and/or their protective equipment, as well as their components, shall be designed, constructed, selected, assembled and combined in accordance with relevant standards so that they can withstand the expected influences. Basic safety principles shall be used.	The occurrence of a fault can lead to the loss of the sub- function.	mainly characterized by selection of components	low to medium	none	not relevant
NOTE For full requirements, see 6.1.3.2.						

Table 5 *(continued)*

Category	Summary of requirements for subsystems	Sub-function behaviour	Principle used to achieve safety	$MTTF_D$ of each function-nal channel	DC_{avg}	CCF
1 (see 6.1.3.2.3)	Requirements of B shall apply. Well-tried components and well-tried safety principles shall be used.	The occurrence of a fault can lead to the loss of the sub-function but the probability of occurrence is lower than for category B.	mainly characterized by selection of components	high	none	not relevant
2 (see 6.1.3.2.4)	Requirements of B and the use of well-tried safety principles shall apply. Subsystems shall be checked at suitable intervals.	The occurrence of a fault can lead to the loss of the sub- function between the checks. The loss of sub-function is detected by the check.	mainly characterized by structure	low to high	low to medium	see Annex F
3 (see 6.1.3.2.5)	Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed, so that — a single fault in any of these parts does not lead to the loss of the sub- function, and — whenever reasonably practicable, the single fault is detected.	When a single fault occurs, the sub-function is always performed. Some, but not all, faults will be detected. Accumulation of undetected faults can lead to the loss of the sub-function.	mainly characterized by structure	low to high	low to medium	see Annex F
4 (see 6.1.3.2.6)	Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed, so that — a single fault in any of these parts does not lead to a loss of the sub-function, and — the single fault is detected at or before the next demand upon the sub-function, but that if this detection is not possible, an accumulation of undetected faults shall not lead to the loss of the sub-function.	When a single fault occurs the sub-function is always performed. Detection of accumulated faults reduces the probability of the loss of the sub- function (high DC). The faults will be detected in time to prevent the loss of the sub-function.	mainly characterized by structure	high	high including accumulation of faults	see Annex F
NOTE For full requirements, see 6.1.3.2.						

When considering the causes of failures in some components it is possible to exclude certain faults (see 6.1.10.3).

The selection of a category for a particular subsystem depends mainly upon

a) the reduction in risk to be achieved by the safety function to which the subsystem contributes,

b) the required performance level,

c) the technologies used,

d) the consequences arising in the case of a fault(s) in an element of the subsystem,

e) the possibilities of avoiding a fault(s) in that subsystem (systematic failure),

f) the mean time to dangerous failure,

g) the diagnostic coverage, and

h) the common cause failure in the case of categories 2, 3 and 4.

6.1.3.2 Designated architectures — Specification of categories

6.1.3.2.1 General

The following designated architectures meet the requirements of the respective category.

The designated architectures show a logical representation of the structure of the subsystems for each category.

NOTE 1 For categories 3 and 4, this means that not all parts are necessarily physically redundant but that there are redundant means of assuring that a single fault cannot lead to the loss of the sub-function. Therefore, the technical realization (for example, the circuit diagram) can differ from the logical representation of the architecture.

Figure 7 to Figure 11 do not show examples but general architectures. A deviation from these architectures is always possible, but any deviation shall be justified, by means of appropriate analytical tools (e.g. Markov modelling, fault tree analysis), such that the subsystem meets the required performance level. For a subsystem that deviates from the designated architectures, a detailed calculation shall be provided to demonstrate the achievement of the required performance level.

The lines and arrows in Figure 7 to Figure 11 represent logical interconnecting means and, where applicable, diagnostic means.

NOTE 2 The structure of a subsystem is a key characteristic having great influence on the PL. Even if the variety of possible structures is high, the basic concepts are often similar. Thus, most structures that are present in the machinery field can be mapped to one of the categories. For each category, a typical representation as a safety-related block diagram can be made. These typical realizations are called designated architectures and are listed in the context of each of the following categories.

If the simplified procedure of 6.1.8 is used to estimate the PL, the architecture of the subsystem shall be equivalent to the designated architecture of the claimed category. Designs fulfilling the characteristics of the respective category in general are equivalent to the respective designated architecture of the category.

6.1.3.2.2 Category B

Subsystem of category B shall, as a minimum, be designed, constructed, selected, assembled and combined in accordance with the relevant standards and use basic safety principles (see ISO 13849-2:2012) for the specific application to withstand

— the expected operating stresses, e.g. the reliability with respect to breaking capacity and frequency,

— the influence of the processed material, e.g. detergents in a washing machine, and

— other relevant external influences, e.g. mechanical vibration, electromagnetic interference, power supply interruptions or disturbances.

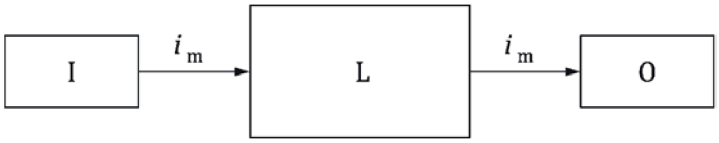
The $MTTF_D$ of the channel shall be at least low.

The maximum PL achievable with category B is PL b.

NOTE 1 There is no diagnostic coverage (DC_{avg} = none) within category B systems. In such structures, the consideration of CCF is not relevant.

NOTE 2 When a fault occurs it can lead to the loss of the sub-function.

Specific requirements for electromagnetic compatibility (EMC) (immunity requirements) are found in the relevant product or generic standards. Immunity requirements are particularly relevant for subsystems. Subsystems containing active electronic components shall meet EMC immunity requirements based on the environment as appropriate. For practical guidance see Annex L.



Key

i_m interconnecting means
I input device, e.g. sensor
L logic
O output device, e.g. main contactor

Figure 7 — Designated architecture for category B

6.1.3.2.3 Category 1

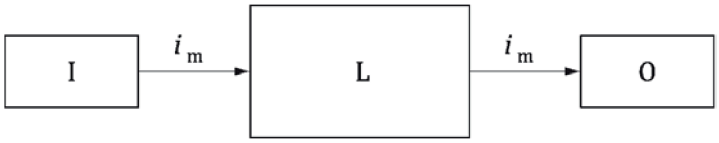
For category 1, the same requirements as those according to 6.1.3.2.2 for category B shall apply. In addition, the following applies.

Subsystems of category 1 shall be designed and constructed using well-tried components according to 6.1.11 and well-tried safety principles (see ISO 13849-2:2012).

NOTE 1 There is no diagnostic coverage (DCavg = none) within category 1 systems. In such structures (single-channel systems) the consideration of CCF is not relevant. The $MTTF_D$ of the channel shall be high.

The maximum PL achievable with category 1 is PL c.

NOTE 2 When a fault occurs it can lead to the loss of the safety function. However, the $MTTF_D$ of the single channel in category 1 is higher than in category B. Consequently, the loss of the safety function is less likely.



Key

i_m interconnecting means
I input device, e.g. sensor
L logic
O output device, e.g. main contactor

Figure 8 — Designated architecture for category 1

6.1.3.2.4 Category 2

For category 2, the same requirements as those according to 6.1.3.2.2 for category B shall apply. "Well–tried safety principles" according to 3.1.47 shall also be followed. In addition, the following applies.

Subsystems of category 2 shall be designed so that their functional channel (I, L, O) is tested at suitable intervals. The test of the sub-function(s) shall be performed before or at least at the demand of the safety function prior to any hazardous situation, e.g.

a) prior to the start of a new cycle and/or,

b) prior to the start of other movements and/or,

c) immediately upon demand of the safety function and/or,

d) periodically during operation if the risk assessment and the kind of operation shows that it is necessary.

The test itself shall not lead to a hazardous situation (e.g. due to an increase in response time). The test equipment may be integral with, or separate from, the safety-related part(s) providing the safety function.

Based on the risk assessment of the machine or part of it, the initiation of this test may be manual. Any test of the sub-function(s) shall either

— allow operation if no faults have been detected, or

— generate an output [output of the test equipment (OTE)] that initiates appropriate control action, if a fault is detected.

For PL_r d the output (OTE) shall initiate a safe state that is maintained until the fault is cleared.

For PL_r up to and including PL_r c, whenever practicable the output (OTE) shall initiate a safe state that is maintained until the fault is cleared. When this is not practicable (e.g. welding of the contact in the final switching device) it may be sufficient for the output of the test equipment OTE to provide a warning.

The calculation of DC_{avg} shall take into account only the blocks of the functional channel (i.e. I, L and O in Figure 9) and not the blocks of the testing channel.

For category 2, the following are required:

— demand rate ≤ 0,01 test rate (see Annex K, Table K.1, Note 1); or testing occurs immediately upon demand of the safety function and the overall time to detect the fault and to bring the machine to a non-hazardous condition (usually to stop the machine) is shorter than the time to reach the hazard (see also ISO 13855:2010).

— $MTTF_D$ of the testing channel (TE and OTE in Figure 9) is greater than one half of $MTTF_D$ of the functional channel (see Table K.1, Note 1).

The diagnostic coverage of all parts of the functional channel (I, L, O) shall be at least low. The $MTTF_D$ of the functional channel shall be low-to-high, depending on the required performance level. Measures against CCF of the functional channel and the test channel shall be applied (see 6.1.6 and Annex F).

The maximum PL achievable with category 2 is PL d.

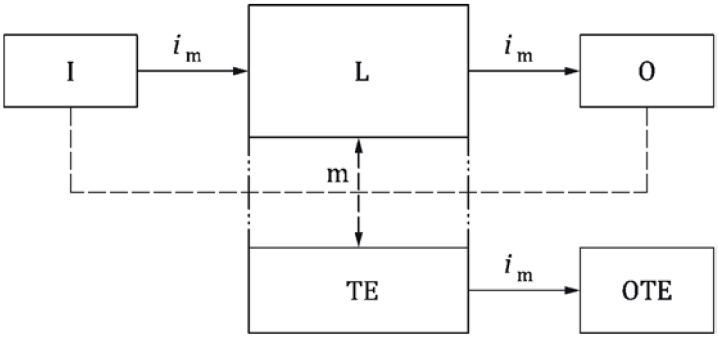
NOTE 1 The test of the blocks in the functional channel can be e.g. realized by direct or indirect monitoring.

NOTE 2 Category 2 system behaviour can be characterized by

— the occurrence of a fault can lead to the loss of the sub-function between tests,

— the loss of sub-function is detected by the tests.

NOTE 2 The principle that supports the validity of a category 2 function is that the adopted technical provisions, and, for example, the choice of test rate and reliability of the test equipment can decrease the probability of occurrence of a dangerous fault.



Key

i_m interconnecting means
I input device, e.g. sensor
L logic
m monitoring/testing
O output device, e.g. main contactor
TE test equipment
OTE output of TE

The dashed lines represent reasonably practicable fault detection.

Figure 9 — Designated architecture for category 2

6.1.3.2.5 Category 3

For category 3, the same requirements as those according to 6.1.3.2.2 for category B shall apply. Well-tried safety principles according to 3.1.47 shall also be followed. In addition, the following applies.

The maximum PL achievable with category 3 is PL d.

Subsystems of category 3 shall be designed so that a single fault does not lead to the loss of the sub-function. Whenever reasonably practicable, the single fault shall be detected at or before the next demand upon the safety function.

The diagnostic coverage of the total subsystem shall be at least low. The $MTTF_D$ of each of the redundant channels shall be low-to-high, depending on the PL_r. Measures against CCF shall be applied (see Annex F).

NOTE 1 The requirement of single-fault detection does not mean that all faults will be detected. Consequently, the accumulation of undetected faults can lead to an unintended output and a hazardous situation at the machine. Typical examples of practicable measures for fault detection are use of the feedback of mechanically guided relay contacts and monitoring of redundant electrical outputs (see Annex E).

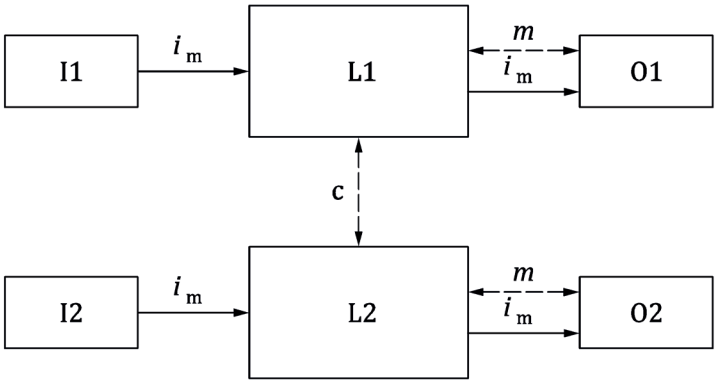
NOTE 2 If necessary because of technology and application, type-C standard makers can give further details on the detection of faults.

NOTE 3 Category 3 subsystem behaviour is characterized by

— continued performance of the sub-function in the presence of a single fault,

— detection of some, but not all, faults, and

— possible loss of the sub-function due to accumulation of undetected faults.



Key

i_m	interconnecting means	L1, L2	logic
c	cross monitoring	m	monitoring
I1, I2	input device, e. g. sensor	O1, O2	output device, e.g. main contactor or drive system

The dashed lines represent reasonably practicable fault detection.

Figure 10 — Designated architecture for category 3

6.1.3.2.6 Category 4

For category 4, the same requirements as those according to 7.1.3.2.2 for category B shall apply. Well-tried safety principles according to 3.1.47 shall also be followed. In addition, the following applies.

The maximum PL achievable with category 4 is PL e.

Subsystem of category 4 shall be designed such that

— a single fault does not lead to a loss of the safety function, and

— the single fault is detected at or before the next demand upon the safety functions, e.g. immediately, at switch on, or at the end of a machine operating cycle but if this detection is not possible, then an accumulation of undetected faults shall not lead to the loss of the safety function.

NOTE 1 Based on e.g. FMEA undetected failures with a very low probability do not need to be considered for accumulation of faults.

The diagnostic coverage (DC_{avg}) of the total subsystem shall be high. The $MTTF_D$ of each of the redundant channels shall be high. Measures against CCF shall be applied (see Annex F).

NOTE 2 Category 4 system behaviour is characterized by

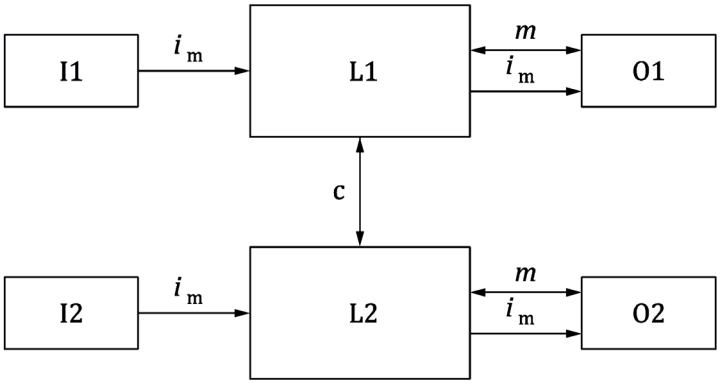
— continued performance of the safety function in the presence of a single fault,

— detection of faults in time to prevent the loss of the safety function,

— the accumulation of undetected faults is taken into account.

NOTE 3 The difference between category 3 and category 4 is a higher DC_{avg} in category 4 and a required $MTTF_D$ of each channel of "high" only.

In practice, the consideration of a fault combination of two faults may be sufficient.



Key

i_m	interconnecting means	L1, L2	logic
c	cross monitoring	m	monitoring
I1, I2	input device, e.g. sensor	O1, O2	output device, e.g. main contactor or drive system

Solid lines for monitoring (m) represent diagnostic coverage that is higher than in the designated architecture for category 3.

Figure 11 — Designated architecture for category 4

6.1.4 Mean time to dangerous failure

The mean time to dangerous failure ($MTTF_D$) is a quantity with the dimension of time to characterize the basic reliability of the components used. Given a constant dangerous failure rate, the $MTTF_D$ is the reciprocal of the dangerous failure rate, converted in years.

For the estimation of $MTTF_D$ of a component, the order of priorities is:

1) use manufacturer's data;

   NOTE 1 When using $MTTF_D$ data of electromechanical devices from a manufacturer, the assumed number of operations of the device is considered so that it matches the use in the application.

2) use methods in Annex C;

3) failure rate field data from identical component applications in similar environments collected over a significant period of time and where the collection and analysis method results in a reasonable level of confidence in the data;

   NOTE 2 Further information about field data is detailed in B.5.4 of IEC 61508-7:2010.

4) choose 10 years.

Annex C gives practical guidance how to calculate or evaluate $MTTF_D$ values for single components. Annex D describes how to derive the $MTTF_D$ of each channel from this, including parts-count method and symmetrisation.

For each subsystem according to Table 5, the maximum value of $MTTF_D$ for each channel is limited to 100 years. For category 4 subsystems the maximum value of $MTTF_D$ for each channel is limited to 2 500 years.

NOTE 3 This higher value is justified because in Category 4 the other quantifiable aspects, structure and DC, are at their maximum point and this allows the series combination of more than 3 subsystems with Category 4 and achieve PL e in accordance with 6.2.

The value of the $MTTF_D$ of each channel is given in three levels (see Table 6) and shall be taken into account for each channel (e.g. single channel, each channel of a redundant system) individually.

Table 6 — Mean time to dangerous failure of each channel

$MTTF_D$	
Denotation of each channel	**Range of each channel**
low	3 years ≤ $MTTF_D$ < 10 years
medium	10 years ≤ $MTTF_D$ < 30 years
high	30 years ≤ $MTTF_D$ ≤ 100 years[a]

NOTE 1 The choice of the $MTTF_D$ ranges of each channel is based on failure rates found in the field as state-of-the-art, forming a kind of logarithmic scale fitting to the logarithmic PL scale. An $MTTF_D$ value of each channel less than three years is not expected to be found for real subsystems since this would mean that after one year about 30 % of all systems on the market will fail and will need to be replaced. An $MTTF_D$ value of each channel greater than 100 years is not acceptable because subsystems for high risks should not depend on the reliability of the components alone. To reinforce the subsystems against systematic and random failure, additional means such as redundancy and testing are necessary. To be practicable, the number of ranges was restricted to three. The limitation of $MTTF_D$ of each channel to a maximum of 100 years refers to the single channel of the subsystem which carries out the safety function. Higher $MTTF_D$ values can be used for single components (see Table D.1).

NOTE 2 The indicated limit values of this table are assumed within an accuracy of 5 %.

[a] For Category 4 the $MTTF_D$ is limited to 2 500 years.

6.1.5 Diagnostic coverage

Diagnostic coverage (DC) is determined as the ratio between rate of detected dangerous failures and the rate of total dangerous failures. Diagnostic coverage shall be considered in categories 2, 3 and 4.

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

where

$\sum \lambda_{DD}$ is the sum of all failure rates of detected dangerous failures;

$\sum \lambda_{Dtotal}$ the sum of all failure rates of total dangerous failures.

Diagnostic coverage shall be based on either failure modes and effects analysis (FMEA, see IEC 60812:2018), or by using simplified estimation of DC based on Clause E.1 and Table E.1. E.2 describes how the average DC (DC_{avg}) can be estimated.

NOTE 1 For the estimation of DC, in most cases, failure mode and effects analysis (FMEA, see IEC 60812 and EN 50495, Annex B) or similar methods can be used to consider all relevant faults and/or failure modes. See also ISO 13849-2:2012, Annex E.5.3.

NOTE 2 Often logic units take care of diagnostic functions of input and output device.

NOTE 3 The technology used will influence the possibilities for the implementation of fault detection.

The value of the DC is given in four levels (see Table 7).

Table 7 — Diagnostic coverage

DC	
Denotation	**Range**
none	DC < 60 %
low	60 % ≤ DC < 90 %
medium	90 % ≤ DC < 99 %
high	99 % ≤ DC

NOTE 1 For subsystem consisting of several parts an average value DC_{avg} for DC is used in Figure 12, Clause 7 and E.2.

NOTE 2 The choice of the DC ranges is based on the key values 60 %, 90 % and 99 % also established in other standards dealing with diagnostic coverage of tests. Investigations show that (1 – DC) rather than DC itself is a characteristic measure for the effectiveness of the test. (1 – DC) for the key values 60 %, 90 % and 99 % forms a kind of logarithmic scale fitting to the logarithmic PL-scale. A DC-value less than 60 % has only slight effect on the reliability of the tested system and is therefore called "none". A DC-value greater than 99 % for complex systems is very hard to achieve. To be practicable, the number of ranges was restricted to four. The indicated limited values of this table are assumed within an accuracy of 5 %.

6.1.6 Common cause failures

The probability of two or more separate faults having a common cause shall be taken into account for subsystems of category 2, 3 and 4. In category 2 CCF refers to common cause failures in the functional channel and the test channel. In category 3 and 4 CCF refers to common cause failures in both functional channels. Sufficient measures against CCF shall be carried out (for guidance, see Annex F).

6.1.7 Systematic failures

Systematic failures occur for a variety of reasons, including e.g.

— wrong design specifications,

— manufacturing failures,

— environmental stress effects,

— operational failures,

— human errors in the safety requirements specification, design of hardware and software.

To establish a sufficient level of systematic integrity, the approach to design and implement safety functions shall be systematic.

Activities that are necessary for the achievement of the required functional safety of the SRP/CS shall be drawn up in a functional safety plan. The functional safety plan is intended to provide measures for preventing incorrect specification, implementation, or modification issues

In the design process especially, control and avoidance of systematic failures shall be implemented (see Clause 10 and Annex G).

6.1.8 Simplified procedure for estimating the performance level for subsystems

This subclause describes a simplified procedure for estimating the PL of a subsystem based on designated architectures. Other architectures may be mapped to these designated architectures in order to obtain an estimation of the PL (see 6.1.1).

The designated architectures are represented as block diagrams, and are listed in the context of each category in 6.1.3.2. Information about the block method and the safety-related block diagrams are given in 6.1.3.2 and Annex B. See also IEC 61078:2016.

A designated architecture is always assigned to a subsystem. In case the SRP/CS consists of one subsystem, the designated architecture will be the same for the entire SRP/CS. In case the SRP/CS consists of multiple subsystems, every subsystem has to be assigned a designated architecture, so a single SRP/CS can comprise multiple architectures.

The simplified approach is based on:

a) mission time (T_M), 20 years (see 3.1.33);

b) constant failure rates within the mission time;

c) sufficient measures to prevent common cause failure have been applied (beta factor of 2% for guidance see Annex F or IEC 61508-6:2010, Annex D)

NOTE 1 The mission time (T_M) is assumed to be 20 years, within which the component reliability by constant failure rates can be described or approximated. This is generally accomplished in electronic subsystems. Typically, the SRP/CS is replaced when the mission time is reached.

In order to claim a mission time of 20 years, the requirements according to 6.1.3.2.2 for Category B shall be observed. The actual mission time may be less than 20 years when using components which wear out sooner or for other technical reasons which should be documented. See also C.4.

The methodology considers the categories as architectures with defined DC_{avg}. The PL of each subsystem depends on the architecture, the mean time to dangerous failure ($MTTF_D$) in each channel and the DC_{avg}.

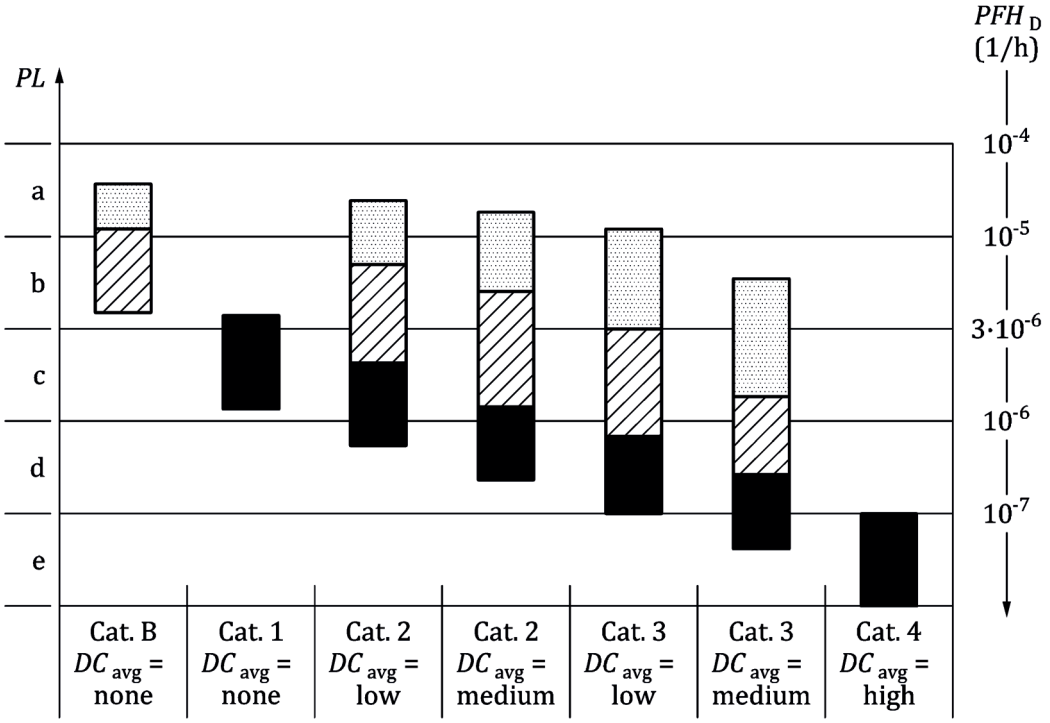
For a subsystem with software, the requirements of Clause 7 shall be applied.

The combination of several subsystems is considered in 6.2.

Figure 12 shows which selection of categories in combination with the $MTTF_D$ of each channel and DC_{avg} is able to achieve the PL. For the estimation of the PL, Figure 12 gives the different possible combinations of category with DC_{avg} (horizontal axis) and the $MTTF_D$ of each channel (columns). The columns in the diagram represent the three $MTTF_D$ ranges of each channel (low, medium and high) which can be selected to achieve the required PL.

Before using this simplified approach with Figure 12 (which represents results of different Markov models based on designated architectures of 6.1.3), the category of the subsystem (see 6.1.3.2) as well as DC_{avg} (see 6.1.5) and the $MTTF_D$ of each channel (see 6.1.4) shall be determined (see Annex C to Annex E). For categories 2, 3 and 4, sufficient measures against common cause failure shall be carried out (for guidance, see 6.1.6 and Annex F). Taking these parameters into account, Figure 12 provides a graphical method for determining the PL, achieved by the subsystem. The combination of category (including common cause failure) and DC_{avg} determines which column of Figure 12 is to be chosen. According to the $MTTF_D$ of each channel, one of the three different shaded areas of the relevant column shall be chosen.

The vertical bands in Figure 12 show the range of performance that can be expected from each combination of $MTTF_D$, Category and DC_{avg}. Finding the appropriate ranges for each of these variables in the bands in the Figure 12 and then reading across to the vertical axis will indicate the PL that can be achieved with this combination. For a more precise numerical selection of PL depending on the precise value of $MTTF_D$ of each channel, see Annex K.



Key

PFH_D average probability of dangerous failure per hour

PL performance level

low $MTTF_D$ of each channel

medium $MTTF_D$ of each channel

high $MTTF_D$ of each channel

Figure 12 — Relationship between categories, DC_{avg}, $MTTF_D$ of each channel and PL

6.1.9 Alternative procedure to determine the performance level and PFH_D without $MTTF_D$

6.1.9.1 General

The alternative procedure to determine the PL without $MTTF_D$ is limited to subsystems incorporating mechanical, hydraulic, pneumatic, electrohydraulic or electropneumatic components where no reliability data is available and where the good engineering practice method given in C.2 cannot be applied. In that case, the machine manufacturer may use the alternative procedure described in 6.1.9.2 to 6.1.9.4 to evaluate the PL without any $MTTF_D$ calculation.

The combination of several subsystems with different PL is considered in 6.2.

6.1.9.2 Preconditions

If for mechanical, hydraulic or pneumatic components (or components comprising a mixture of technologies) no application–specific or component manufacturer reliability data is available and the good engineering practice method of C.2 cannot be applied, the machine manufacturer may evaluate the quantifiable aspects of the PL without any $MTTF_D$ calculation. Where no $MTTF_D$ data is available, the

safety-related performance level (PL) can be implemented by the architecture, the diagnostic coverage and the measures against CCF.

As a worst case assumption the T_{10D} value is limited to 10 years. For well-tried components an assumption for T_{10D} of 20 years may be accepted. In this procedure the calculation of the DC_{avg} is reduced to the arithmetic mean value of all individual component DC values in the functional channel.

The mission time (T_M) is assumed to be 20 years. For category 2 a sufficient test rate is required (see 6.1.3.2.4). The requirements, e.g. according to DC_{avg} and CCF and systematic issues, for each category (see 6.1.3) shall be fulfilled.

6.1.9.3 Inputs and outputs

Table 8 shows the relationship between achievable PL (corresponding to Figure 12) and categories. PL a and PL b can be implemented with Cat. B if basic safety principles are followed. PL c can be implemented with Cat. 1 or Cat. 2, if well-tried components and well-tried safety principles are used.

PL d can be implemented with Cat. 3, respectively PL e with Cat. 4, if well-tried components, basic and well-tried safety principles are used.

Table 8 — Performance level and PFH_D estimation based on category and component selection

Category[a]	Additional requirements		estimated PFH_D (1/h)	estimated achievable PL[b]
B		→	$5{,}0 \times 10^{-6}$	b
1		→	1,7 × 10-6	c
2	Only well-tried components are used	→	$2{,}9 \times 10^{-7}$	c
3	Only well-tried components are used	→	$2{,}9 \times 10^{-7}$	d
4	Only well-tried components are used	→	$4{,}7 \times 10^{-8}$	e

[a] All requirements in 6.1.3.2.2 to 6.1.3.2.6 for the respective category shall be fulfilled, except $MTTF_D$.

[b] The achievable PL mentioned here only covers quantifiable aspects. Additional requirements for non-quantifiable aspects as systematic failure and software (see 6.1.1) shall be fulfilled.

6.1.9.4 Logic

Where no $MTTF_D$ data is available a conservative approach using $MTTF_D$ can be assumed

— for category B, 2 and 3 $MTTF_D$ for each channel is 10 years.

— for category 1 a $MTTF_D$ of the channel of 30 years can be assumed and well-tried components shall be used. The maximum PL that can be achieved is PL c (see Annex K).

For category 2 and category 3 common-cause failures and diagnostic coverage shall be considered. The DC_{avg} shall match at least 60 % for category 2 and category 3.

Category 4 is excluded in this method.

With the category, the $MTTF_D$ and the DC_{avg}, the PL and the PFH_D of the subsystem can be determined with Table K.1.

6.1.10 Fault consideration and fault exclusion

6.1.10.1 General

When designing safety subsystems, faults and their effects shall be assessed. Each element, whose fault may cause the failure of the safety function in one of the functional channels of a subsystem, shall be considered. The designer shall make a list of faults, which can occur in the SRP/CS. This list shall include all considered faults, explanation how these faults have been noted in the design, and if fault

exclusion is claimed to give reasons for these exclusions. For subsystems pre-validated by component manufacturer, it is not necessary by the designer of the safety functions to take into account internal failures of the component(s), only failures of the interfaces,.

NOTE Faults of elements, which are not directly necessary for the execution of the safety function, but can support it (for example, filter elements, protection against over-voltage); generally do not contribute to the $MTTF_D$ of each channel.

6.1.10.2 Fault consideration

ISO 13849-2:2012 lists the important faults and failures for the various technologies. The lists of faults are not exhaustive and, if necessary, additional faults shall be considered and listed. In such cases, the method of evaluation shall also be clearly elaborated. For components not mentioned in ISO 13849-2:2012, a methodology to evaluate the impact of probable faults and/or failures of components shall be carried out, e.g. failure mode and effects analysis (FMEA, see IEC 60812), aiming at the identification of faults that are to be considered for those components.

In general, the following fault criteria shall be taken into account:

— if, as a consequence of a fault, further components fail, the first fault together with all following faults shall be considered as a single fault;

— the simultaneous occurrence of two or more faults having separate causes is considered highly unlikely and therefore needs not be considered.

Two or more separate faults having a common cause shall be considered as a common cause failure (known as a CCF, see Annex F).

6.1.10.3 Fault exclusion

It may be necessary to exclude faults in order to evaluate subsystems. Fault exclusion is a compromise between technical safety requirements and the theoretical possibility of occurrence of a fault.

Fault exclusion can be based on:

a) the technical improbability of occurrence of some faults,

b) generally accepted technical experience, independent of the considered application, and

c) technical requirements related to the application and the specific hazard.

Fault exclusion is only applicable for certain failures of an element and it is up to the designer (manufacturer or integrator) to prove the exclusion of the respective faults based on the limits set forward by the design and use. Such fault exclusion is only possible provided that their unlikely occurance can be justified based on the known laws of physical science. Any such fault exclusions shall be justified and documented.

The application of fault exclusion to certain faults for an element inside a subsystem does not limit the necessity of the application measures against systematic failures.

It is possible that some faults are excluded by the manufacturer and some by the subsystem integrator.

There shall be a specific characterization of the type of fault that is excluded. It would not be acceptable to state simply that a component will not break, distort or degrade due to wear. It would be necessary to state the direct influence under which the component will not break, distort or degrade due to wear. For example, the component will have no faults when subjected to a force of X Newtons from direction Y.

The fault exclusion must be justifiable under all expected environmental conditions including temperature, pressure, vibration, pollution, corrosive atmosphere.

PL e shall not depend solely on fault exclusion.

NOTE 1 Information on fault exclusions is available in ISO 13849-2:2012, Annex A to Annex D.

NOTE 2 Product standards can give further information.

6.1.11 Well-tried component

A well-tried components for safety-related applications is a component, which shall be either

a) widely used in the past with documented successful results in similar applications;

NOTE See IEC 61508-2: 2010, 7.4.10, for "proven in use".

b) listed in the informative annexes A to D of ISO 13849-2:2012, or

c) made, verified and validated using principles which demonstrate its suitability and reliability for safety-related applications according to relevant product and application standards.

The decision to accept a particular component as being well-tried depends on the application, e.g. owing to the environmental influences.

Complex electronics and components (e.g. PLC, microprocessor, and application-specific integrated circuit) shall not be considered as equivalent to well-tried.

6.2 Combination of subsystems to achieve an overall performance level of the safety function

6.2.1 General

An SRP/CS may be realized using a combination of subsystems and an overall PL may be achieved using the methods described in this clause. In this case, the validation of the combination of subsystems as an SRP/CS is required (see Figure 13). These subsystems may be assigned to one or different categories.

According to 6.1.3.2, the combination of subsystems to an SRP/CS starts at the points where the safety-related signals are initiated and ends at the output of the power control elements. The combined subsystems could consist of several parts connected in a linear (series alignment) way. To avoid a new complex estimation of the performance level (PL) achieved by combined subsystems where the separate PLs of all parts are already calculated, the following estimations are presented for a combination of subsystems.

If previously validated subsystems according to IEC 62061 or IEC 61508 (SIL) for high demand or continuous mode that use Route 1_H (see IEC 61508-2:2010, 7.4.4.2) are used the SIL can be correlated to a PL using 6.1.2 and 6.2.2. PFH values calculated according to IEC 61508 or IEC 62061 with the above mentioned limitations can be considered as PFH_D values according to this document.

Category cannot always be deduced and is not required from a subsystem validated according to IEC 62061 or IEC 61508.

6.2.2 Known PFH_D values

When combining subsystems with known PFH_D values, the PFH_D values can be combined as shown below. Assumed that there are *n* separate subsystems SB_1 to SB_n. These subsystems operate in a series combination, which as a whole performs a safety function. For each SB_i, a PL_i has already been evaluated. This situation is illustrated in Figure 13 (see also Figure 5 and Figure H.2).

If the PFH_D values of all SB_n are known, then the PFH_D of the SRP/CS is the sum of all PFH_D values of the *n* individual SB_n. The PL of the SRP/CS is limited by:

— the lowest PL of any individual SB_i involved in performing the safety function and

— the PL corresponding to the PFH_D of the combined SRP/CS according to Table 2.

NOTE See Annex H for an example of this method.

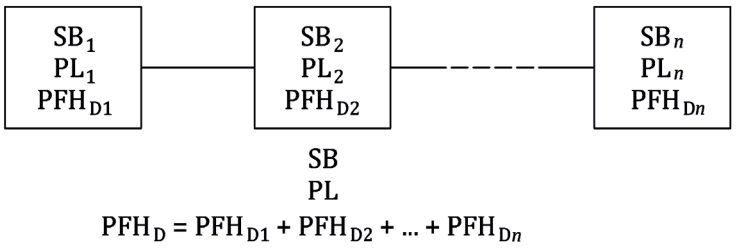


Figure 13 — Combination of subsystems to achieve overall PL

6.2.3 Unknown PFH_D values

If the PFH_D values of all individual SB_i are not known, then as an alternative to 6.2.2, the PL of the SRP/CS performing the safety function may be defined according to 6.1 or calculated using Table 9 as follows:

a) Identify the lowest PL of all subsystems: this is $PL_{low;}$

b) Identify the number of subsystems with PL_{low}: this number is N_{low}

c) Look-up PL in Table 9.

Table 9 — Calculation of PL for series alignment of subsystems

PL_{low}	N_{low}	⇒	PL of the SRP/CS
a	>3	⇒	None, not allowed
	≤ 3	⇒	a
b	>2	⇒	a
	≤ 2	⇒	b
c	>2	⇒	b
	≤ 2	⇒	c
d	>3	⇒	c
	≤ 3	⇒	d
e	>3	⇒	d
	≤ 3	⇒	e
NOTE This table is based on the defined PFH_D ranges for each PL (see Table 2) forming a kind of logarithmic scale.			

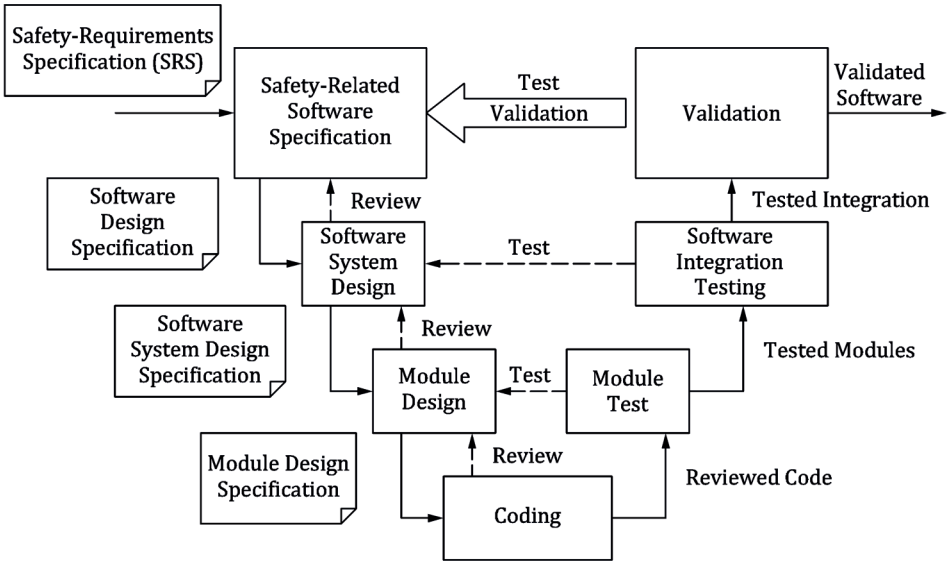
7 Software safety requirements

7.1 General

Activities related to the development of safety-related embedded or application software shall primarily consider the avoidance of faults during the software lifecycle (see figure 14a). The main objective of the following requirements is to have readable, understandable, testable and maintainable software.

NOTE 1 Annex J gives more detailed recommendations for lifecycle activities.

NOTE 2 Annex N gives an overview, which measures apply to SRASW performed by usage of LVL and SRASW performed by usage of FVL.



Key

→ result

⇢ verification

Figure 14a — Simplified V-model of software safety lifecycle

If pre-assessed safety-related hardware and software modules are used in combination with LVL a simplified software lifecycle shown in Figure 14b is applicable. Typically, this applies to the use of module based programming in LVL, that only require simple interconnections to be configured, which limits the inputs and outputs to a pre-defined set of values, including a combination of modules.

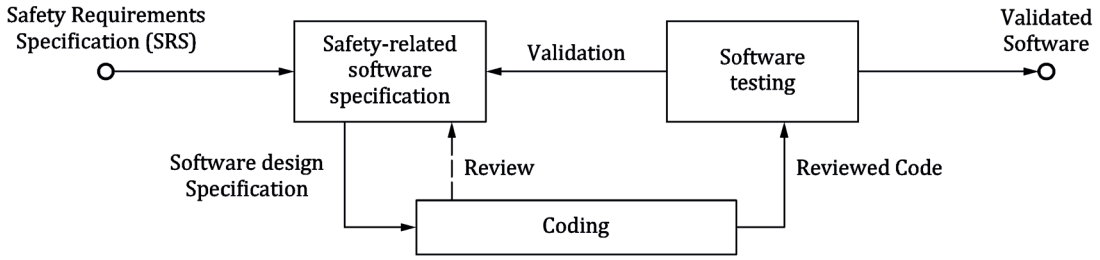


Figure 14b — Simplified V-model for software if pre-assessed safety-related hardware and software modules are used in combination with LVL

7.2 Limited variability language and full variability language

7.2.1 Limited variability language

Limited variability language is a software programming language, whose notation is textual or graphical or has characteristics of both, for commercial and industrial programmable electronic controllers with a range of capabilities limited to their application (IEC 61508-4:2010, 3.2.14).

NOTE Limited variability language (LVL) should be designed to be easily understandable by the software designer and should be stringently focused on the applications to be implemented.

When safety and non-safety functions are implemented in the same hardware environment, it shall be demonstrated that the safety functions are not impacted by the non-safety functions under normal or

fault conditions. This may include but is not limited to blocking or delaying a safety response which is required to be performed at any time.

The following are examples of limited variability languages:

a) ladder diagram (see IEC 61131-3:2013, 8.2); a graphical language consisting of a series of input symbols (representing behavior similar to devices such as normally open and normally closed contacts) interconnected by lines (to indicate the flow of current) to output symbols (representing behaviour similar to relays);

b) Function block diagram (see IEC 61131-3:2013, 8.3); in addition to Boolean operators, allows the use of more complex functions such as data transfer file, block transfer read/write, shift register and sequencer instructions;

c) Sequential function chart (see IEC 61131-3:2013, 6.7); a graphical representation of a sequential program consisting of interconnected steps, actions and directed links with transition conditions;

d) Boolean algebra; a low-level language based on Boolean operators such as AND, OR and NOT with the ability to add some mnemonic instructions.

7.2.2 Full variability language

This type of language is designed for computer programmers and provides the capabilities to implement a wide variety of functions and applications.

Typical examples of systems using full variability language (FVL) are general purpose computers. In the machinery sector, FVL is found in embedded software and rarely in application software.

EXAMPLE Ada, C, Pascal, Instruction List, assembler languages, C++, Java, MATLAB, Simulink and SQL (without limitations for use and full variety of instructions)

7.2.3 Decision for limited variability language or full variability language

In general software can be written in FVL or LVL. The designer of the SRP/CS shall follow Figure 15 for the determination, if a programming language is FVL or LVL.

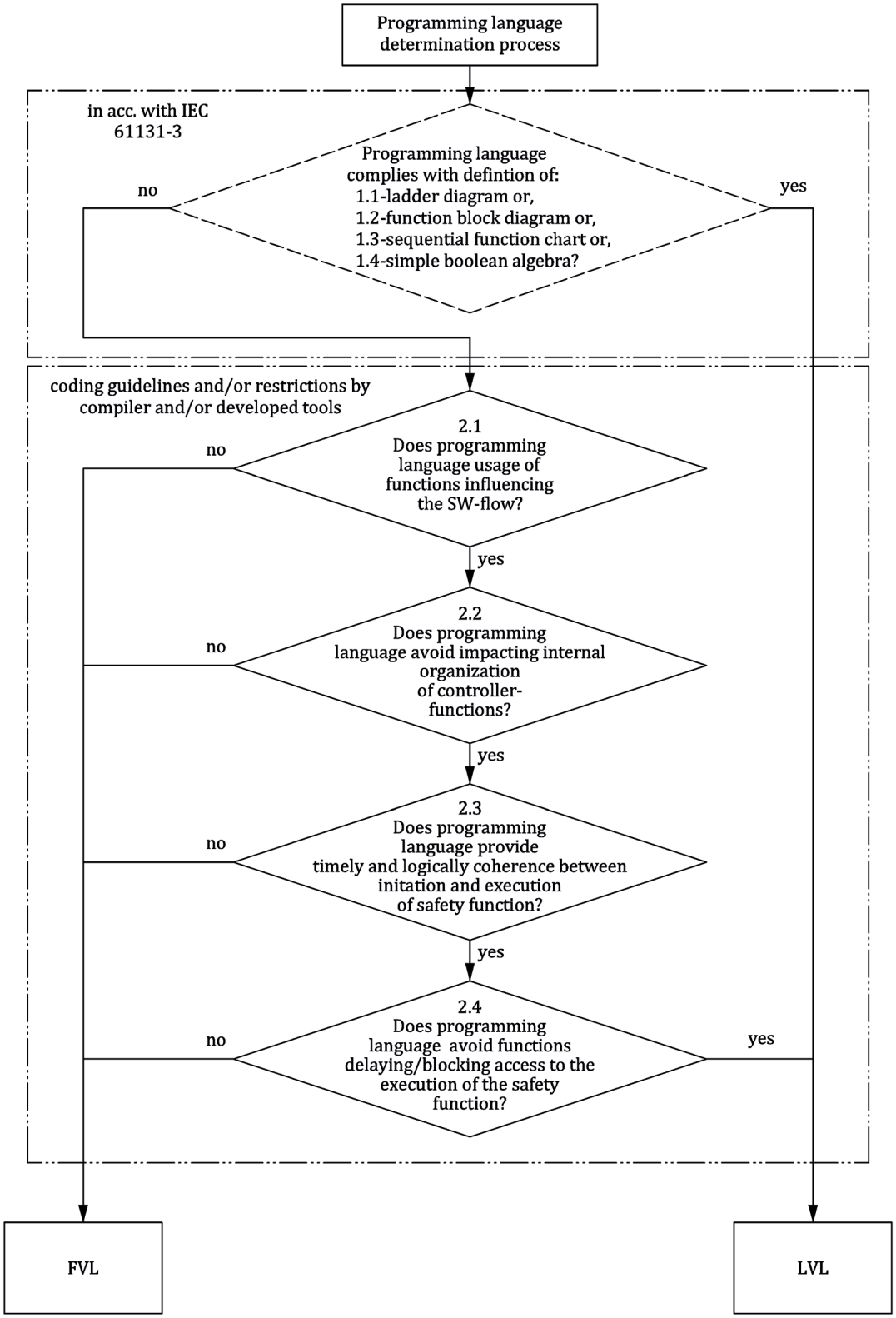


Figure 15 — Decision guideline for FVL or LVL

EXAMPLE 1 If C is used there is no accordance with IEC 61131-3 and if any of the questions 2.1 to 2.4 are answered with no, the result will be FVL.

EXAMPLE 2 If a type of structured text or a limited sub-set of C is used with restrictions within the complier and/or development tools and restrictive coding guidelines which fulfil 7.3 a) and b) and if any of the questions 2.1 to 2.4 can be answered with yes, the result will be LVL.

EXAMPLE 3 If Visual Basic is used there is no accordance with IEC 61131-3 and the Questions 2.1 to 2.4 answered with no, the result will be FVL.

EXAMPLE 4 If a function block diagram is used with self-declared functions blocks in structured text in accordance with IEC 61131-3 and the restrictions of 7.3 a) and b) are fulfilled the result will be LVL.

NOTE 1 The technical documentation – especially safety manuals of products – can be followed for both, LVL and FVL. Both limitations via internal functions of the compiler and limitations via coding guideline can be used.

NOTE 2 Annex N gives an overview, which measures apply to SRASW and SRESW performed either by usage of LVL or FVL.

7.3 Safety-related embedded software

For safety-related embedded software (SRESW) for components with PL_r a to d, the following basic measures shall be applied:

a) software safety lifecycle with verification and validation activities, e.g. reviews and tests, see Figure 14a;

b) documentation of specification and design, e.g. software design specification, software system design specification, module design specification, code listings including comments;

c) modular and structured design and coding, e.g. hierarchy and limitation of functionality, clear program structure, definition of interfaces, well-structured call-graph, avoidance of interrupts, use of coding guidelines;

d) control of systematic failures, e.g. program sequence monitoring, controlling errors in the data communication process (see G.2);

e) where using software-based measures for control of random hardware failures, verification of correct implementation, e.g. correct implementation of diagnostic measures, RAM/ROM/CPU tests, hardware tests, plausibility checks;

f) functional testing, e.g. black box testing, e.g. by verification of correct output data based on input data (valid, invalid and border values), compatibility of interfaces, timing;

g) appropriate software safety lifecycle activities after modifications, e.g. based on an impact analysis.

For SRESW for components with PL_r c or d, the following additional measures shall be applied:

h) project management and quality management comparable to, e.g. IEC 61508 e.g. definition of workflow, responsibilities, configuration management;

i) documentation of all relevant activities during software safety lifecycle, e.g. documentation of reviews, testing, validation and verification;

j) configuration management to identify all configuration items and documents related to a SRESW release, e.g. version control of code listings, modules, design documents, test plans, release control, archiving;

k) structured specification with safety requirements and structured design;

l) use of suitable programming languages and computer-based tools with confidence from use;

m) modular and structured programming, separation from non-safety-related software, limited module sizes with fully defined interfaces, use of design and coding standards;

n) coding verification by walk-through/review with control flow analysis, e. g. to check for faults, quality of comments, compliance with coding guidelines, clarity, readability, completeness;

o) extended functional testing, e.g. grey box testing, performance testing or simulation, e.g. by using unspecified input data, extreme environmental conditions, full load, testing based on knowledge of internal coding.

SRESW for components with PL_r e shall comply with IEC 61508-3:2010, Clause 7, appropriate for SIL 3. When using diversity in specification, design and coding, for the two channels used in a subsystem with category 3 or 4, PLr e can be achieved with the above-mentioned measures for PLr of c or d.

NOTE For SRESW with diversity in design and coding, for components used in a subsystem with category 3 or 4, the effort involved in taking measures to avoid systematic failures can be reduced by, for example, reviewing parts of the software only by considering structural aspects instead of checking each line of code. Annex G gives guidance referring the usable measures to carry out these aspects.

For components for which SRESW requirements are not fulfilled, e.g. PLCs without safety rating by the manufacturer, these components may be used under the following alternative conditions:

— the subsystem is limited to PL a or b and uses category B, 2 or 3;

— the subsystem is limited to PL c with category 2 or PL d with category 3 and it is necessary to fulfil the diversity requirements of the CCF, where both channels use diverse technologies/design or physical principles.

The associated hardware and SRASW shall be assessed in accordance with the requirements of this document, especially of CCF (see Annex F)

7.4 Safety-related application software

The software safety lifecycle (see 7.1) applies also to safety-related application software (SRASW).

SRASW written in LVL and complying with the following requirements can achieve a PL a to PL e. If SRASW is written in FVL, the requirements for SRESW shall apply and PL a to PL e is achievable. 7.4 shows a decision guideline for FVL or LVL.

If a part of the SRASW within one component has any impact (e.g. due to its modification) on several safety functions with different PL, then the requirements related to the highest PL shall apply.

For SRASW for components with PL_r from a to e, the following basic measures shall be applied:

— development lifecycle with verification and validation activities, e.g. reviews and tests, see Figure 14a;

— documentation of specification and design;

— modular and structured programming;

— functional testing;

— appropriate development activities after modifications.

For SRASW for components with PL_r from c to e, the following additional measures with increasing efficiency (lower effectiveness for PL_r of c, medium effectiveness for PL_r of d, higher effectiveness for PL_r of e) apply.

a) The software design specification shall be reviewed (see also Annex J), made available to every person involved in the lifecycle and shall contain the description of:

   1) safety functions with required PL and associated operating modes,

   2) performance criteria, e.g. reaction times,

3) communication interfaces,

4) detection and control of hardware failures to achieve the required diagnostic coverage and fault reaction.

b) Selection of tools, libraries, languages:

1) Tools shall be suitable for the application. For PL e achieved with one component and its tool, the tool shall comply with the applicable component standard. If two diverse components with diverse tools are used, successful operating experience gained from prior projects may be sufficient. Technical features which detect conditions that could cause systematic error (such as data type mismatch, ambiguous dynamic memory allocation, incomplete called interfaces, recursion, pointer arithmetic) shall be used. Checks shall mainly be carried out during compile time and not only at runtime. Tools should enforce language subsets and coding guidelines or at least supervise or guide the developer using them.

2) Whenever reasonable and practicable, validated function block (FB) libraries should be used – either safety-related FB libraries provided by the tool manufacturer (highly recommended for PL e) or validated application specific FB libraries and in conformity with this document.

3) A justified LVL-subset suitable for a modular approach should be used, e.g. accepted subset of IEC 61131-3 languages.

c) Software design shall feature:

1) semi-formal methods to describe data and control flow, e.g. state diagram or program flow chart,

2) modular and structured programming predominantly realized by function blocks deriving from safety-related validated function block libraries or other modularity structure to achieve easy code reading and testability,

3) function blocks of limited size of coding,

4) code execution inside function block which should have one entry and one exit point,

5) architecture model of three stages: inputs ⇒ processing ⇒ outputs (see Figure 16 and Annex J),

6) assignment of a safety output at only one program location, and

7) use of techniques for detection and control of hardware failure and for defensive programming within input, processing and output blocks which lead to safe state.

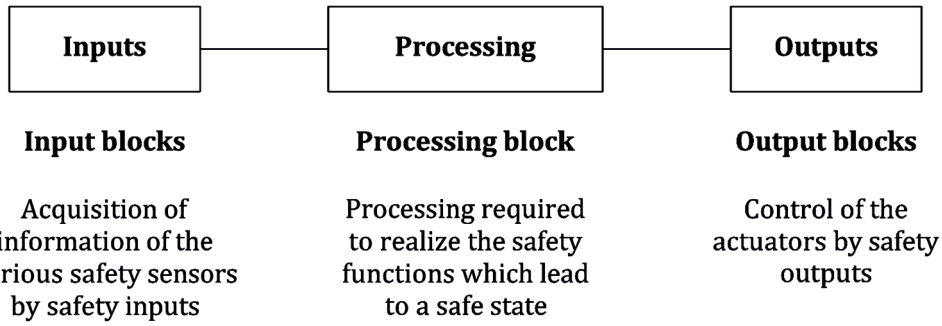


Figure 16 — General architecture model of software

d) Where SRASW and non-SRASW are combined in one component:

1) SRASW and non-SRASW shall be coded in different function blocks with well-defined interfaces;

2) there shall be no logical combination of non-safety-related and safety-related data which could lead to downgrading of the integrity of safety-related signals, for example, combining safety-related and non-safety-related signals by a logical "OR" where the result controls safety-related signals.

e) Software implementation/coding:

1) code shall be readable, understandable and testable and, because of this symbolic variables (instead of explicit hardware addresses) should be used;

2) justified or accepted coding guidelines shall be used (see also Annex J);

3) data integrity and plausibility checks (e.g. range checks.) available on application layer (defensive programming) should be used;

4) code should be tested by simulation;

5) verification should be performed by control flow analysis and data flow analysis for PL d or e.

f) Testing:

1) the appropriate validation method is black-box testing of functional behaviour and performance criteria (e.g. timing performance);

2) for PL d or e, test case execution from boundary value analysis is recommended;

3) test planning is recommended and should include test cases with completion criteria and required tools;

4) I/O testing shall ensure that safety-related signals are correctly used within SRASW.

g) Documentation:

1) all lifecycle and modification activities shall be documented;

2) documentation shall be complete, available, readable and understandable;

3) code documentation within source text shall contain module headers with legal entity, functional and I/O description, version of used library function blocks, and sufficient comments of networks/statement and declaration lines.

h) Verification

NOTE Verification is only used for application-specific code, and not for validated library functions.

Verification shall be performed by e.g. review, inspection, walkthrough or other appropriate activities.

i) Configuration management

It is highly recommended that procedures and data backup be established to identify and archive documents, software modules, verification/validation results and tool configuration related to a specific SRASW version.

j) Modifications

Prior to a modification of SRASW an impact analysis shall be performed to ensure consistency with the software design. Appropriate lifecycle activities shall be performed after modifications. Access rights to modifications shall be controlled and modification history shall be documented.

7.5 Software-based manual parameterization

7.5.1 General

This subclause is limited in scope to only manual, software-based parameterization that is performed and controlled by an authorized person. See also 5.2.3.6 and Table M.2.

Some safety-related subsystems or SRP/CS need parameterization for a safety function or a sub-function.

EXAMPLES A converter with integrated sub-functions can be parameterized via a PC-based configuration tool for setting the upper speed limit parameter. To establish the detection zone of a laser scanner, parameters such as angle and distance can be configured per the manufacturer's safety documentation and the machine risk assessment.

The objective of the requirements for software based manual parameterization is to guarantee that the safety-related parameters specified for a safety function or a sub-function are correctly transferred into the hardware performing the safety function or a sub-function. Different methods can be applied to set such parameters; even dip switch based parameterization can be used to set or change safety-related parameters. However, PC-based tools with dedicated parameterization software, commonly called configuration or parameterization tools, are becoming more prevalent.

NOTE 1 Safety-related parameterization which is carried out automatically without human interaction, for example, based on input signals, is not considered in this subclause.

NOTE 2 Direct control of a machine by an operator, e.g. speed control of a forklift truck is not considered as manual parameterization as described in this subclause.

If the configuration or parameterization tool is pre-designed in accordance with this document or IEC 61508, for example together with its dedicated subsystem, it is assumed that there will be no dangerous failures due to the influences listed in 7.5.2 or any other influence that is reasonable foreseeable. The requirements of 7.5.5 apply when a software based manual parameterization is performed with the pre-designed tool.

If a safety-related subsystem or SRP/CS is not capable of being parameterized by software based manual parameterization as described above, 8.5 does not apply.

7.5.2 Influences on safety-related parameters

During software based manual parameterization the parameters can be affected by several influences, such as:

a) data entry errors by the person responsible for parameterization;

b) faults of the software of the parameterization tool;

c) faults of further software and/or service provided with the parameterization tool;

d) faults of the hardware of the parameterization tool;

e) faults during transmission of parameters from the parametrization tool to the SRP/CS or a subsystem;

f) faults of the SRP/CS or a subsystem to store transmitted parameters correctly;

g) systematic interference during the parameterization process, e.g. by electromagnetic interference or loss of power.

h) interference due to external influences or factors, such as electromagnetic interference or (random) loss of power.

With no measures applied to counteract, avoid or control potential dangerous failures caused by the influences listed above, such influence can lead to the following:

— parameters are not updated by the parameterization process, completely or in parts without notice to the person responsible for the parametrization;

— parameters are incorrect, completely or in parts;

— parameters are applied to an incorrect device, such as when transmission of parameters is carried out via a wired or wireless network.

7.5.3 Requirements for software based manual parameterization

Software based manual parameterization shall use a dedicated tool provided by the manufacturer or supplier of the SRP/CS or the related subsystem(s). This tool shall have its own identification (name, version). The SRP/CS or the related subsystem(s) and the parameterization tool shall have the capability to prevent unauthorized modification, for example by using a dedicated password.

Parameterization while the machine is running shall be permitted only if it does not cause an unsafe state.

It is possible to fulfil the requirements by using a pre-designed subsystem or the design shall follow this document as detailed below.

When using a pre-designed SRP/CS or subsystem that is capable of software based manual parameterization, the target is to prevent dangerous failure due to the influences listed in 7.5.2 or any other influence that is reasonable foreseeable. The validation of the pre-designed subsystem shall include the issue of parameterization.

When an SRP/CS or subsystem that is capable of software based manual parameterization is designed according to this document there shall be no undetected dangerous failure due to the influences listed above or any other influence that is reasonable foreseeable. The following requirements shall be fulfilled in addition:

a) The design of the software based manual parameterization shall be considered as a safety-related aspect of SRP/CS design that is described in a safety requirements specification.

b) The SRP/CS or subsystem shall provide means to check the data plausibility, e.g. checks of data limits, format and/or logic input values.

c) The integrity of all data used for parameterization shall be maintained. This shall be achieved by applying measures to:

   1) control the range of configured values by a validity (range) check;

   2) control data corruption before transmission;

   3) control the effects of errors from the parameter transmission process;

   4) control the effects of incomplete parameter transmission;

   5) control the effects of faults and failures of hardware and software of the parameterization;

   6) control the effect of the interruption of the power supply.

d) The parameterization tool shall fulfil all requirements for SRP/CS according to this document or IEC 61508.

e) Alternatively to d) a special procedure shall be used for setting the safety-related parameters. This procedure shall include confirmation of input parameters to the SRP/CS by either:

   — retransmitting of modified parameters to the parameterization tool; or

— other means to confirm the integrity of the parameters;

— as well as subsequent confirmation, for example by a suitably skilled person and by means of an automatic check by a parameterization tool. New values of safety-related parameters shall not be used for safety-related operation before the changes are acknowledged and confirmed.

NOTE This is of particular importance where a parameterization software tool uses a device not specifically intended for this purpose (e.g. personal computer or equivalent).

The software modules used for encoding/decoding within the transmission/retransmission process and software modules used for visualization of the safety-related parameters to the user shall, as a minimum, use diversity in function(s) to avoid systematic failures.

7.5.4 Verification of the parameterization tool

The following verification activities shall be performed to verify the basic functionality of the parameterization tool:

— verification of the correct setting for each safety-related parameter (minimum, maximum and representative values);

— verification that the safety-related parameters are checked for plausibility, for example by detection of invalid values;

— verification that means are provided to prevent unauthorized modification of safety-related parameters.

NOTE This is of particular importance where the parameterization is carried out using a device not specifically intended for this purpose (e.g. personal computer or equivalent).

7.5.5 Documentation of software based manual parameterization

Software based manual parameterization shall be carried out using the dedicated parameterization tool provided by the manufacturer or supplier of the SRP/CS or the related subsystem(s) and shall be documented according to the requirements given in the information for use. This information can originate from different parties, see also Clause 13 (information for use). Protective measures against unauthorized access shall be activated and used.

The initial parameterization, and subsequent modifications to the parameterization, shall be documented. The documentation shall include:

a) the date of initial parameterization or change;

b) data or version number of the data set;

c) name of the person carrying out the parameterization;

d) an indication of the origin of the data used (e.g. pre-defined parameter sets);

e) clear identification of safety-related parameters.

8 Verification that achieved performance level meets required performance level

For each individual safety function the PL of the related SRP/CS shall match or be greater than the required performance level (PL_r) determined according to 5.3 (see Figure 4) and 6.1.1. If this is not the case, iteration in the process described in Figure 4 is necessary.

The PL of the different subsystems which are part of a safety function shall be greater than or equal to the required performance level of this safety function (see 5.3 and 6.1.1).

9 Ergonomic aspects of design

The interface between operators and the SRP/CS shall be designed and realized to minimize exposures to hazards during the intended use and the reasonable foreseeable misuse of the machine due to neglecting ergonomic principles.

The ergonomic principles given in ISO 12100:2010, 6.2.8, apply.

NOTE Ergonomic principles are intended to improve the ease of use of the control systems to avoid motivation for defeating or unintended misuse of the machine. See ISO/TR 22100-3 and ISO 9241-210 for guidance on ergonomics.

10 Validation

10.1 Validation principles

10.1.1 General

The purpose of the validation process is to confirm that the SRP/CS meets the overall safety requirements specification created in accordance with Clause 5 and Clause 7.

Figure 17 gives an overview of the validation process: validation consists of applying analysis (see 10.3) and executing functional tests (see 10.4) under foreseeable conditions in accordance with the validation plan.

NOTE 1 The validation is limited to the designed SRP/CS or a part of it supporting the safety functions required in achieving the intended risk reduction at the machine level given in ISO 12100. The SRP/CS validation is intended to be part of the overall validation process of the machine.

The validation activities shall ensure the completeness and correctness of each design activity identified in the validation plan.

The validation to be applied to the SRP/CS includes inspection (e.g. by analysis) and testing of the SRP/CS to ensure that it achieves the requirements stated in the safety requirements specification (according to Clause 6).

The validation shall demonstrate that the SRP/CS meets the requirements and, in particular, the following:

a) the specified functional requirements of the safety functions provided by that part, as set out in the safety requirements specification;

b) the requirements of the specified PL shall be in accordance to 7.1.1:

   1. the requirements of the specified category,
   2. the measures for control and avoidance of systematic failures (systematic integrity),
   3. if applicable, the requirements of the software, and
   4. the ability to perform a safety function under expected environmental conditions;

c) the ergonomic design, interaction and positioning of the operator interface.

Validation process should be carried out by person(s) who is/are independent from the design of the SRP/CS.

NOTE 2 An independent person is a person not involved in the design of the SRP/CS and does not necessarily mean that a third-party is required.

The analysis should be started as early as possible in, and in parallel with, the design process. Problems can then be corrected early while they are still relatively easy to correct, i.e. during steps “design and technical realization of the safety function” and “evaluate the PL”. It can be necessary for some parts of the analysis to be delayed until the design is well developed.

Where necessary due to the system’s size, complexity or the effects of integrating it with the control system (of the machinery), special arrangements should be made for:

— validation of the subsystem separately before integration, including simulation of the appropriate input and output signals, and

— validation of the effects of integrating safety-related parts into the remainder of the control system within the context of its use in the machine.

The balance of analysis and testing depends on the technology used for the safety-related parts and the required performance level. For categories 2, 3 and 4 the validation of the safety function shall also include testing by appropriate fault injection to show that. Among other things, the fault reaction will be initiated by the implemented diagnostic function.

“Modification of the design” in Figure 17 refers to the design process. If the validation cannot be successfully completed, changes in the design are necessary. The validation of the modified parts of the SRP/CS shall then be repeated. This process shall be iterated until the SRP/CS for each safety function is successfully validated.

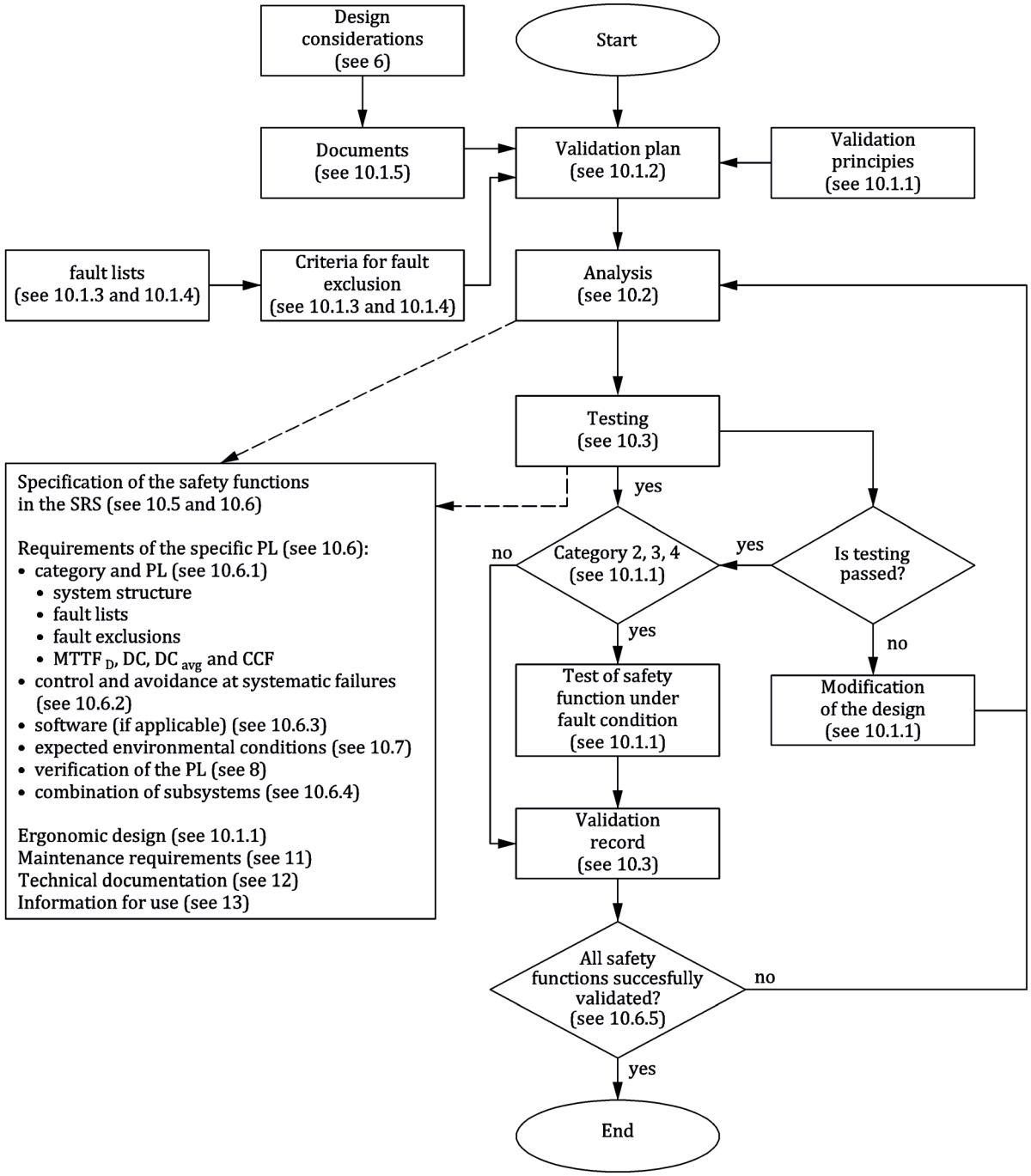


Figure 17 — Overview of the validation process

10.1.2 Validation plan

The validation plan shall identify and describe the requirements for carrying out the validation process and shall be made available to all persons and parties involved in the validation process. The validation plan shall also identify the means to be employed to validate the specified safety functions. It shall identify, where appropriate:

a) the specification documents,

b) the operational and environmental conditions during testing,

c) the analyses and tests to be applied,

d) the reference to test standards to be applied, and

e) the persons or parties responsible for each step in the validation process.

10.1.3 Generic fault lists

Validation involves consideration of the behaviour of the SRP/CS for all faults to be considered. A basis for fault consideration is given in the tables of fault lists in ISO 13849-2:2012, Annex A to Annex D, which are based on experience and which contain:

— the components/elements to be included, e.g. conductors/cables,

— the faults to be taken into account, e.g. short circuits between conductors,

— the permitted fault exclusions, taking into account environmental, operating and application aspects, and

— a remarks section giving the reasons for the fault exclusions.

Only permanent faults are taken into account in the fault lists.

10.1.4 Specific fault lists

If necessary, a specific product-related fault list shall be generated as a reference document for the validation of the subsystem(s) and/or subsystem element(s). The list can be based on the appropriate generic list(s) found in the annexes of ISO 13849-2:2012 or (reoccurring) faults found at a result of product observation.

Where the specific product-related fault list is based on the generic list(s) it shall state:

a) the faults taken from the generic list(s) to be included,

b) any other relevant faults to be included but not given in the generic list (e.g. common-cause failures),

c) the faults taken from the generic list(s) which may be excluded on the basis that the criteria given in the generic list(s) are satisfied, and

d) exceptionally any other faults for which the generic list(s) do not permit an exclusion, but for which justification and rationale for an exclusion is presented.

Where this list is not based on the generic list(s), the designer shall give the rationale for fault exclusions.

10.1.5 Information for validation

The information required for validation will vary with the technology used, the category or categories and PL to be demonstrated, safety requirements specification, and the contribution of the SRP/CS to the reduction of the risk. Documents containing sufficient information from the following list shall be included in the validation to demonstrate that the safety-related parts perform the specified safety functions to the required PL and category:

a) safety requirements specification, including the required characteristics of each safety function, e.g. response time (e.g. ISO 13855:2010), operating mode, PL, interfaces between the subsystems of the SRP/CS and if necessary characteristics of used category of each subsystem of the SRP/CS;

b) drawings and specifications, e.g. for mechanical, hydraulic and pneumatic parts, printed circuit boards, assembled boards, internal wiring, enclosure, materials, mounting;

c) block diagram(s) and where needed for clarification with a functional description of the blocks;

d) circuit diagram(s), including interfaces/connections;

e) functional description of the circuit diagram(s), where needed for clarification;

f) time sequence diagram(s) for switching components, signals relevant for safety;

g) description of the relevant characteristics of components previously validated;

h) for safety-related parts other than those listed in g), component lists e.g. with item designations, rated values, tolerances, relevant operating stresses, type designation, failure rate data and component manufacturer, and any other data relevant to safety;

NOTE 1 Data can be transmitted according to VDMA 66413.

i) report of analysis of all relevant faults according to 10.1.3 and 10.1.4, such as those listed in the tables of ISO 13849-2:2012, Annex A to Annex D, including the justification of any excluded faults;

j) report of analysis of the influence of processed materials;

k) information for use, maintenance requirements e.g. installation and operation manual/instruction handbook.

Where software is relevant to the safety function(s), the software documentation shall include:

— a specification which is clear and unambiguous,

— evidence that the software is designed to achieve the required PL (see 10.6.3), and

— details of tests (in particular test reports) carried out to prove that the required PL is achieved.

Information is required on how the PL and average probability of a dangerous failure per hour (PFH_D) is determined. The documentation of the quantifiable aspects shall include:

— the safety-related block diagram (see Annex B) or designated architecture according to 6.1.3.2,

— the determination of $MTTF_D$, DC_{avg} and CCF, and

— the determination of the category.

Information is required for documentation on measures against systematic failures of the SRP/CS.

Information is required to describe how the combination of several subsystems achieves the required PL.

NOTE 2 Where practicable a clear and traceable reference to existing documents will suffice.

10.2 Validation of the safety requirements specification

Prior to the validation of the design of the SRP/CS or the combination of subsystems providing the safety function, the requirements specification for the safety function shall be verified to ensure consistency and completeness for its intended use (see 5.4).

The requirements for all safety functions of the machine control system shall be documented.

In order to validate the specification, appropriate measures to detect systematic failures (errors, omissions or inconsistencies) shall be applied.

Validation may be performed by reviews and inspections of the safety requirements specification, in particular to prove that all aspects of

— the intended application requirements and safety needs (i.e. risk assessment), and

— the operational and environmental conditions and possible human errors (e.g. misuse) have been considered.

10.3 Validation by analysis

10.3.1 General

Validation of the SRP/CS shall be carried out by analysis. Inputs to the analysis include the following:

— the safety function(s), their characteristics and the safety integrity specified according to 5.2;

— the system structure (e.g. designated architectures) according to 6.1.3.2;

— the quantifiable aspects ($MTTF_D$, DC_{avg} and CCF) according to 6.1.4, 6.1.5, Annex F by validating assumptions and data that were associated in selecting the values used in the system calculations;

— the non-quantifiable, qualitative aspects which affect system behaviour (if applicable, software aspects);

— deterministic arguments;

— fault lists;

— criteria for fault exclusion.

NOTE A deterministic argument is an argument based on qualitative aspects (e.g. quality of manufacture, experience of use). This consideration depends on the application, which, together with other factors, can affect the deterministic arguments. Deterministic arguments differ from other evidence in that they show that the required properties of the system follow logically from a model of the system. Such arguments can be constructed on the basis of simple, well-understood concepts.

10.3.2 Analysis techniques

The following are two basic techniques that can be used for analysis:

a) Top-down (deductive) techniques are suitable for determining the initiating events that can lead to identified top events, and calculating the probability of top events from the probability of the initiating events. They can also be used to investigate the consequences of identified multiple faults.

   EXAMPLE 1 Fault tree analysis (FTA, see IEC 61025), event tree analysis (ETA, see IEC 62502).

b) Bottom-up (inductive) techniques are suitable for investigating the consequence of identified single faults.

   EXAMPLE 2 Failure modes and effects analysis (FMEA, see IEC 60812) and failure modes, effects and criticality analysis (FMECA, see IEC 60812).

10.4 Validation by testing

10.4.1 General

Testing shall be part of the validation unless category is B or 1 and analysis alone is considered sufficient.

Validation tests shall be planned and implemented in a logical manner. In particular:

a) a test plan shall be produced before testing begins that shall include

   1) the test specifications;

   2) the required outcome of the tests for compliance, and

3) the chronology of the tests, if applicable;

b) test records shall be produced that include:

1) the name of the person carrying out the test;

2) the environmental conditions;

3) the test procedures and equipment used;

4) the date of the test, and

5) the results of the test;

c) the test records shall be compared with the test plan to ensure that the specified functional and performance targets are achieved.

The test sample shall be operated as near as possible to its final operating configuration, i.e. with all peripheral devices and covers attached.

This testing may be applied manually or automatically, e.g. by computer.

Where applied, validation of the safety functions by testing shall be carried out by applying input signals, in various combinations, to the SRP/CS. The resultant response at the outputs shall be compared to the appropriate specified outputs.

The combination of these input signals should be applied systematically to the control system and the machine, e.g. power-on, start-up, operation, directional changes and restart-up. An expanded range of input data should be applied to take into account anomalous or unusual situations, in order to see how the SRP/CS responds. Such combinations of input data should take into account foreseeable incorrect operation(s).

When validation by analysis is not conclusive, testing shall be carried out to complete the validation. Testing is always complementary to analysis and is often necessary.

10.4.2 Measurement accuracy

The accuracy of measurements during the validation by testing shall be appropriate for the test carried out. In general, these measurement accuracies shall be within 5 K for temperature measurements and 5 % for the following:

a) time measurements;

b) pressure measurements;

c) force measurements;

d) electrical measurements;

e) relative humidity measurements;

f) linear measurements.

Deviations from these measurement accuracies shall be justified.

10.4.3 Additional requirements for testing

If the SRP/CS needs to fulfil more stringent requirements than those within this document, the testing must be extended to cover these more stringent requirements as well.

NOTE Depending on the risk assessment more stringent requirements can apply if the control system has to withstand particularly adverse service conditions, e.g. rough handling, humidity effects, hydroxylation, ambient temperature variations, effects of chemical agents, corrosion, and high strength of electromagnetic fields; for example, due to close proximity of transmitters.

10.4.4 Number of test samples

Unless otherwise specified in the test specification, the tests shall be made on a single production sample of the subsystem being tested.

Subsystem(s) under test shall not be modified during the course of the tests.

Certain tests can permanently change the performance of some components. Where a permanent change in a component causes the safety-related part to be incapable of meeting the requirements of further tests, a new sample or samples shall be used for subsequent tests.

Where a particular test is destructive and equivalent results can be obtained by testing part of SRP/CS in isolation, a sample of that part of the SRP/CS may be used instead of the whole SRP/CS for the purpose of obtaining the results of the test. This approach shall only be applied where it has been shown by analysis that testing of a part of SRP/CS is sufficient to demonstrate the safety integrity of the whole SRP/CS that performs the safety function.

10.4.5 Testing methods

Depending on the application, different testing methods shall be used to validate the SRP/CS. In some applications it can be necessary to divide the connected safety-related parts into several functional groups and to subject these groups and their interfaces to fault simulation tests. The precise instant at which a fault is injected into a system can be critical. The worst-case effect of a fault injection shall be determined by analysis and by injecting the fault at this appropriate critical time. Common test methods are:

a) simulation of control system behaviour in the event of a fault, e.g. by means of hardware and/or software models;

b) software simulation of faults;

c) functional testing of the safety functions in all operating modes of the machine, to establish whether they meet the specified characteristics (see Clause 5). the functional tests shall ensure that all safety-related outputs are realized over their complete ranges and respond to safety-related input signals in accordance with the specification. The test cases are normally derived from the specifications but could also include some cases derived from analysis of the schematics or software;

d) extended functional testing to check foreseeable abnormal signals or combinations of signals from any input source, including power interruption and restoration, and incorrect operations;

e) fault injection tests on the actual circuit and fault initiation on actual components, particularly in parts of the system where there is doubt regarding the results obtained from failure analysis;

f) fault injection tests into a production sample;

g) fault injection tests into a hardware model;

h) subsystem failure test (e.g. power supplies).

10.5 Validation of the safety functions

The validation of safety functions shall demonstrate that the SRP/CS, or combination of subsystems, provides the safety function(s) in accordance with their specified characteristics.

Validation of the specified characteristics of the safety functions shall be achieved by the application of appropriate measures from the following list:

a) Functional analysis of schematics, reviews of the software (see 10.6.3).

NOTE Where a machine has complex or a large number of safety functions, an analysis can reduce the number of functional tests required.

b) Simulation.

c) Check of the hardware components installed in the machine and details of the associated software to confirm their correspondence with the documentation (e.g. manufacture, type, version).

d) Functional testing of the safety functions in all operating modes of the machine, to establish whether they meet the specified characteristics (see Clause 6). The functional tests shall ensure that all safety-related outputs are realized over their complete ranges and respond to safety-related input signals in accordance with the specification. The test cases are normally derived from the specifications but could also include some cases derived from analysis of the schematics or software.

e) Extended functional testing to check foreseeable abnormal signals or combinations of signals from any input source, including power interruption and restoration, and incorrect operations.

f) Check of the operator-SRP/CS interface for the meeting of ergonomic principles.

10.6 Validation of the safety integrity of the SRP/CS

10.6.1 Validation of subsystem(s)

The safety integrity of each subsystem of the SRP/CS shall be validated by confirming the requirements of Table 10 according to the category used.

Table 10 — Basic requirements for categories to be validated

Requirements	Category				
	B	1	2	3	4
Basic safety principles	X	X	X	X	X
Expected operating stresses	X	X	X	X	X
Influences of processed material	X	X	X	X	X
Performance during other relevant external influences	X	X	X	X	X
Well-tried components	—	X	—	—	—
Well-tried components for the case of determination the PL without $MTTF_D$	—	X	X	X	X
Well-tried safety principles	—	X	X	X	X
$MTTF_D$ of each channel	X	X	X	X	X
The check procedure of the safety function(s)	—	—	X	—	—
The recognizable faults and the associated diagnostic measures, including fault reaction	—	—	X	X	X
Checking intervals, when specified	—	—	X	X	X
DC_{avg}	—	—	X	X	X
X required — not required NOTE The categories are those given in 6.1.3.2.					

Table 10 *(continued)*

Requirements	Category				
	B	1	2	3	4
CCF identified and how to prevent them	—	—	X	X	X
Justification for fault exclusion	X	X	X	X	X
How the safety function is maintained in the case of each of the faults	—	—	—	X	X
How the safety function is maintained for each of the combinations of faults	—	—	—	—	X
Measures against systematic failures	X	X	X	X	X
Measures against software faults	X	—	X	X	X
X required — not required					
NOTE The categories are those given in 6.1.3.2.					

In addition the safety integrity of each subsystem of the SRP/CS shall be validated by confirming:

— the probability of dangerous random hardware failure and

— the systematic integrity (see Annex G, Software, CCF).

In this context the validation of $MTTF_D$, DC_{avg} and CCF is typically performed by analysis and visual inspection.

The $MTTF_D$ values for components (including B_{10D}, T_{10D} and n_{op} values) shall be checked for plausibility. Where fault exclusion claims mean that particular components do not contribute to the channel $MTTF_D$, the plausibility of the fault exclusion shall be checked.

NOTE 1 A fault exclusion implies infinite $MTTF_D$; therefore, fault excluded failure modes of the component does not contribute to the calculation of channel $MTTF_D$.

The $MTTF_D$ of each channel of the subsystem, including application of the symmetrisation formula (see Annex D) to dissimilar redundant channels, shall be checked for correct calculation. $MTTF_D$ of individual channels shall be restricted to no greater than 100 years (2 500 years for category 4) before the symmetrisation formula is applied.

The DC values for components (subsystem elements) and/or logic blocks shall be checked for plausibility (e.g. against measures in Annex E). The correct implementation (hardware and software) of checks and diagnostics, including appropriate fault reaction, shall be validated by testing under typical environmental conditions in use.

The correct implementation of sufficient measures against common-cause failures shall be validated (e.g. Annex F). Typical validation measures are static hardware analysis and functional testing under environmental conditions.

NOTE 2 Generally for the specification of the $MTTF_D$ values of electronic components, an ambient temperature of +40 °C is taken as a basis. During validation, it is important to ensure that, for $MTTF_D$ values, the environmental and functional conditions (in particular temperature) taken as basis are met. Where a device, or component, is operated significantly above the specified temperature of +40 °C, it is necessary to use $MTTF_D$ values for the increased ambient temperature.

10.6.2 Validation of measures against systematic failures

The validation of measures against systematic failures can typically be provided by:

a) inspections of design documents which confirm the application of

   — basic and well-tried safety principles (see ISO 13849-2:2012, Annex A to Annex D);

   — further measures for avoidance of systematic failures according to Annex G, and

— further measures for the control of systematic failures such as hardware diversity, modification protection or failure assertion programming;

b) failure analysis (e.g. FMEA);

c) fault injection tests/fault initiation;

d) inspection and testing of data communication, where used;

e) checking that a quality management avoid in the causes of systematic failures in the manufacturing process.

NOTE 1 Systematic faults can be caused by errors made during the design and integration stages (a misinterpretation of the safety function characteristics, an error in the logic design, an error in hardware assembly, an error in typing the code of software). Some of these error will be revealed during the design process, while others are revealed during the validation process or are remain unnoticed. In addition, it is possible for an error to be made (e.g. failure to check a characteristic) during the validation process.

10.6.3 Validation of safety-related software

The validation of software shall include:

— the specified functional behaviour and performance criteria (e.g. timing performance) of the software when performed on the target hardware,

— verification that the software measures are sufficient for the specified PL_r of the safety function, and

— verification that the protective measures and activities planned to be taken during software development to avoid systematic software faults have been employed, by inspecting the documented evidence.

As a first step, check that there is documentation for the specification and design of the safety-related software. This documentation shall be reviewed for completeness and absence of erroneous interpretations, omissions or inconsistencies.

In general, software can be considered a “black box” or “grey box” (see Clause 7) and validated by the black- or grey-box test, respectively.

NOTE 1 In the case of small programs, an analysis of the program by means of reviews or walk-through of control flow, procedures, using the software documentation (control flow chart, source code of modules or blocks, I/O and variable allocation lists, cross-reference lists) can be sufficient.

NOTE 2 Black-box testing aims to check the dynamic behaviour under real functional conditions, and to reveal failures to meet functional specification, and to assess utility and robustness. Grey-box testing is similar to black-box testing but additionally monitors relevant test parameter(s) inside the software module.

Depending on the PL_r the tests should include:

— black-box or grey box testing of functional behaviour and performance (e.g. timing performance),

— additional extended test cases based upon limit value analyses, recommended for PL d or PL e,

— I/O tests to ensure that the safety-related input and output signals are used properly, and

— test cases which simulate faults determined analytically beforehand, together with the expected response, in order to evaluate the adequacy of the software-based measures for control of failures.

Individual software functions which have already been validated do not need to be validated again. Where a number of such safety function blocks are combined for a specific project, however, the resulting total safety function shall be validated.

The measures for software implementation and configuration and modification management according to Clause 7, which depend on the PL to be attained, shall be examined with regard to their proper implementation.

Should the safety-related software be subsequently modified, it shall be revalidated on an appropriate scale.

10.6.4 Validation of combination of subsystems

Where the safety function is implemented by two or more subsystems, validation of the combination – by analysis and by testing – shall be undertaken to establish that the combination achieves the safety integrity specified in the design. Existing recorded validation results of subsystems can be taken into account. The following validation steps shall be performed:

— inspection of design documents describing the overall safety function(s);

— a check that the overall PL of the subsystem combination has been correctly evaluated, based on the PL of each individual subsystem (according to 6.2);

— consideration of the characteristics of the interfaces, e.g. voltage, current, pressure, data format of information, signal level;

— failure analysis relating to combination/integration, e.g. by FMEA;

— ftesting of the subsystem combination;

— for redundant systems, fault injection tests relating to combination/integration.

10.6.5 Overall validation of safety integrity

The following steps shall be performed:

— checking/verification for correct evaluation of PL, based on PFH_D and PL/SIL of subsystems (see 7.2).

— checking/verification for correct evaluation of PL based on the category, DC_{avg} and $MTTF_D$, CCF and measures against systematic failures;

— checking/verification that the PL achieved by the SRP/CS satisfies the PL_r in the safety requirements specification for the machinery: $PL \geq PL_r$.

10.7 Validation of environmental requirements

The performance specified in the design of the SRP/CS shall be validated with respect to the environmental conditions specified for the control system.

Validation shall be carried out by analysis and, if necessary, by testing. The extent of the analysis and of the testing will depend upon the safety-related parts, the system in which they are installed, the technology used, and the environmental condition(s) being validated. The use of operational reliability data on the system or its components, or the confirmation of compliance to appropriate environmental standards (e.g. for waterproofing, vibration protection) can assist this validation process.

Where applicable, validation shall address

— expected mechanical stresses from shock, vibration, ingress of contaminants,

— mechanical durability,

— electrical ratings and power supplies,

— climatic conditions (temperature and humidity), and

— electromagnetic compatibility (immunity).

When testing is needed to determine compliance with the environmental requirements, the procedures outlined in the relevant standards shall be followed as far as required for the application.

After the completion of validation by testing, the safety functions shall continue to be in accordance with the specifications for the safety requirements, or the SRP/CS shall provide output(s) for a safe state.

10.8 Validation record

Validation by analysis and testing shall be recorded. The record shall demonstrate the validation process for each of the safety requirements. Cross-reference may be made to previous validation records, provided they are properly identified.

For any safety-related part which has failed an element of the validation process, the validation record shall describe which elements in the validation analysis/testing have been failed. It shall be ensured that all safety-related parts are successfully re-validated after modification.

10.9 Validation maintenance requirements

The validation process shall demonstrate that the provisions for maintenance requirements have been implemented.

Validation of maintenance requirements shall include the following, as applicable:

a) a review of the information for use confirming that

   1) maintenance instructions are complete [including procedures, required tools, frequency of inspections, time interval for changing components subjected to wear (T_{10d}) etc.] and understandable,

   2) if appropriate, there are provisions for the maintenance to be performed only by skilled maintenance personnel;

b) a check that measures for ease of maintainability (e.g. provision of diagnostic tools to aid fault-finding and repair) have been applied.

In addition, the following measures shall be included when applied:

— measures against mistakes during maintenance (e.g. detection of wrong input data via plausibility checks);

— measures against modification (e.g. password protection to prevent access to the program by unauthorized persons).

11 Maintainability of SRP/CS

Preventive or corrective maintenance can be necessary to maintain the specified performance of the SRP/CS.

NOTE Exceeding specified lifetime or test interval can lead to deterioration in safety or to a hazardous situation.

When designing an SRP/CS, the following factors shall be taken into account to enable maintenance of the SRP/CS:

— accessibility, taking into account the environment and the human body measurements, including the dimensions of the working clothes and tools used;

— ease of handling, taking into account human capabilities;

— limitation of the number of special tools and equipment for those applications where special;

— indication(s) that maintenance is necessary (e.g. increased vibration) ideally with automated generation of warning signals (e.g. lifetime recording, self-test, monitoring of process parameters);

— required illumination levels.

12 Technical documentation

When designing an SRP/CS according to this document at least the following information relevant to the safety-related part shall be documented for internal purpose:

a) safety requirements specification including the specification of each safety function (see 5.2.1);

b) exact points at which the safety-related part(s) start and end;

c) decomposition into subsystems (see 5.2.2), if applicable;

d) environmental conditions (e.g. EMC immunity, temperature, vibration);

e) achieved performance level and PFH_D value;

f) category or categories selected (may not be applicable for previously validated subsystems);

g) parameters relevant to the reliability ($MTTF_D$, DC, CCF and T_{10D}) and the mission;

h) measures against systematic failure;

i) the technology or technologies used;

j) the safety-relevant faults considered;

k) justification for fault exclusions (see 6.1.10.3 and all annexes of ISO 13849-2:2012);

l) software documentation if applicable;

m) measures against reasonably foreseeable misuse;

n) safety-related block diagram;

o) test, verification and validation records, where applicable.

NOTE In general, this documentation is foreseen as being for the manufacturer's internal purposes and is not be distributed to the machine user.

13 Information for use

13.1 General

The information for use of the SRP/CS shall include all relevant instructions for the intended target groups. The lifecycle phases of the machine where an SRP/CS is involved shall be covered by this information.

13.2 Information for SRP/CS integration

The information which is important for the correct integration of SRP/CS shall be given to the integrator. This shall include, but is not limited to the following:

a) limits (e.g. environmental conditions) appropriate information to ensure the continued justification of the fault exclusions, e.g. regarding modification, maintenance and repair;

b) clear descriptions of the interfaces to the SRP/CS and protective devices;

c) response time;

d) operating limits (e.g. demand frequency);

e) indications and alarms;

f) muting and suspension of safety functions;

g) control modes and reset;

h) maintenance (see Clause 11);

i) maintenance check lists;

j) how to access and replace the parts of SRP/CS;

k) means for easy and safe trouble shooting;

l) test intervals where relevant;

m) mission time (e.g. ISO 13855:2010).

NOTE The integrator can be a manufacturer, assembler, engineering company or the user.

Specific information for each safety function on categories and performance level shall be provided (see 5.3), as follows:

— dated reference to this document (i.e. “ISO 13849-1:2022”);

— the categories of the subsystems forming the SRP/CS;

— the performance level, a, b, c, d or e;

— the PFH_D value for SRP/CS, if relevant for subsystem(s).

13.3 Information for user

The information which is important for the correct use of SRP/CS shall be given to the user.

This can include, but is not limited to, the relevant aspects of 13.1 and 13.2. Also relevant information with respect to testing of the safety functions shall be provided. The designer of the SRP/CS shall provide information for use that describes the necessary maintenance tasks for the SRP/CS.

Information for maintenance can include tasks and applications, for example:

a) setting;

b) teaching/programming;

c) process /tool changeover;

d) cleaning;

e) preventive maintenance;

f) corrective maintenance;

g) troubleshooting/fault finding;

h) nature and frequency of inspections and safety functions;

i) instructions relating to maintenance operations which require technical knowledge and/or particular skills and hence should be carried out exclusively by qualified personnel (e.g. maintenance staff, specialists);

j) instructions relating to maintenance actions (e.g. replacement of parts) which do not require specific skills and hence may be carried out by users (e.g. operators). It should be brought to the attention of maintenance staff which parts are critical to safety and must only be replaced with "like" parts or similar. In cases of non-identical parts being used to replace safety critical components, a revalidation of the safety function will likely be required;

k) controlling hazardous energy (manual measures/other means) guidance, signs, and devices;

l) drawings/diagrams enabling maintenance personnel to perform their tasks (especially fault-finding tasks to isolate conditions that caused the fault);

m) information about replacement of components at or before the T_{10D} period ends (see also C.4.2).

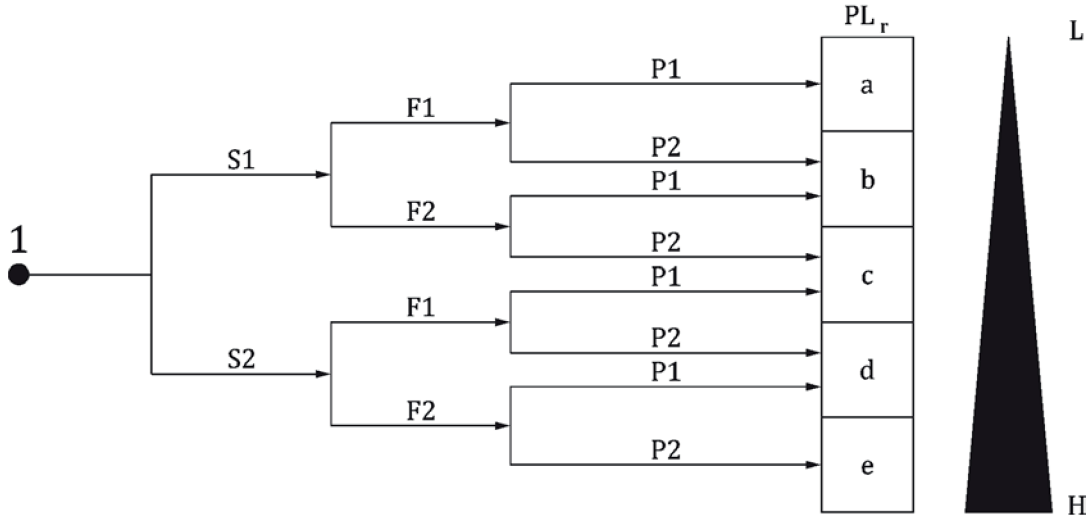
NOTE For additional information see ISO 20607:2019 and IEC 60204-1:2016, 17.2, f.

If any maintenance activity requires the modification of an SRP/CS this will then require a functional test of the relevant safety functions.

Annex A
(informative)

Guideline for the determination of required performance level

A.1 General



Key

1 starting point for evaluation of safety function's contribution to risk reduction
L low contribution to risk reduction
H high contribution to risk reduction
PL_r required performance level

Risk parameters:

S severity of injury
S1 slight (normally reversible injury)
S2 serious (normally irreversible injury or death)
F frequency and/or exposure to hazard
F1 seldom-to-less-often and/or exposure time is short
F2 frequent-to-continuous and/or exposure time is long
P possibility of avoiding the hazard or limiting harm
P1 possible under specific conditions
P2 scarcely possible

Figure A.1 — Graph for determining PL_r for safety function

Figure A.1 provides guidance for the determination of the safety-related PL_r for the safety function. The graph should be considered for each safety function.

A.2 Selection of required performance level

Annex A is concerned with the contribution to the risk reduction made by the safety-related parts of the control system being considered. The method given in this clause is based on the estimation of risk parameters (which is by nature partly subjective as for any other risk estimation method). Therefore, this method is only a guidance to machine designers and standard makers for estimating the PL_r for each safety function to be carried out by an SRP/CS.

NOTE This methodology to estimate the PL_r is not mandatory. It is a generic approach which assumes a worst case probability of occurrence of a hazardous event (the probability of occurrence is 100 %). In cases where the probability of occurrence can be assessed as low, a downgrade by one performance level is possible. Other risk estimation methods for specific types of machine can be used as appropriate and experience in successfully dealing with similar machines/hazards should be taken into account when estimating PL_r. Therefore, the PL required by a type-C standard can deviate from that indicated by the generic approach given at Figure A.1.

The graph in Figure A.1 is based on the situation prior to the provision of the intended safety function (see also ISO/TR 22100-2:2013). Risk reduction by technical measures independent of the control system (e.g. mechanical guards), or additional safety functions, are to be taken into account in determining the PL_r of the intended safety function; in which case, the starting point of Figure A.1 is selected after the implementation of these measures (see also Figure 4).

These parameters used in determining the PL_r are

— severity of injury (S)

— frequency and time of exposure to the hazard (F),

— possibility of avoiding the hazard or limiting the harm (P).

Experience has shown that these parameters can be combined, as in Figure A.1, to give a gradation of the contribution to required risk reduction from low to high. It is emphasized that this is a qualitative process giving only an estimation of a required performance level.

A.3 Guidance for selecting parameters S, F and P for the risk estimation

A.3.1 Severity of injury S1 and S2

In estimating the risk, only slight injuries or serious injuries are considered.

To make a decision the usual consequences of accidents and normal healing processes should be taken into account in determining S1 and S2. For example, bruising and/or lacerations without complications would be classified as S1, whereas amputation or death would be S2.

NOTE For guidance about the evaluation of severe or slight injury see also ISO/TR 14121-2.

A.3.2 Frequency and/or exposure times to hazard, F1 and F2

A generally valid time period to be selected for parameter F1 or F2 cannot be specified. However, the following explanation could facilitate making a decision where doubt exists.

F2 should be selected if a person is frequently or continuously exposed to the hazard. It is irrelevant whether the same or different persons are exposed to the hazard on successive exposures, e.g. for the use of lifts. The frequency parameter should be chosen according to the frequency and duration of access to the hazard.

Where the demand on the safety function is known by the designer, the frequency and duration of this demand can be chosen instead of the frequency and duration of access to the hazard. In this document, the frequency of demand on the safety function is assumed to be more than once per year.

The period of exposure to the hazard should be evaluated on the basis of an average value which can be seen in relation to the total period of time over which the equipment is used. For example, if it is

necessary to reach regularly between the tools of the machine during cyclic operation in order to feed and move work pieces, then F2 should be selected.

In case of no other justification, F2 should be chosen if the frequency is higher than once per 15 min.

F1 may be chosen if the accumulated exposure time does not exceed 1/20 of the overall operating time and the frequency is not higher than once per 15 min.

A.3.3 Possibility of avoiding hazard or limiting harm

It is important to know whether a hazardous event can be recognized before it can cause harm and be avoided. For example, can the exposure to a hazard be directly identified by its physical characteristics, or recognized only by technical means, e.g. indicators. Other important aspects which influence the selection of parameter P include, for example:

a) speed with which the hazard arises (e.g. quickly or slowly);

b) possibilities for hazard avoidance (e.g. by escaping);

c) practical safety experiences relating to the process;

d) whether operated by trained and suitable operators;

e) operated with or without supervision.

When a hazardous event occurs, P1 should only be selected if there is a realistic possibility of avoiding a hazard or of significantly reducing its effect; otherwise P2 should be selected.

The parameter P can be determined by the following approach:

— determine the letter of each factor of the Table A.1 that reflects the specific application (only one choice for each factor is possible);

— count the number of chosen letters “A”, “B” and “C”;

— determine the correspond value of the parameter P in Table A.2.

Only one choice for each factor is possible in Table A.1.

Table A.1 — Determination of parameter P based on five factors

Factor	C	B	A
1. use of the machine by		unskilled person	skilled person
2. speed of the part of the machine that can create a hazardous event (depending on the specific machine and time to escape from or to avoid a hazardous situation (hot/cold surface, radiation etc.)	high speed event no time to escape e.g. due to high speed e.g. above 1 000 mm/s, time to hazard <1 s	medium speed event limited time to escape, e.g. due to medium speed e.g. 251 mm/s to 1 000 mm/s, time to hazard <3 s	low or very low speed event enough time to escape, e.g. due to low speed e.g. max of 250 mm/s, time to hazard ≥ 3 s
3. spatial possibility to withdraw from the hazard	not possible	possible in less than 50 % of the cases	possible in more or equal to 50 % of the cases
NOTE Any numbers in this table are purely indicative and might be different in type-C standards or based on the specific machine application.			

Table A.1 *(continued)*

Factor	C	B	A
4. possibility of recognition/awareness of the hazard	not possible e.g. instrumentation necessary, humans sense are not able to perceive the hazard, environmental conditions hide the perception	possible only in less than 50 % of the cases	possible in more or equal to 50 % of the cases
5. complexity of the operations (human interaction in terms of numbers of operation and/or timing available for this operations)		high complexity e.g. troubleshooting or medium complexity e.g. use hold-to-run control to setup a part of the machine	low complexity e.g. adjust the workpiece clamps, or very low complexity / or no interaction e.g. put a workpiece into the machine
NOTE Any numbers in this table are purely indicative and might be different in type-C standards or based on the specific machine application.			

Table A.2 — Selection of parameter P1 or P2

Overall score		Parameter "P"
one or more "C"		P2
no "C", three or more "B"		P2
no "C", two "B", the rest "A"		P1 or P2 depending on the specific hazard
no "C", one or no "B", the rest "A"		P1

P1 should only be selected if there is a realistic possibility of avoiding a hazard or of significantly reducing its effect; otherwise P2 should be selected.

13.4 Overlapping hazards

When using ISO 13849-1, all hazards are considered as a specific hazard or hazardous situation. Each hazard can therefore be evaluated separately.

When it is obvious that there is a combination of directly linked hazards which always occur simultaneously then they should be combined during risk estimation.

The determination of whether hazards should be considered separately or in combination should be considered during the risk assessment of the machine.

EXAMPLE 1 A continuous welding robot can create various simultaneous hazardous situations, for example crushing caused by movement and burning due to the welding process. This can be considered as a combination of directly linked hazards.

EXAMPLE 2 For a robot cell in which separate robots are working, for the cell areas where only one robot can create at the same time a hazard the robots can be considered separately.

EXAMPLE 3 As a result of a risk assessment it can be sufficient for a rotary table with clamping devices to consider each clamping device separately.

Annex B
(informative)

Block method and safety-related block diagram

B.1 Block method

The simplified approach requires a block-oriented logical representation of the subsystem. The subsystem should be separated into a small number of blocks according to the following:

a) blocks should represent logical units of the subsystem related to the execution of the safety function;

b) different channels performing the sub-function should be separated into different blocks

c) if one block is no longer able to perform its function, the execution of the sub-function through the blocks of the other channel should not be affected;

d) each channel may consist of one or several blocks – three blocks per channel in the designated architectures, input, logic and output, is not an obligatory number, but simply an example for a logical separation inside each channel;

e) each hardware unit of the subsystem should belong only to one block, thus allowing for the calculation of the $MTTF_D$ of the block based on the $MTTF_D$ of the hardware units belonging to the block (e.g. by failure mode and effects analysis or the parts count method, see D.1).

B.2 Safety-related block diagram

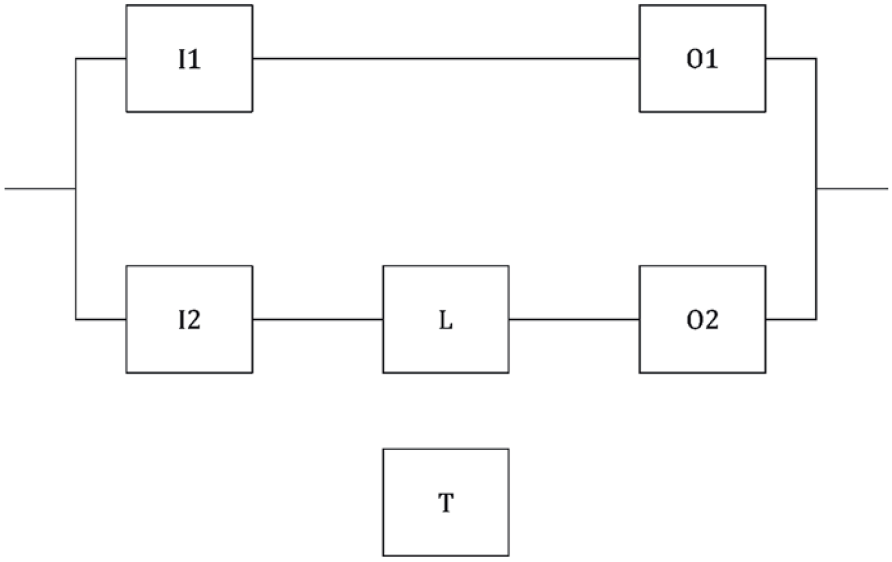
The blocks defined by the block method may be used to graphically represent the logical structure of the subsystem in a safety-related block diagram. For such a graphical representation, the following may be of guidance:

— the failure of one block in a series alignment of blocks leads to the failure of the whole channel (e.g. if one hardware unit in one channel of the subsystem fails dangerously, the whole channel might not be able to execute the sub-function any longer);

— only the dangerous failure of all channels in a parallel alignment leads to the loss of the sub-function (e.g. a sub-function performed by several channels is performed as long as at least one channel has no failure); common cause failures are capable of creating this type of condition (see 7.1.6 and Annex F and Annex G);

— blocks used only for testing purposes of cat 3 or cat 4 SRP/CS's that do not affect the execution of the sub-function when they fail dangerously may be separated from blocks in the different channels.

See Figure B.1 for an example.



Key

I1, I2	input devices, e.g. sensor
L	logic
O1, O2	output devices, e.g. main contactor
T	testing device
I1 and O1	build up the first channel (series alignment)
I2, L and O2	build up the second channel (series alignment); with both channels executing the sub-function redundantly (parallel alignment)
T	Used for testing only

Figure B.1 — Example of safety-related block diagram

Annex C
(informative)

Calculating or evaluating $MTTF_D$ values for single components

C.1 General

Annex C gives several methods for calculating or evaluating $MTTF_D$ values for single components: the method given in C.2 is based on the application of good engineering practices for the different kinds of components; that given in C.3 is applicable to hydraulic components; C.4 provides a means of calculating the $MTTF_D$ of pneumatic, mechanical and electromechanical components from B_{10} (see C.4.1); C.5 lists $MTTF_D$ values for electrical components.

C.2 Good engineering practices method

If the following criteria are met, the $MTTF_D$ or B_{10D} value for a component can be estimated according to Table C.1.

a) The components are manufactured according to basic and well-tried safety principles in accordance with ISO 13849-2:2012, or the relevant standard (see Table C.1) for the design of the component.

   NOTE This information can be found in the data sheet of the component manufacturer.

b) The manufacturer of the component specifies the appropriate application and operating conditions for the SRP/CS designer.

c) The design of the SRP/CS fulfils the basic and well-tried safety principles according to ISO 13849-2:2012, for the implementation and operation of the component.

Table C.1 — International Standards dealing with $MTTF_D$ or B_{10D} for components

	Basic and well-tried safety principles according to ISO 13849-2:2012	Relevant standards	Typical values: $MTTF_D$ (years) B_{10D} (cycles)
mechanical components	Table A.1 and Table A.2	—	$MTTF_D$ = 150
hydraulic components with n_{op} ≥ 1 000 000 cycles per year[a]	Table C.1 and Table C.2	ISO 4413	$MTTF_D$ = 150
hydraulic components with 1 000 000 cycles per year > n_{op} ≥ 500 000 cycles per year [a]	Table C.1 and Table C.2	ISO 4413	$MTTF_D$ = 300

For the definition and use of B_{10D}, see C.4.

NOTE 1 B_{10D} is estimated as two times B_{10} (50 % dangerous failure) if no other information (e.g. product standard) is available.

"Nominal load" or "small load" should take into account safety principles described in ISO 13849-2:2012, like over-dimensioning of the rated current value. "Small load" means, for example, 20 %.

NOTE 2 Emergency stop devices according to IEC 60947-5-5 and ISO 13850 and enabling switches according to IEC 60947-5-8 can be estimated as a category 1 or category 3/4 subsystem depending on the number of electrical output contacts and on the fault detection in the subsequent subsystem. Each contact element (including the mechanical actuation) can be considered as one channel with a respective B_{10D} value. For enabling switches according to IEC 60947-5-8 this implies the opening function by pushing through or by releasing. In some cases, it is possible that the machine builder can apply fault exclusion according to ISO 13849-2:2012, Table D.8, considering the specific application and environmental conditions of the device.

NOTE 3 Reducing off switching cycles can lead to an increasing probability of sticking of the switching elements in spool valves (see ISO 4413).

NOTE 4 The $MTTF_D$ for mechanical components refers exclusively to mechanically moving components/parts (not to housing).

[a] B_{10d} calculation for hydraulic components is not permitted as a reverse calculation from standard $MTTF_D$ values.

[b] If fault exclusion for direct opening action is possible.

[c] In general, this value can be assumed for most pneumatic components. However, depending on the application and type, e.g. shut-off valve, this value can be significantly lower.

Table C.1 *(continued)*

	Basic and well-tried safety principles according to ISO 13849-2:2012	Relevant standards	Typical values: $MTTF_D$ (years) B_{10D} (cycles)
hydraulic components with 500 000 cycles per year > n_{op} ≥ 250 000 cycles per year[a]	Table C.1 and Table C.2	ISO 4413	$MTTF_D$ = 600
hydraulic components with n_{op}[a] < 250 000 cycles per year	Table C.1 and Table C.2	ISO 4413	$MTTF_D$ = 1 200
pneumatic components	Table B.1 and Table B.2	ISO 4414	B_{10D} = 20 000 000[c]
relays and contactor relays with small load	Table D.1 and Table D.2	IEC 61810-3 IEC 60947	B_{10D} = 20 000 000
relays and contactor relays with nominal load	Table D.1 and Table D.2	IEC 61810-3 IEC 60947	B_{10D} = 400 000
proximity switches with small load	Table D.1 and Table D.2	IEC 60947 ISO 14119	B_{10D} = 20 000 000
proximity switches with nominal load	Table D.1 and Table D.2	IEC 60947 ISO 14119	B_{10D} = 400 000
contactors with small load	Table D.1 and Table D.2	IEC 60947	B_{10D} = 20 000 000
contactors with nominal load	Table D.1 and Table D.2	IEC 60947	B_{10D} = 1 300 000
position switches[b]	Table D.1 and Table D.2	IEC 60947 ISO 14119	B_{10D} = 20 000 000
position switches (with separate actuator, guard-locking)[b]	Table D.1 and Table D.2	IEC 60947 ISO 14119	B_{10D} = 2 000 000
emergency stop devices[b]	Table D.1 and Table D.2	IEC 60947 ISO 13850	B_{10D} = 100 000
push buttons (e.g. enabling switches)[b]	Table D.1 and Table D.2	IEC 60947	B_{10D} = 100 000

For the definition and use of B_{10D}, see C.4.

NOTE 1 B_{10D} is estimated as two times B_{10} (50 % dangerous failure) if no other information (e.g. product standard) is available.

"Nominal load" or "small load" should take into account safety principles described in ISO 13849-2:2012, like over-dimensioning of the rated current value. "Small load" means, for example, 20 %.

NOTE 2 Emergency stop devices according to IEC 60947-5-5 and ISO 13850 and enabling switches according to IEC 60947-5-8 can be estimated as a category 1 or category 3/4 subsystem depending on the number of electrical output contacts and on the fault detection in the subsequent subsystem. Each contact element (including the mechanical actuation) can be considered as one channel with a respective B_{10D} value. For enabling switches according to IEC 60947-5-8 this implies the opening function by pushing through or by releasing. In some cases, it is possible that the machine builder can apply fault exclusion according to ISO 13849-2:2012, Table D.8, considering the specific application and environmental conditions of the device.

NOTE 3 Reducing off switching cycles can lead to an increasing probability of sticking of the switching elements in spool valves (see ISO 4413).

NOTE 4 The $MTTF_D$ for mechanical components refers exclusively to mechanically moving components/parts (not to housing).

[a] B_{10d} calculation for hydraulic components is not permitted as a reverse calculation from standard $MTTF_D$ values.

[b] If fault exclusion for direct opening action is possible.

[c] In general, this value can be assumed for most pneumatic components. However, depending on the application and type, e.g. shut-off valve, this value can be significantly lower.

C.3 Hydraulic components

If the following criteria are met, the $MTTF_D$ value for a single hydraulic component, e.g. valve, can be estimated at 150 years. If the mean number of annual operations (n_{op}) is below 1 000 000 cycles per year, then the $MTTF_D$ value can be estimated higher as shown in Table C.1:

a) The hydraulic components are manufactured according to basic and well-tried safety principles in accordance with ISO 13849-2:2012, Table C.1 and Table C.2, for the design of the hydraulic component (confirmation in the data sheet of the component).

b) The manufacturer of the hydraulic component specifies the appropriate application and operating conditions for the SRP/CS designer. The SRP/CS designer should provide information pertaining to their responsibility to apply the basic and well-tried safety principles according to

ISO 13849-2:2012, Table C.1 and Table C.2, for the implementation and operation of the hydraulic component.

But if either a) or b) is not achieved, the $MTTF_D$ value for the single hydraulic component should be given by the manufacturer. Instead of using a fixed value for the $MTTF_D$ as described above it is permissible to use the B_{10D} concept for $MTTF_D$ of pneumatic, mechanical and electromechanical components also for hydraulic components if the manufacturer can provide data, e.g., B_{10}, B_{10D}, T_{10}, T_{10D}.

C.4 $MTTF_D$ of pneumatic, mechanical and electromechanical components

C.4.1 General

For pneumatic, mechanical and electromechanical components (pneumatic valves, relays, contactors, position switches, cams of position switches,.) it may be difficult to calculate the mean time to dangerous failure ($MTTF_D$ for components), which is given in years and which is required by this document. Most of the time, the manufacturers of these kinds of components only give the mean number of cycles until 10 % of the components fail (B_{10}) or fail dangerously (B_{10D}). This clause gives a method for calculating a $MTTF_D$ for components by using B_{10} or T (lifetime) given by the manufacturer related closely to the application dependent cycles.

If all the following criteria are met, the $MTTF_D$ value for a single pneumatic, electromechanical or mechanical component can be estimated according to C.4.2.

a) The components are designed and manufactured according to basic safety principles in accordance with ISO 13849-2:2012, Table A.1, Table B.1 or Table D.1.

   NOTE 1 This information can be found in the data sheet of the component manufacturer.

b) The components to be used in category 1, 2, 3 or 4 are designed and manufactured according to well-tried safety principles in accordance with ISO 13849-2:2012, Table A.2, Table B.2 or D.2.

   NOTE 2 This information can be found in the data sheet of the component manufacturer.

c) The manufacturer of the component specifies the appropriate application and operating conditions for the SRP/CS designer. The SRP/CS designer should provide information pertaining to their responsibility to fulfil the basic safety principles according to ISO 13849-2:2012, Table A.1, Table B.1 or Table D.1, for the implementation and operation of the component. For category 1, 2, 3 or 4, the user should be informed of their responsibility to fulfil the well-tried safety principles according to ISO 13849-2:2012, Table A.1, Table B.2 or Table D.2, for the implementation and operation of the component.

C.4.2 Calculation of $MTTF_D$ for components from B_{10D}

The mean number of cycles until 10 % of the components fail dangerously (B_{10D})[1)] should be determined by the manufacturer of the component in accordance with relevant product standards for the test methods (e.g. ISO 19973-series, IEC 60947-4-1, IEC 60947-5-1, IEC 60947-5-5, IEC 61810-2-1). The dangerous failure modes of the component should be defined, e.g. sticking at an end position or change

1) If the ratio of dangerous failure (RDF) of B_{10} is not given (e.g. by components manufacturer), 50 % of B_{10} can be used, so $B_{10D} = 2\ B_{10}$ is recommended.

of switching times. With B_{10D} and n_{op}, the mean number of annual operations, $MTTF_D$ for components can be calculated as

$$MTTF_D = \frac{B_{10D}}{0{,}1 \times n_{op}} \quad \text{(C.1)}$$

where

$$n_{op} = \frac{d_{op} \times h_{op} \times 3\,600 \text{s/h}}{t_{cycle}} \quad \text{(C.2)}$$

With the following assumptions having been made on the application of the component:

h_{op} is the mean operation, in hours per day;

d_{op} is the mean operation, in days per year;

t_{cycle} is the mean operation time between the beginning of two successive cycles of the component. (e.g. switching of a valve) in seconds per cycle.

The operating life time of the component is limited to T_{10D}, the mean time until 10 % of the components fail dangerously:

$$T_{10D} = \frac{B_{10D}}{n_{op}} \quad \text{(C.3)}$$

In case no B_{10D} is given by the manufacturer of the component, it is permitted to determine the B_{10D} by the formula (C.4)

$$B_{10D} = \frac{B_{10}}{RDF} \quad \text{(C.4)}$$

If the ratio of dangerous failures (RDF) given by the component manufacturer is estimated at less than 50% than T_{10D} value is limited to $T_{10} \times 2$.

When the T_{10D} value for a component is less than the mission time (20 years or less), the manufacturer responsible for the integration of the SRP/CS providing the safety function will inform the user to replace the component at or before the T_{10D} period ends. Limiting to T_{10D} the use of component allows maintaining the expected performance level of the safety function.

C.4.3 Explanation of the equations

The reliability methods in this document assume that the failure of components is distributed exponentially over time: $F(t) = 1 - e^{-\lambda_D t}$. For non-electronic components, a Weibull distribution is more likely, but if the operation time of the components is limited to the mean time until 10 % of the

components fail dangerously (T_{10D}) then a constant dangerous failure rate (λ_D) over this operation time can be estimated as

$$\lambda_D = \frac{0,1}{T_{10D}} = \frac{0,1 \times n_{op}}{B_{10D}} \quad \text{(C.5)}$$

Formula (C.6) takes into account that with a constant failure rate, 10 % of the components in the assumed application fail after T_{10D} [years], corresponding to B_{10D} [cycle]. To be exact:

$$F(T_{10D}) = 1 - e^{-\lambda_D T_{10D}} = 10\ \% \text{ means } \lambda_D = -\frac{\ln(0,9)}{T_{10D}} = \frac{0,10\ 536}{T_{10D}} \approx \frac{0,1}{T_{10D}} \quad \text{(C.6)}$$

With $MTTF_D = 1/\lambda_D$ for exponential distributions, this yields

$$MTTF_D = \frac{T_{10D}}{0,1} = \frac{B_{10D}}{0,1 \times n_{op}} \quad \text{(C.7)}$$

NOTE All variables used in the equations are physical quantities expressed as the product of a numerical value and a unit of measurement. The correct application of Formula (C.5), Formula (C.6) and MTTFD = 1/λD can require the transformation of "years" to "hours" using 1 year = 8 760 h.

C.4.4 Example

For a pneumatic valve, a manufacturer determines a mean value of 60 million cycles as B_{10D}. The valve is used for two shifts each day on 220 operation days a year. The mean time between the beginnings of two successive switching of the valve is estimated as 5 s. This yields the following values:

— d_{op} of 220 d per year;

— h_{op} of 16 h per day;

— t_{cycle} of 5 s per cycle;

— B_{10D} of 60 000 000 cycles.

With these input data the following quantities can be calculated:

$$n_{op} = \frac{220 \times 16 \times 3\ 600}{5s} = 2,53 \times 10^6 \text{ cycles/year} \quad \text{(C.8)}$$

$$T_{10D} = \frac{60 \times 10^6}{2,53 \times 10^6} = 23,7 \text{ years} \quad \text{(C.9)}$$

$$MTTF_D = \frac{23,7}{0,1} = 237 \text{years} \quad \text{(C.10)}$$

This calculation gives a $MTTF_D$ for the component "high" according to Table C.5. These assumptions are only valid for a restricted operation time of 23.7 years for the valve.

C.5 $MTTF_D$ data of electrical components

C.5.1 General

Table C.2 to Table C.7 indicate some typical average values of $MTTF_D$ for electronic components. The data are extracted from the SN 29500 series database[46]. All data are of general type. Various databases are available (see the non-exhaustive list in the Bibliography) which present $MTTF_D$ values for various electronic components. If the designer of an SRP/CS has other, reliable, specific data on the components used, then the use of that specific data instead is highly recommended.

The values given in Table C.2 to Table C.7 are valid for an ambient temperature of 40 °C, nominal load for current and voltage. A correction factor for $MTTF_D$ should be used where the electronic components operate outside the stated values for temperature; load. (see also SN 29500).

In the MTTF column of the tables, the values from SN 29500 are for generic components for all possible failure modes which are not necessarily dangerous failures. In the $MTTF_D$ column, it is typically assumed that not all failures modes lead to a dangerous failure. This depends mainly on the application. A precise way of determining the "typical" $MTTF_D$ for components is to carry out an FMEA. Some components, e.g. transistors used as switches, can have short circuits or interruptions as failure. Only one of these two modes can be dangerous; therefore the "remarks" column assumes only 50 % dangerous failure, which means that the $MTTF_D$ for components is twice the given MTTF value.

C.5.2 Semiconductors

See Table C.2 and Table C.3.

Table C.2 — Transistors (used as switches)

Transistor	Example	MTTF for components years	$MTTF_D$ for components years **Typical**	Remark
ipolar	TO18, TO92, SOT23	38 052	76 104	50 % dangerous failure
ipolar, low power	TO5, TO39	5 708	11 416	50 % dangerous failure
bipolar, power	TO3, TO220, D-Pack	1 903	3 806	50 % dangerous failure
FET	Junction MOS	22 831	45 662	50 % dangerous failure
MOS, power	TO3, TO220, D-Pack	1 903	3 806	50 % dangerous failure

Table C.3 — Diodes, power semiconductors and integrated circuits

Diode	Example	MTTF for components years	$MTTF_D$ for components years **Typical**	Remark
general purpose	—	114 155	228 311	50 % dangerous failure
suppressor	—	16 308	32 616	50 % dangerous failure
zener diode P_{tot} < 1 W	—	114 155	228 311	50 % dangerous failure
rectifier diodes	—	57 078	114 155	50 % dangerous failure
rectifier bridges	—	11 415	22 831	50 % dangerous failure
thyristors	—	2 283	4 566	50 % dangerous failure
triacs, diacs	—	1 522	3 044	50 % dangerous failure
integrated circuits (programmable and non-programmable)	use manufacturer's data			50 % dangerous failure

C.5.3 Passive components

See Table C.4 to Table C.7.

Table C.4 — Capacitors

Capacitor	Example	MTTF for components years	$MTTF_D$ for components years Typical	Remark
standard, no power	KS, KP, KC, KT, MKT, MKC, MKP, MKU, MP, MKV	57 078	114 155	50 % dangerous failure
ceramic	—	22 831	45 662	50 % dangerous failure
aluminium electrolytic	non-solid electrolyte	22 831	45 662	50 % dangerous failure
aluminium electrolytic	solid electrolyte	38 052	76 104	50 % dangerous failure
tantalum electrolytic	non-solid electrolyte	11 415	22 831	50 % dangerous failure
tantalum electrolytic	solid electrolyte	114 155	228 311	50 % dangerous failure

Table C.5 — Resistors

Resistor	Example	MTTF for components years	$MTTF_D$ for components years Typical	Remark
carbon film	—	114 155	228 311	50 % dangerous failure
metal film	—	570 776	114 1552	50 % dangerous failure
metal oxide and wire-wound	—	22 831	45 662	50 % dangerous failure
variable	—	3 805	7 610	50 % dangerous failure

Table C.6 — Inductors

Inductor	Example	MTTF for components years	$MTTF_D$ for components years Typical	Remark
for MC application	—	38 052	76 104	50 % dangerous failure
low frequency inductors and transformers	—	22 831	45 662	50 % dangerous failure
main transformers and transformers for switched modes and power supplies	—	11 415	22 831	50 % dangerous failure

Table C.7 — Optocouplers

Optocouplers	Example	MTTF for components years	$MTTF_D$ for components years Typical	Remark
bipolar output	SFH 610	7 610	15 220	50 % dangerous failure
FET output	LH 1056	2 854	5 708	50 % dangerous failure

Annex D
(informative)

Simplified method for estimating $MTTF_D$ for each channel

D.1 Parts count method

Use of the "parts count method" serves to estimate the $MTTF_D$ for each channel separately. The $MTTF_D$ values of all single components which are part of that channel are used in this calculation.

NOTE The parts count method is an approximation which always errs on the safe side.

The general Formula (D.1) is

$$\frac{1}{MTTF_D} = \sum_{i=1}^{N} \frac{1}{MTTF_{Di}} = \sum_{j=1}^{\tilde{N}} \frac{nj}{MTTF_{Dj}} \quad (D.1)$$

where

$MTTF_D$ is the mean time to dangerous failure for the complete channel;

$MTTF_{D\,I}$, $MTTF_{D\,j}$ is the $MTTF_D$ of each component which has a contribution to the sub-function; The first sum is over each component separately; the second sum is an equivalent, simplified form where all n_j identical components with the same $MTTF_{D\,j}$ are grouped together.

The example given in Table D.1 gives a $MTTF_D$ of the channel of 22.4 years, which is "medium" according to 6.1.4, Table 7.

Table D.1 — Example of the parts list of a circuit board

j	**Component**	**Units** n_j	$MTTF_{D\,j}$ typical years	$1/MTTF_{D\,j}$ typical 1/year	$n_j/MTTF_{D\,j}$ typical 1/year
1	transistors, bipolar, low power (see Table C.2)	2	11 416	0,000 087 6	0, 0,000 175 2
2	resistor, carbon film (see Table C.5)	5	228 311	0,000 004 4	0,000 021 9
3	capacitor, standard, no power (see Table C.4)	4	114 155	0,000 008 8	0,000 035 0
4	relay, value given by the manufacturer (B_{10D} = 20 000 000 cycles, n_{op} = 633 600 cycles per year)	4	315,7	0,003 167 6	0,012 670 3
5	contactor, value given by the manufacturer (B_{10D} = 2 000 000 cycles, n_{op} = 633 600 cycles per year)	1	31,6	0,031 645 6	0,031 645 6
$\sum(n_j / MTTF_{D\,j})$					0,044 548 0
$MTTF_D = 1 / \sum(n_j / MTTF_{D\,j})$ [years]					22,4

NOTE 1 This method is based on the presumption that a dangerous failure of any component (worst case estimation) within a channel leads to dangerous failure of the channel. The $MTTF_D$ calculation illustrated by Table D.1 is based upon this.

NOTE 2 In this example, the main influence comes from the contactor. The chosen values for $MTTF_D$ and B_{10D} for this example are based on Annex C. For the example application d_{op} = 220 days/year, h_{op} = 8 h/day and t_{cycle} = 10 s/cycles is assumed, giving n_{op} = 633 600 cycles/year. In general, taking manufacturer's values for $MTTF_D$ and B_{10D} leads to a much better result, that is, a higher $MTTF_D$ for the channel.

NOTE 3 When MTTR (mean time to restoration) can be considered negligible, MTTF can be considered equal to MTBF.

NOTE 4 Where only MTBF values are available, a conversion to $MTTF_D$ values can be done by $MTTF_D \approx 2*MTBF$.

D.2 $MTTF_D$ for different channels, symmetrisation of $MTTF_D$ for each channel

The designated architectures of 6.1.3.2 assume that for different channels in a redundant SRP/CS the values for $MTTF_D$ for each channel are the same. This value per channel should be input for Figure 12.

If the $MTTF_D$ of the channels differ, there are two possibilities:

— as a worst-case assumption, the lower value should be taken into account;

— Formula (D.2) can be used as an estimation of a value that can be substituted for $MTTF_D$ for each channel:

$$MTTF_D = \frac{2}{3}\left[MTTF_{DC1} + MTTF_{DC2} - \frac{1}{\frac{1}{MTTF_{DC1}} + \frac{1}{MTTF_{DC2}}} \right] \quad \text{(D.2)}$$

where

$MTTF_{D\,C1}$ is the values for two different redundant channels each limited to a maximum value of 100 years (categories B, 1, 2 and 3);

$MTTF_{D\,C2}$ is the values for two different redundant channels each limited to a maximum value of 2 500 years (category 4).

EXAMPLE One channel has an $MTTF_{D\,C1}$ = 3 years, the other channel has an $MTTF_{D\,C2}$ = 100 years, then the resulting $MTTF_D$ = 66 years for each channel. This means a redundant system with 100 years $MTTF_D$ in one channel and 3 years $MTTF_D$ in the other channel is equal to a system where each channel has a $MTTF_D$ of 66 years.

A redundant system with two channels and different $MTTF_D$ values for each channel can be substituted by a redundant system with identical $MTTF_D$ in each channel by using the above formula. This procedure is necessary for the correct use of Figure 12.

NOTE This method assumes independent parallel channels.

Annex E
(informative)

Estimates for diagnostic coverage for functions and subsystems

E.1 Examples of diagnostic coverage

See Table E.1.

Table E.1 — Estimates for diagnostic coverage

Measure	DC
Input device	
cyclic test stimulus by dynamic change of the input signals	90 %
plausibility check, e.g. use of normally open and normally closed mechanically linked contacts	99 %
cross monitoring of inputs without dynamic test	percentage to be defined depending on the specific application, e.g. depending on how often a signal change is done by the application (see Note 5)
cross monitoring of input signals with dynamic test if short circuits are not detectable (for multiple I/O)	90 %
cross monitoring of input signals and intermediate results within the logic (L), and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99 %
indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of machine actuators) only applicable if the dangerous failure of the single channel can be detected for redundant channels	90 % to 99 %, depending on the application (see Note 3)
NOTE 1 For additional estimations for DC, see, e.g. IEC 61508-2:2010, Table A.2 to Table A.14. NOTE 2 If medium or high DC is claimed for the logic, at least one measure for variable memory, invariable memory and processing unit with each DC at least 60 % has to be applied. There are other measures that can be used other than those listed in this table. For measures where a DC range is given (e.g. fault detection by the process) the correct DC value can be determined by considering all dangerous failures and then deciding which of them are detected by the DC measure. In case of any doubt a FMEA should be the basis for the estimation of the DC. NOTE 3 For the DC measure "Fault detection by the process" the demand rate of the safety function (rd) and the process diagnostic (test) rate (rt) could be considered together with a limitation of the effective DC of the tested component: 1) $r_t/r_d = 1$ DC is limited to 60 % 2) $r_t/r_d = 10$ DC is limited to 90 % 3) $r_t/r_d = 100$ DC is limited to 99 % NOTE 4 The effect of the test rate (how often a signal change is done by the application) can be incorporated using the following limitations for the effective DC of the tested component: For Category 3 and 4: — $r_t < 1$/year DC is 0 % — $r_t \geq 1$/year DC is limited to 90 % — $r_t \geq 1$/month DC is limited to 99 %	

Table E.1 *(continued)*

Measure	DC
direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99 %
fault detection by the process	percentage to be defined depending on the specific application, e.g. depending on the application; this measure alone is not sufficient for the required performance level e (see Note 3 and Note 4)
monitoring some characteristics of the sensor (response time, range of analogue signals, e.g. electrical resistance, capacitance)	60 %
Logic	
indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of machine actuators, plausibility check of final result) only applicable if the dangerous failure of the single channel can be detected for redundant channels.	90 % to 99 %, depending on the application (see Note 3)
direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements, plausibility check of intermediate results)	99 %
simple temporal time monitoring of the logic (e.g. timer as watchdog, where trigger points are within the program of the logic)	60 %
temporal and logical monitoring of the logic by the watchdog, where the test equipment does plausibility checks of the behaviour of the logic	90 %
start-up self-tests to detect latent faults in parts of the logic (e.g. program and data memories, input/output ports, interfaces)	90 % (depending on the testing technique)
checking the monitoring device reaction capability (e.g. watchdog) by the main channel at start-up or whenever the safety function is demanded or whenever an external signal demand it, through an input facility	90 %
dynamic principle (all components of the logic are required to change the state ON-OFF-ON when the safety function is demanded), e.g. interlocking circuit implemented by relays	99 %

NOTE 1 For additional estimations for DC, see, e.g. IEC 61508-2:2010, Table A.2 to Table A.14.

NOTE 2 If medium or high DC is claimed for the logic, at least one measure for variable memory, invariable memory and processing unit with each DC at least 60 % has to be applied. There are other measures that can be used other than those listed in this table.

For measures where a DC range is given (e.g. fault detection by the process) the correct DC value can be determined by considering all dangerous failures and then deciding which of them are detected by the DC measure. In case of any doubt a FMEA should be the basis for the estimation of the DC.

NOTE 3 For the DC measure "Fault detection by the process" the demand rate of the safety function (rd) and the process diagnostic (test) rate (rt) could be considered together with a limitation of the effective DC of the tested component:

1) $r_t/r_d = 1$ DC is limited to 60 %

2) $r_t/r_d = 10$ DC is limited to 90 %

3) $r_t/r_d = 100$ DC is limited to 99 %

NOTE 4 The effect of the test rate (how often a signal change is done by the application) can be incorporated using the following limitations for the effective DC of the tested component:

For Category 3 and 4:

— $r_t < 1/\text{year}$ DC is 0 %

— $r_t \geq 1/\text{year}$ DC is limited to 90 %

— $r_t \geq 1/\text{month}$ DC is limited to 99 %

Table E.1 *(continued)*

Measure	DC
invariable memory: signature of one word (single bus width)	90 %
invariable memory: signature of double word (double bus width)	99 %
variable memory: RAM-test by use of redundant data e.g. flags, markers, constants, timers and cross comparison of these data	60 %
variable memory: check for readability and write ability of used data memory cells	60 %
variable memory: RAM self-test (e.g. "galpat" or "Abraham") or double RAM with hardware or software comparison and read/write test.	99 %
processing unit: self-test by software (see IEC 61508-7:2010, A.3)	60 % to 90 %
processing unit: coded processing (see IEC 61508-7:2010, A.3)	90 % to 99 % (see Note 3)
fault detection by the process	percentage to be defined depending on the specific application, e.g. depending on the application; this measure alone is not sufficient for the required performance level "e" (see Note 3 and Note 4)
Output device	
monitoring of outputs by one channel without dynamic test	percentage to be defined depending on the specific application, e.g. depending on how often a signal change is done by the application (see Note 5)
cross monitoring of outputs without dynamic test	percentage to be defined depending on the specific application, e.g. depending on how often a signal change is done by the application (see Note 5)
cross monitoring of output signals with dynamic test without detection of short circuits (for multiple I/O)	90 %
cross monitoring of output signals and intermediate results within the logic (L) and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99 %
redundant shut-off path with monitoring of the outputs by logic and test equipment, see example ISO 13849-2:2012, Annex E	99 %

NOTE 1 For additional estimations for DC, see, e.g. IEC 61508-2:2010, Table A.2 to Table A.14.

NOTE 2 If medium or high DC is claimed for the logic, at least one measure for variable memory, invariable memory and processing unit with each DC at least 60 % has to be applied. There are other measures that can be used other than those listed in this table.

For measures where a DC range is given (e.g. fault detection by the process) the correct DC value can be determined by considering all dangerous failures and then deciding which of them are detected by the DC measure. In case of any doubt a FMEA should be the basis for the estimation of the DC.

NOTE 3 For the DC measure "Fault detection by the process" the demand rate of the safety function (rd) and the process diagnostic (test) rate (rt) could be considered together with a limitation of the effective DC of the tested component:

1) $r_t/r_d = 1$ DC is limited to 60 %

2) $r_t/r_d = 10$ DC is limited to 90 %

3) $r_t/r_d = 100$ DC is limited to 99 %

NOTE 4 The effect of the test rate (how often a signal change is done by the application) can be incorporated using the following limitations for the effective DC of the tested component:

For Category 3 and 4:

— $r_t < 1$/year DC is 0 %

— $r_t \geq 1$/year DC is limited to 90 %

— $r_t \geq 1$/month DC is limited to 99 %

Table E.1 *(continued)*

Measure	DC
indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of machine actuators) only applicable if the dangerous failure of the single channel can be detected for redundant channels	90 % to 99 %, depending on the application (see Note 3)
fault detection by the process	percentage to be defined depending on the specific application, e.g. depending on the application; this measure alone is not sufficient for the required performance level "e"! (see Note 3 and Note 4)
direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99 %

NOTE 1 For additional estimations for DC, see, e.g. IEC 61508-2:2010, Table A.2 to Table A.14.

NOTE 2 If medium or high DC is claimed for the logic, at least one measure for variable memory, invariable memory and processing unit with each DC at least 60 % has to be applied. There are other measures that can be used other than those listed in this table.

For measures where a DC range is given (e.g. fault detection by the process) the correct DC value can be determined by considering all dangerous failures and then deciding which of them are detected by the DC measure. In case of any doubt a FMEA should be the basis for the estimation of the DC.

NOTE 3 For the DC measure "Fault detection by the process" the demand rate of the safety function (rd) and the process diagnostic (test) rate (rt) could be considered together with a limitation of the effective DC of the tested component:

1) $r_t/r_d = 1$ DC is limited to 60 %

2) $r_t/r_d = 10$ DC is limited to 90 %

3) $r_t/r_d = 100$ DC is limited to 99 %

NOTE 4 The effect of the test rate (how often a signal change is done by the application) can be incorporated using the following limitations for the effective DC of the tested component:

For Category 3 and 4:

— $r_t < 1/\text{year}$ DC is 0 %

— $r_t \geq 1/\text{year}$ DC is limited to 90 %

— $r_t \geq 1/\text{month}$ DC is limited to 99 %

For the application of Table E.1 see the indicative examples below.

EXAMPLE 1 Annex E of ISO 13849-2:2012 presents a complete worked example (which is very detailed) for the validation of fault behaviour and diagnostic means on an automatic assembly machine.

EXAMPLE 2 ISO/TR 24119 describes a pragmatic step-by-step table-based methodology for evaluation of diagnostic coverage for series connected interlocking devices.

EXAMPLE 3 The DC measure "fault detection by the process" can only be applied if the safety-related component is involved in the production process, e.g. a standard PLC or standard sensors are used for workpiece processing and as part of one of two channels executing the safety function. The appropriate DC level depends on the overlap of the commonly used resources (logic, inputs/outputs). For example, when all faults of a rotary encoder on a printing machine lead to highly visible interruption of the printing process, the DC for this sensor used to monitor a safely limited speed can be estimated as 90 % up to 99 %.

E.2 Estimation of the average diagnostic coverage

In many systems, several measures for fault detection might be used. These measures could check different parts of the SRP/CS and have different diagnostic coverage. For an estimation of the PL according to 6.1.8 and Figure 12 only one average DC for the whole SRP/CS performing the safety function is applicable.

DC may be determined as the ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures. According to this definition an average diagnostic coverage DC_{avg} is estimated by the Formula (E.1):

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

Here, all components of the SRP/CS without fault exclusion should be considered and summed up. For each block, the $MTTF_D$ and the DC are taken into account. DC in this equation means the ratio of the failure rate of detected dangerous failures of the part (regardless of the measures used to detect the failures) to the failure rate of all dangerous failures of the part. Thus, DC refers to the tested part and not to the testing device. Components without failure detection (e.g. which are not tested) have DC = 0 and contribute only to the denominator of DC_{avg}.

Annex F
(informative)

Measures against common cause failures

F.1 General

The comprehensive procedure for measures against CCF as described in F.2 and F.3 should be followed for each subsystem of category 2, 3 or 4 which contributes to the SRP/CS.

The simplified procedure in 6.1.8 of this document assumes a β-factor of 2 % according to IEC 61508-6:2010, Annex D. This can be reached by following the procedure in F.2.

The measures described in F.2 and F.3 should be documented in order to support a minimum score of 65 points is achieved.

F.2 Estimation of effect of measures against CCF

Every part of the subsystem should be considered for CCF.

Table F.1 lists the measures, based on engineering judgement, which represent the contribution each measure makes in the reduction of common cause failures.

In F.3 the measures are described in detail. For each listed measure, the full score can only be claimed, if the measure is fully implemented. If a measure is only partly fulfilled a score of zero must be assumed.

Table F.1 — Scoring process and quantification of measures against CCF

No.	Measure against CCF	Score
1	separation/segregation	15
2	diversity	20
3	design/application/experience	
3.1	protection against over-voltage, over-pressure, over-current, over-temperature	15
3.2	components used are well-tried	5
4	assessment/analysis	5
5	training	5
6	environmental	
6.1	prevention of EMI or impurity of fluidic medium	25
6.2	other influences	10
	total	[max. achievable 100]

Total score[a]	**Measures for avoiding CCF**
65 or better	Meets the requirements
Less than 65	Process failed ⇒ apply additional measures

[a] Where technological measures are not relevant, points attached to this column can be considered in the comprehensive calculation.

F.3 Description of the measures against common cause failure in Table F.1

F.3.1 General

The measures listed in Table F.1 should be evaluated according to their effectiveness to avoid or control common cause failures of redundant channels. Engineering judgement should support that typical causes for CCF are reduced as much as reasonably possible.

NOTE 1 The calculation of the CCF is usually performed on a subsystem level, as the measures for the individual subsystems differ (e.g. inputs, logic and outputs) .

NOTE 2 Redundant channels in this annex means functional channel and test channel in category 2 or redundant functional channels in categories 3 and 4.

NOTE 3 Typical causes are over-voltage, over-pressure, over-current, over-temperature, humidity, shock, vibration, electromagnetic interference, impurity of the pressure medium. The appropriate level of these causes is deduced from the expected application of the SRP/CS including foreseeable faults (e.g. failure of a cooling fan) and reasonably foreseeable misuse. The measures can vary for different categories (category 2 vs. 3 and 4) or input/logic/output parts of the SRP/CS.

F.3.2 Separation/segregation

Physical separation between signal paths of redundant channels, for example:

a) separation in wiring (e.g. multi conductor cable with suitable insulation between conductors);

b) separation in piping (e.g. avoiding damaging of a hydraulic pipe due to high pressure released from another adjacent pipe);

c) detection of short circuits and open circuits in cables by dynamic test;

d) separate shielding for the signal path of each channel;

e) redundant channels on separate printed-circuit boards or in separate housings or cabinets;

f) sufficient clearances and creepage distances between redundant channels on printed-circuit boards, also taking into account e.g. tin whiskers (see ISO 13849-2:2012, D.2.2).

F.3.3 Diversity

Diversity considerations include, for example:

a) Different technologies/design or physical principles are used, for example:

   — first channel electronic or programmable electronic and second channel electromechanical hardwired,

   — different initiation of safety function for each channel (e.g. position, pressure, temperature),

   — first channel valve with rubber seal and second channel with metal seal,

   — two position switches are used to detect the opening of a movable guard (safety guard), the first one is operated when the safety guard is opened and uses a break-contact element with direct opening action in accordance with IEC 60947-5-1:2020 Annex K, the second one is operated when the safety guard is closed and uses a make-contact element;

b) Sensing elements employ different measurement principles (e.g. digital and analogue) or physical principles (e.g. distance, pressure or temperature);

c) Different components e.g. of different manufacturers (not re-badged);

d) Different loads, e.g. the first contact/valve switches without load, the second contact/valve switches under load.

F.3.4 Design/application/experience

F.3.4.1 Protection against or control of over-voltage, over-pressure, over-current, over-temperature, for example:

a) Inputs and outputs of the SRP/CS and the power supply of the logic are protected from potential levels of over-voltage and/or over-current (see also IEC 60204-1;

NOTE Parts of the SRP/CS are capable of withstanding or are protected from potential levels of over-voltage and/or over-current. Possible maximum overvoltage level of SW mode PSU (switch mode power supply) depends on the applied standard (e.g. maximum voltages limit under single fault condition).

It is important to take into account the possible maximum overvoltage level by applied standard SW mode PSU as well as other operating conditions (e.g. overvoltage category, operating temperature).

b) The measure against over-pressure can be a single channel system if the primary pressure in case of failure can never rise over the operating pressure multiplied 1,5. ISO 4414 defines a requirement for protection from unintended pressure (e.g. a pressure relief valve).

F.3.4.2 Components used are well-tried

All components used in the channels of the safety function are well-tried (see also ISO 13849-2:2012).

F.3.5 Assessment/analysis

For each part of safety-related parts of control system a failure mode and effect analysis or fault tree analysis has been carried out to identify potential causes for CCF and its results are taken into account to avoid common cause failures in the design.

F.3.6 Training

Designers have been trained (with training documentation, e.g. certificate of training) to understand the causes and consequences of common cause failures.

F.3.7 Environmental

F.3.7.1 Prevention of EMI or impurity of the pressure medium

For electrical/electronic systems, contamination and electromagnetic disturbances are prevented to protect against common cause failures in accordance with appropriate standards (e.g. IEC 61326-3-1, IEC 61000-6-7:2014, IEC 61000-1-2:2016, IEC 61800-5-2).

NOTE 1 These EMC standards usually have more stringent requirements than standard components (e.g. general purpose PLC) are designed to meet. See IEC 61800-3 for further information.

NOTE 2 Annex L provides further guidance in relation to EMC immunity.

For fluidic systems, filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, is implemented in compliance with the component manufacturers' requirements concerning purity of the pressure medium, see ISO 8573-1 for guidance.

For combined fluidic and electric systems, both aspects should be considered.

F.3.7.2 Other influences

The SRP/CS is immune to all relevant environmental influences such as temperature, shock, mechanical stresses, vibration, humidity, as specified in relevant standards, e.g. IEC 60068 series, taking into account the increased requirements for safety-related application.

If components are used in the SRP/CS that are not sufficiently protected against over-voltage, environmental influences by internal measures this protection should be reached on system level using external protection components, filters, shielding.

F.4 Measures against common cause failure and other relevant standards

For some SRP/CS (subsystems) not all the measures against CCF listed in Table F.1 can provide an appropriate reduction of the CCF impact since the potential risk reduction that can be provided by those SRP/CS is limited also by their systematic capabilities (e.g. detection principle of sensors).

NOTE Some relevant standards (e.g. 62024:2018 for the application of protecting equipment to detect the presence of persons or ISO 14119:2014 for the selection and application of interlocking devices associated with guards) can include application limits related to systematic capabilities.

The designer of the complete SRP/CS applies the measures stated in these standards and complies with the instructions for use provided by the manufacturer.

Annex G
(informative)

Systematic failure

G.1 General

This Annex provides guidance on measures to control and avoid systematic failures during the design and integration of SRP/CS.

G.2 Measures for the control of systematic failures

The following measures should be applied:

a) Use of de-energization (see ISO 13849-2:2012): The safety-related parts of the control system (SRP/CS) should be designed so that the machine will achieve or maintain a safe state upon a power supply loss.

c) Measures for controlling the effects of voltage breakdown, voltage variations, overvoltage, undervoltage: SRP/CS behaviour in response to voltage breakdown, voltage variations, overvoltage, and undervoltage conditions should be predetermined so that the SRP/CS can achieve or maintain a safe state of the machine (see also IEC 60204-1 and IEC 61508-7:2010, A.8).

e) Measures for controlling or avoiding the effects of the physical environment (for example, temperature, humidity, water, vibration, dust, corrosive substances, electromagnetic interference and its effects): SRP/CS behaviour in response to the effects of the physical environment should be predetermined so that the SRP/CS can achieve or maintain a safe state of the machine (see also, for example, IEC 60529, IEC 60204-1).

g) Program sequence monitoring should be used with SRP/CS containing software in order to detect defective program sequences: A defective program sequence exists if the individual elements of a program (e.g. software modules, subprograms or commands) are processed in the wrong sequence or period of time or if the clock of the processor is faulty (see IEC 61508-7:2010, A.9).

i) Measures for controlling the effects of errors and other effects arising from any data communication process (see IEC 61508-2:2010, 7.4.11)

In addition, one or more of the following measures should be applied, taking into account the complexity of the SRP/CS and its PL:

— failure detection by automatic tests;

— tests by redundant hardware;

— diverse hardware;

— operation in the positive mode;

— mechanically linked contacts;

— direct opening action;

— oriented mode of failure;

— over-dimensioning by a suitable factor, where the manufacturer can demonstrate that derating improves reliability.

NOTE Examples for over-dimensioning see ISO 13849-2:2012, Table D.2.

G.3 Measures for avoidance of systematic failures

The following measures should be applied:

a) Use of suitable materials and adequate manufacturing;

Selection of material, manufacturing methods and treatment in relation to, e.g. stress, durability, elasticity, friction, wear, corrosion, temperature, conductivity, dielectric rigidity.

b) Correct dimensioning and shaping;

Consideration of e.g. stress, strain, fatigue, temperature, surface roughness, tolerances, manufacturing.

c) Proper selection, combination, arrangements, assembly and installation of components, including cabling, wiring and any interconnections;

Apply appropriate standards and manufacturer's application notes, e.g. catalogue sheets, installation instructions, specifications, and use of good engineering practice.

d) Compatibility;

Use components with compatible operating characteristics.

NOTE Components such as hydraulic or pneumatic valves can require cyclic switching to avoid failure by non-switching or unacceptable increase in switching times. In this case a periodic test is necessary.

e) Withstanding specified environmental conditions;

Design the SRP/CS so that it is capable of working in all expected environments and in any foreseeable adverse conditions, e.g. temperature, humidity, vibration and electromagnetic interference (EMI) (see ISO 13849-2:2012, D.2).

f) Use of components designed to an appropriate standard and having well-defined failure modes.

To reduce the risk of undetected faults by the use of components with specific characteristics (see IEC 61508-7:2010, B.3.3).

In addition, one or more of the following measures should be applied, taking into account the complexity of the SRP/CS and its PL:

— Hardware design review (e.g. by inspection or walk-through);

To reveal by reviews and analysis discrepancies between the specification and implementation.

— Computer-aided design tools capable of simulation or analysis;

Perform the design procedure systematically and include appropriate automatic construction elements that are already available and tested.

— Simulation.

Perform a systematic and complete inspection of an SRP/CS design in terms of both the functional performance and the correct dimensioning of their components.

G.4 Measures for avoidance of systematic failures during SRP/CS integration

The following measures should be applied during integration of the SRP/CS:

— functional testing;

— project management;

— documentation.

In addition, black-box testing should be applied, taking into account the complexity of the SRP/CS and its PL.

G.5 Management of functional safety

A functional safety plan should be drawn up and documented for each SRP/CS design project, and should be updated as necessary. The functional safety plan is intended to provide measures for preventing incorrect specification, implementation, or modification issues.

The functional safety plan should identify the relevant activities (see Figure 4, Iterative process for design of SRP/CS) and should be adapted to the project.

NOTE 1 The functional safety plan can be part of other design documents.

NOTE 2 The content of the functional safety plan depends upon the specific circumstances, which can include:

— size of project;

— degree of complexity;

— degree of novelty of design and technology;

— degree of standardization of design features;

— possible consequence(s) in the event of failure.

In particular the functional safety plan should:

a) identify the relevant activities in the SRP/CS design process (specification, design, integration, analysis, testing, verification, validation) and details of when they should take place;

b) identify the roles and resources necessary for carrying out and reviewing each of these activities

c) identify procedures for release, configuration, documentation and modification of hardware and software design;

d) establish a validation plan (see 10.1.2);

e) identify relevant activities before carrying out any modification.

In addition, black-box testing should be applied, taking into account the complexity of the SRP/CS and its PL.

NOTE 3 The request for a modification can arise from, for example:

— safety requirements specification changed;

— conditions of actual use;

— incident/accident experience;

— change of material processed;

— obsolescence;

— modifications of the machine or of its operating modes.

The effect of the requested modification should be analysed to establish the effect on the safety function.

All accepted modifications that have an effect on the SRP/CS should initiate a return to an appropriate design phase for its hardware and/or for its software (e.g. specification, design, integration, installation,

commissioning, and validation). All subsequent phases and management procedures should then be carried out in accordance with the procedures specified for the specific phases in this document. All relevant documents should be revised, amended and reissued accordingly.

Annex H
(informative)

Example of combination of several subsystems

Figure H.1 is a schematic diagram of the combination of subsystems of an SRP/CS providing one of the safety functions controlling a machine actuator. This is not a functional/working diagram and is included only to demonstrate the principle of combining categories and technologies in this one function.

The control is provided through electronic control logic and a hydraulic directional control valve. The risk is reduced by an AOPD, which detects access to the hazard zone and prevents start-up of the fluidic actuator when the light beam is interrupted.

The subsystems of the SRP/CS which provide the safety function are: AOPD, electronic control logic, hydraulic directional control valve and their interconnecting means.

These combined subsystems provide a stop function as a safety function. As the AOPD is interrupted, the outputs transfer a signal to the electronic control logic, which provides a signal to the hydraulic directional control valve to stop the hydraulic flow as the output of the SRP/CS. At the machine, this stops the hazardous movement of the fluidic actuator.

This combination of subsystems creates a safety function demonstrating the combination of different categories and technologies based on the requirements given in Clause 6. Using the principles given in this document, the subsystems shown in Figure H.2 can be described as follows.

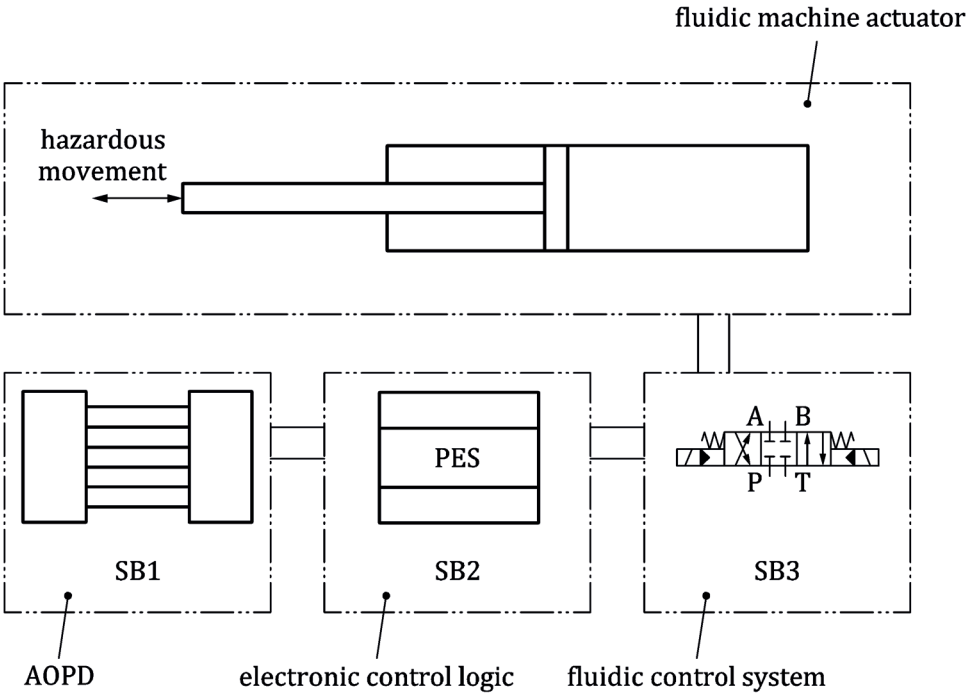
— Category 2, PL c for the electro-sensitive protective device (light barrier). To reduce the probability of faults this device uses well-tried safety principles;

— Category 3, PL d for the electronic control logic. To increase the level of safety performance of this electronic control logic, the structure of this subsystem is redundant and implements several fault detection measures such that it is able to detect most of single faults;

— Category 1, PL c for the hydraulic directional control valve. The status of being well-tried is mainly application-specific. In this example, the valve is considered to be well-tried. In order to reduce the probability of faults, this device comprises well-tried components applied using well-tried safety principles and all application conditions are considered (see 6.1.3.2.4).

NOTE 1 The position, size and layout of the interconnecting means have also to be taken into account. This combination leads with PL_{low} c and $N_{low} = 2$ to an overall performance level of PL c (see 6.2).

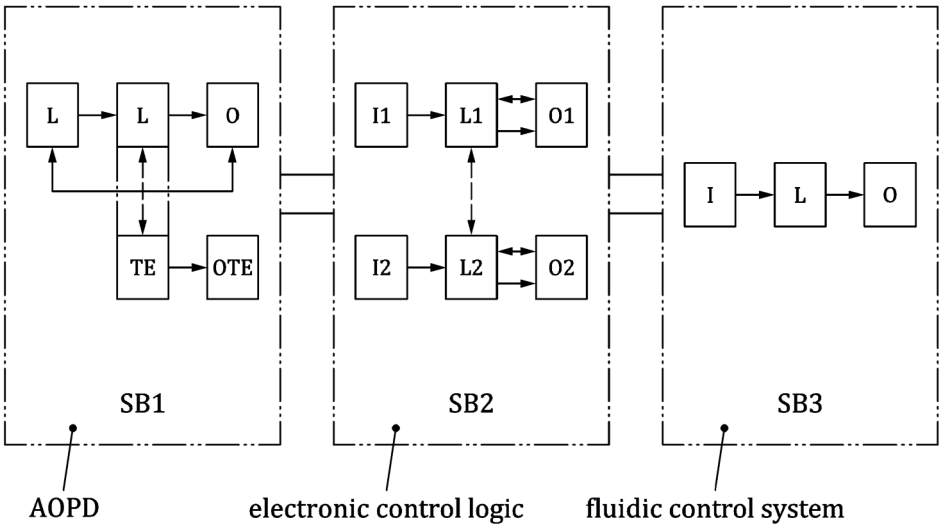
NOTE 2 In case of one fault in the category 1 or the category 2 subsystem of Figure H.2 there can be a loss of the safety function.



Key

AOPD active optoelectronic protective device (e.g. light barrier)
SB1 category 2 [Type 2], PL c
SB2 category 3, PL d (electronic control logic)
SB3 category 1, PL c (fluidic control system)
PES programmable electronic system

Figure H.1 — Example — Block diagram explaining combination of subsystems



Key

AOPD	active optoelectronic protective device (e.g. light barrier)
I, I1, I2	input devices, e.g. sensor
L, L1, L2	logic
O, O1, O2, OTE	output devices, e.g. main contactor
SB1	category 2 [Type 2], PL c
SB2	category 3, PL d (electronic control logic)
SB3	category 1, PL c (fluidic control system)
TE	test equipment

Figure H.2 — Substitution of Figure H.1 by designated architectures

Annex I
(informative)

Examples

I.1 General

Annex I illustrates the use of the simplified procedure for estimating PL given in 6.1.8 and the preceding annexes for identifying safety functions and determining the PL. The quantification of two control circuits is given. For the stepwise procedure, see Figure I.3.

The following examples do not take into account the measures to ensure systematic integrity, software requirements, the correct application of basic and well-tried principles. They are only intended to show quantification of $MTTF_D$, DC_{avg}, CCF, category and corresponding PL.

Two examples (A and B) of control circuits for different machines are examined, see Figure I.1 and Figure I.3. Both illustrate the performance of the same safety function of the interlocking of the guard door, but they have different PL_r due to differences in the applications. The first example consists of one channel of electromechanical components with medium and high $MTTF_D$ values, while the second example is made up of two channels — one electromechanical and the other programmable electronic — of components with medium and high $MTTF_D$ values, and with appropriate diagnostic testing.

I.2 Safety function and required performance level

For both examples, the requirements of the safety function associated with the guard door interlocking can be specified as follows.

The dangerous movement will be stopped (by decelerating or de-energising the electric motor) when the interlocking guard is opened.

NOTE For the example B, the risk assessment determined that a loss of controlled deceleration of the motor as a result of a malfunction (SW2, CC or PLC) was acceptable.

The minimum distance between the interlocking guard and moving parts of the machine was determined according to ISO 13855:2010, based on the machine stopping performance.

For example A, the risk parameters according to the risk graph method (see Figure A.1) are as follows:

— severity of injury, *S* = S2, serious;

— frequency and/or exposure time to hazard, *F* = F1, seldom to less often and/or the exposure time is short;

— possibility of avoiding the hazard, *P* = P1, possible under specific conditions.

These risk parameter selections lead to a required performance level PL_r of c.

Determination of the preferred category: a performance level of “c” can be achieved typically by very reliable single-channel systems (category 1), tested single-channel systems (category 2) or redundant architectures (category 3) (see Figure 12).

For example B, the risk parameters S2 and P1 are the same, but for frequency and/or exposure time to hazard, *F* = F2, frequent to continuous and/or the exposure time is long.

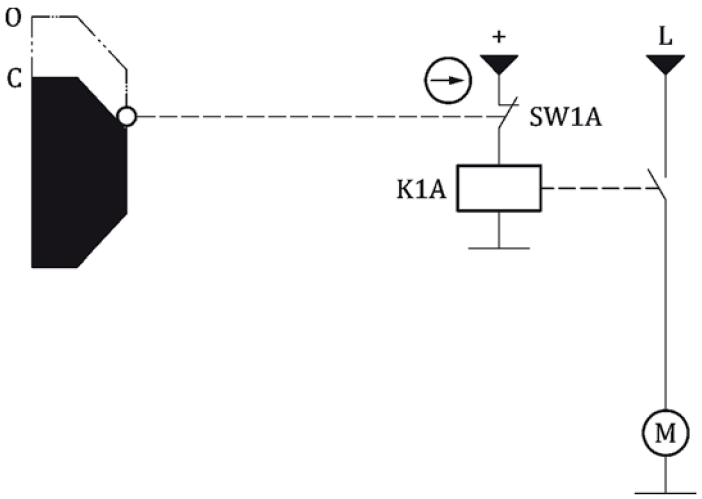
These decisions lead to a required performance level PL_r of d.

Determination of the preferred category: a performance level of “d” can be achieved typically by redundant architectures (category 2 or 3) (see Figure 12).

I.3 Example A, single-channel system

I.3.1 Identification of safety-related parts

All components contributing to the guard interlocking safety function are represented in Figure I.1. Other components that do not contribute to the safety function (for example, start and stop switches) are omitted for simplicity.



Key

O	guard interlocking is open
C	guard interlocking is not open
M	motor
K1A	contactor relay
SW1A	position switch (NC)
L	power supply
⊖	direct opening

Figure I.1 — Control circuit A for performing safety function

In this example, a position switch SW1A with direct opening action is used in the positive mode of actuation but no fault exclusion is justified for the mechanical parts. The position switch is connected to a contactor relay K1A, which is able to switch off the power to the motor. The key features of these safety-related parts are therefore:

— one channel of electromechanical components;

— position switch SW1A (NC) has direct opening action of the contact and high B_{10D};

— contactor relay K1A has high $B_{10D.}$

The position switch and contactor relay in this example are both well-tried components when implemented according to ISO 13849-2:2012.

The safety-related parts can be illustrated in a safety-related block diagram as shown in Figure I.2.

Key

SW1A position switch

K1A contactor relay

Figure I.2 — Safety-related block diagram identifying safety-related parts of example A

I.3.2 Quantification of $MTTF_D$, DC_{avg}, measures against CCF, category, and performance level

The values for $MTTF_D$, DC_{avg} and measures against CCF are assumed to be estimated according to Annex C, Annex D, Annex E and Annex F, or to be given by the manufacturer. The categories are estimated according to 6.1.3.

— $MTTF_D$

The position switch SW1A and the contactor relay K1A contribute to the $MTTF_D$ of the one channel. The values of $B_{10D,SW1A}$ = 20 000 000 cycles (position switch independent of load) and $B_{10D,K1A}$ = 400 000 cycles (contactor relay with maximum load) are assumed to be provided by the manufacturer. Applying the method of C.4.2 with 220 working days per year, 8 working hours per day and a cycle time of 60 min, this gives $MTTF_{D,SW1A}$ = 113 636 years and $MTTF_{D,K1A}$ = 2 273 years. Then using the parts count method of D.1, the $MTTF_D$ of the one channel is calculated as:

$$\frac{1}{MTTF_D} = \frac{1}{MTTF_{D,SW1A}} + \frac{1}{MTTF_{D,K1A}} = \frac{1}{113\ 636\text{years}} + \frac{1}{2\ 273\text{years}} = \frac{0{,}000\ 45}{\text{year}} \quad \text{(I.1)}$$

which gives an $MTTF_D$ = 2 222 years (limited to 100 years) for the channel, which is "high" according to 6.1.4, Table 5.

NOTE If no B_{10D} information for SW1A or K1A is available, a worst-case assumption according to C.2 or C.4 could be made.

— T_{10D}

The method given in C.4.2 gives $T_{10D,SW1A}$ of 11 364 years and $T_{10D,K1A}$ of 227 years, which both exceed the mission time of 20 years and therefore eliminate the need for any preventive exchange.

— DC

No diagnostic testing is performed in control circuit A, the DC = 0 or "none", as only one channel is used, DC is not relevant.

— CCF

As only one channel is used, measures against CCF are not relevant.

— Category

The characteristics of category 1 (basic and well-tried safety principles, well tried components) are fulfilled, including the requirement for the $MTTF_D$ of the channel to be "high".

Input data for Figure 12: $MTTF_D$ of the channel is "high" (100 years), DC_{avg} is "none" and category is 1.

Using Figure 12, this is interpreted as performance level c.

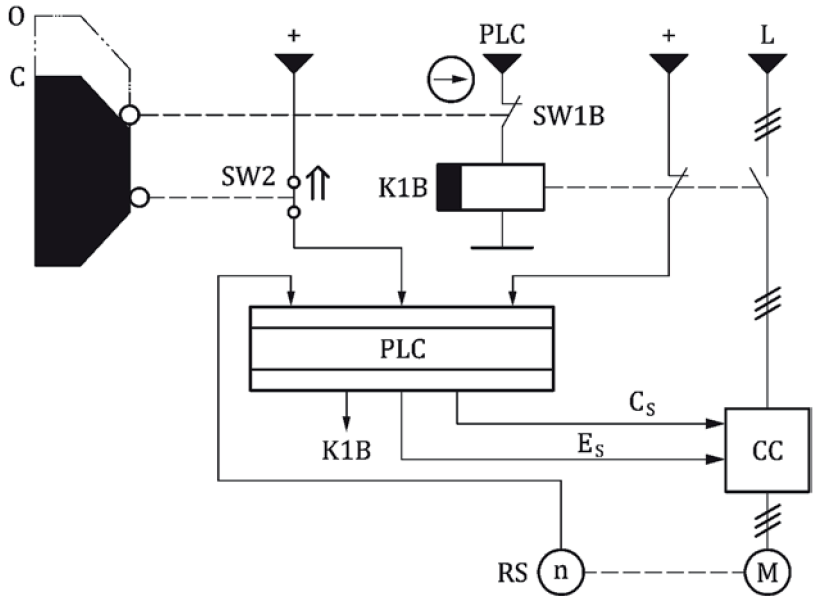
Application of Annex K gives an average probability of a dangerous failure per hour (PFH_D) of $1{,}14 \times 10^{-6}$/h and PL c.

This result matches the required performance level c according to Figure I.2. Control system of example A therefore satisfies the requirements for risk reduction of the example A application of I.2, with S2, F1, P1 and PL_r c.

I.4 Example B, redundant system

I.4.1 Identification of safety-related parts

All components contributing to the guard interlocking safety function are represented in Figure I.3. Other components that do not contribute to the safety function (for example, start and stop switches or delayed switching of K1B) are omitted for simplicity.



Key

PLC	programmable logic controller	C_s	stop signal (standard)
CC	current converter	E_S	enable (standard)
M	motor	K1B	contactor relay
RS	rotation sensor	SW1B	position switch (NC)
O	guard interlocking is open	SW2	position switch (NO)
C	guard interlocking is not open	⊖	direct opening
L	power supply	⇑	actuated position

Figure I.3 — Control circuit B to perform the safety function

In this second example, a two-channel architecture is used to provide redundancy. As in example A, the first channel includes a position switch SW1B with direct opening action used in the positive mode of actuation. This position switch is connected to a contactor relay K1B, which is able to switch off the power to the motor. In the second channel, which includes (programmable) electronic components, a second position switch SW2 is connected to a programmable logic controller PLC that can command the current converter CC to switch off the power to the motor. The key features of these safety-related parts are therefore:

— redundant channels, one electromechanical and the other programmable electronic;

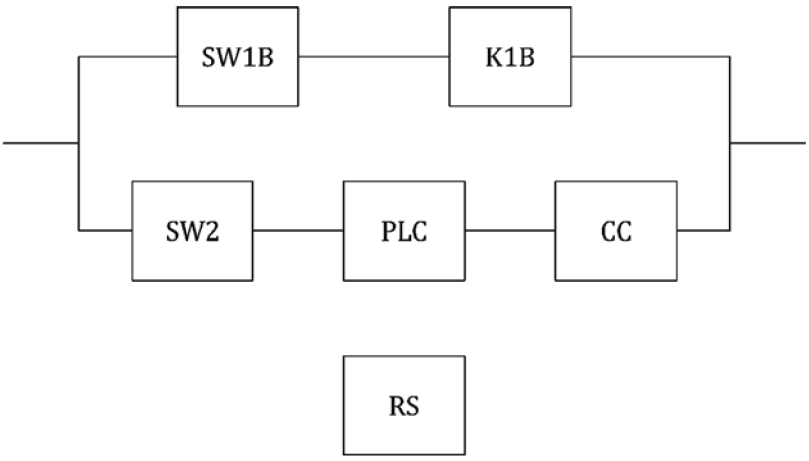
— only position switch SW1B (NC) has direct opening action of the contact, but both position switches SW1B and SW2 have high B_{10D};

— contactor relay K1B has high $MTTF_D$;

— electronic components PLC and CC have medium $MTTF_D$;

— the safety-related application software of the PLC (SRASW), e.g. the part of the software related to the monitoring of the input signals SW2, K1B, RS and the outputs commands to the current converter, is specified, designed and verified according to Clause 7.3 for a PL_r of d.

The safety-related parts and their division into channels can be illustrated in a safety-related block diagram as shown in Figure I.4. The first channel therefore consists of SW1B and K1B and the second channel consists of SW2, PLC and CC, while RS is only used to test the current converter.



Key

SW1B position switch
K1B contactor relay
SW2 position switch
PLC programmable logic controller
CC current converter
RS rotation sensor

Figure I.4 — Block diagrams identifying safety-related parts of example B

I.4.2 Quantification of $MTTF_D$ for each channel, average diagnostic coverage, measures against CCF, category and performance level

The values for $MTTF_D$ for each channel, DC_{avg} and measures against common cause failure are assumed to be evaluated according to Annex C, Annex D, Annex E and Annex F, or to be provided by the manufacturer. The categories are determined according to 6.1.3.

The position switch SW1B has a direct opening action and is used in the positive mode of actuation but no fault exclusion is justified for the mechanical parts.

— $MTTF_D$

The position switch SW1B and contactor relay K1B contribute to the $MTTF_{D,C1}$ of the first channel. The values of $B_{10D,SW1B}$ = 20 000 000 cycles (position switch independent of load) and $B_{10D,K1B}$ = 400 000 cycles (contactor relay with maximum load) are assumed to be provided by the manufacturer. Applying the method of C.4.2 with 300 working days per year, 16 working hours per day and a cycle time of 4 min, this gives $MTTF_{D,SW1B'}$ = 2 778 years and $MTTF_{D,K1B}$ = 56 years. Then using the parts count method of D.1, the $MTTF_{D,C1}$ of the first channel is calculated as

$$\frac{1}{\mathrm{MTTF_{D,C1}}} = \frac{1}{\mathrm{MTTF_{D,SW1B}}} + \frac{1}{\mathrm{MTTF_{D,K1B}}} = \frac{1}{2\ 778\mathrm{years}} + \frac{1}{56\mathrm{years}} = \frac{0{,}018\ 2}{\mathrm{year}} \quad \text{(I.2)}$$

which gives an $\mathrm{MTTF_D}$ = 55 years for the channel, which is "high" according to 6.1.4 and Table 6.

In the second channel SW2, PLC and CC all contribute to $\mathrm{MTTF_{D,C2}}$. The $B_{10D,SW2}$ of 1 000 000 cycles is assumed to be given by the manufacturer. Applying the method of C.4.2 as for the first channel gives an $\mathrm{MTTF_{D,SW2}}$ of 139 years. For PLC and CC an $\mathrm{MTTF_D}$ of 20 years is assumed to be given by the manufacturer. Applying the parts count method of D.1, to calculate the $\mathrm{MTTF_{D,C2}}$ of the second channel gives

$$\frac{1}{\mathrm{MTTF_{D,C2}}} = \frac{1}{\mathrm{MTTF_{D,SW2}}} + \frac{1}{\mathrm{MTTF_{D,PLC}}} + \frac{1}{\mathrm{MTTF_{D,CC}}} = \frac{1}{139\mathrm{years}} + \frac{1}{20\mathrm{years}} + \frac{1}{20\mathrm{years}} = \frac{0{,}107\ 2}{\mathrm{year}} \quad \text{(I.3)}$$

which gives an $\mathrm{MTTF_D}$ = 9,3 years for the channel, which is "low" according to 6.1.4, Table 6.

NOTE If no $\mathrm{MTTF_D}$ information for SW1B, SW2 or K1B is available, a worst-case assumption according to C.2 or C.4 can be made.

As both channels have different values of $\mathrm{MTTF_D}$, the Formula (D.2) can be used to calculate equivalent identical values of $\mathrm{MTTF_D}$ for a symmetrical two-channel system. Applying this equation yields an $\mathrm{MTTF_D}$ = 37 years for each channel, which is "high" according to 6.1.4, Table 6.

— T_{10D}

The method of C.4.2 gives $T_{10D,SW1B}$ of 278 years, $T_{10D,K1B}$ of 5.5 years and $T_{10D,SW2}$ of 13.9 years, with the latter two being lower than the mission time of 20 years. The estimation of PL and PFH is therefore only valid if K1B is exchanged before 5,5 years and if SW2 is exchanged before 13.9 years of operation respectively.

— DC

In control circuit B, five of the safety-related parts are tested by the PLC. This testing consists of SW1B, SW2 and K1B being read back by the PLC, the CC being read back by the PLC via RS and the PLC performing self-tests. The DC values associated with each of these tested parts are

1) $\mathrm{DC_{SW1B}} = \mathrm{DC_{SW2}}$ = 99 %, "high", due to plausibility check, see Table E.1 (second line of input device part),

2) $\mathrm{DC_{K1B}}$ = 99 %, "high", due to normally open and normally closed mechanically linked contacts, see Table E.1 (second line of input device part),

3) $\mathrm{DC_{PLC}}$ = 30 %, "none", due to low effectiveness of self-tests (this value comes out of the specific application), and

4) $\mathrm{DC_{CC}}$ = 90 %, "medium", due to indirect monitoring of the machine actuator by control logic, see Table E.1 (sixth line of output device part) – if the PLC monitors a failure of CC, it is able to stop the motion with the enable (standard) and to de-energize the contactor relay K1B (additional shut-off path).

For an estimation of the PL, an average DC value is needed as input for Figure 12:

$$DC_{avg} = \frac{\frac{DC_{SW1B}}{MTTF_{D,SW1B}} + \frac{DC_{K1B}}{MTTF_{D,K1B}} + \frac{DC_{SW2}}{MTTF_{D,SW2}} + \frac{DC_{PLC}}{MTTF_{D,PLC}} + \frac{DC_{CC}}{MTTF_{D,CC}}}{\frac{1}{MTTF_{D,SW1B}} + \frac{1}{MTTF_{D,K1B}} + \frac{1}{MTTF_{D,SW2}} + \frac{1}{MTTF_{D,PLC}} + \frac{1}{MTTF_{D,CC}}} =$$

$$= \frac{\frac{0,99}{2778} + \frac{0,99}{56} + \frac{0,99}{139} + \frac{0,3}{20} + \frac{0,9}{20}}{\frac{1}{2778} + \frac{1}{56} + \frac{1}{139} + \frac{1}{20} + \frac{1}{20}} = \frac{0,09}{0,13} = 67,9\ \% \qquad \text{(I.4)}$$

Thus, the resulting DC_{avg} is "low".

— CCF

For an estimation of the measures against CCF according to F.2, the scores for control circuit B are given in Table I.1.

Table I.1 — Estimation of the measures against CCF for example B

No.	Item	Score for control circuit	Maximum possible score
1	**Separation/segregation**		
	physical separation between signal paths	15	15
2	**Diversity**		
	different technologies/design or physical principles are used	20	20
3	**Design/application/experience**		
3.1	protection against over-voltage, over-pressure, over-current, over-temperature.	15	15
3.2	components used are well-tried	none (only partly fulfilled, see F.2)	5
4	**Assessment/analysis**		
	For each part of safety-related parts of control system a failure mode and effect analysis has been carried out and its results taken into account to avoid common-cause-failures in the design.	None	5
5	**Training**		
	Training of designers to understand the causes and consequences of common cause failures.	None	5
6	**Environmental**		
6.1	For electrical/electronic systems, prevention of contamination and electromagnetic disturbances (EMI) to protect against common cause failures in accordance with appropriate standards (e.g. IEC 61326-3-1).	25	25
6.2	Other Influences Consideration of the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards).	10	10
	Total	85	Max. 100

NOTE External measures e.g. for protection against overvoltage and EMI are integrated which are not illustrated in Figure I.3.

Sufficient measures against CCF require a minimum score of 65, so for example B the score of 85 is sufficient to fulfil the requirements against CCF.

The characteristics of category 3 are fulfilled because a single fault in any of the parts does not lead to the loss of the safety function. Whenever reasonably practicable the single fault is detected at or before the next demand upon the safety function, the diagnostic coverage (DC_{avg}) is in the range 60 % to 90 %, the measures against CCF are sufficient and the equivalent $MTTF_D$ for each channel is "high".

Input data for Figure 12: $MTTF_D$ for the channel is "high" (37 years), DC_{avg} is "low" and category is 3.

Using Figure 12 this can be interpreted as performance level d.

Application of Annex K (use 36 years) gives an average probability of a dangerous failure per hour (PFH_D) of $5{,}16 \times 10^{-7}$/h and PL d.

This result matches the required performance level d according to I.2. Control circuit B therefore satisfies the requirements for risk reduction of the example B application of I.2 with S2, F2, P1 and PL_r d.

Annex J
(informative)

Example of SRESW realisation

J.1 Description of example

In Annex J the process steps for realizing the SRESW of an SRP/CS for PL_r d are presented. The SRP/CS is interfaced with the machine equipment. It ensures

— the acquisition of information sent by the various sensors,

— the processing required to operate the power control elements taking into account the safety requirements, and

— the piloting of the power control elements.

The function diagram of this application's SRESW is as shown in Figure J.1.

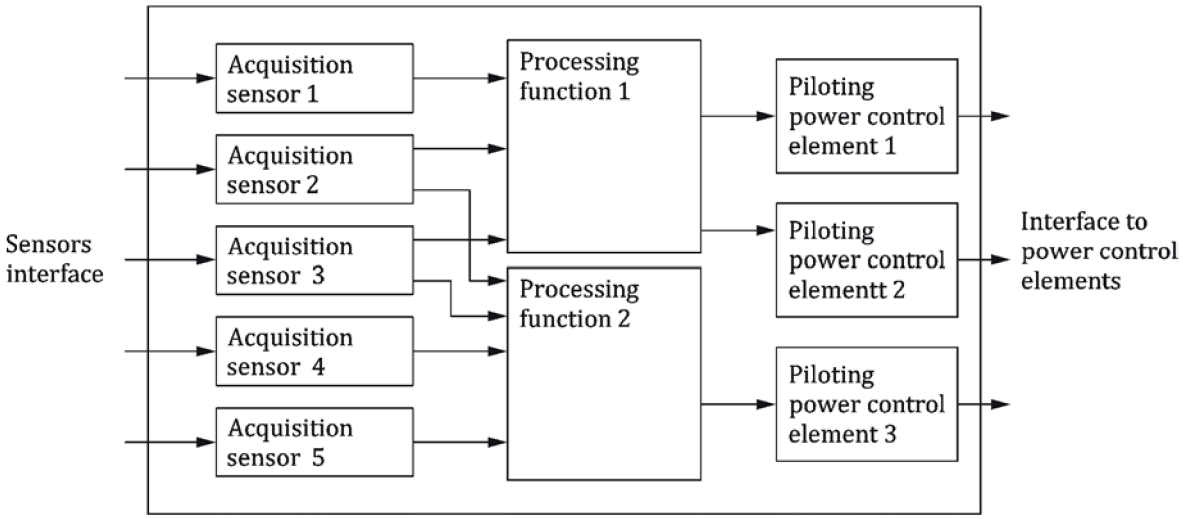


Figure J.1 — Function block level design of software example

J.2 Application of V-model of software safety lifecycle

Table J.1 presents the development activities, their corresponding verification steps, and the related documentation. These activities follow the V-model of software safety lifecycle according to Figure 14a..

Table J.1 — Activities and documents within software safety lifecycle

Development activity	Lifecycle activity	Associated documentation
machine aspect (hardware and software): identification of the functions involving the SRP/CS	— identification of safety functions	Output: — safety requirements specification (SRS)
architecture aspect (hardware and software): definition of the control architecture with sensors and power control elements	— comments upon safety characteristics of chosen components — planning of the test of the SRS	Output: — definition of the control architecture — test plan for SRS
software specification aspect: — specification of the requirements of the safety-related software (SRSS), including — transcription of machine functions into software functions	— review of the descriptions SRSS against SRS (see J.3) — planning of the test of the SRSS against the SRS	Input: — safety requirements specification (SRS) Output: — software design specification (SDS) including software descriptions — test plan for the SDS — documentation of review activity
software architecture aspect: Software system design, including to detail the functions into functional blocks	— review of the system design against the SDS including definition of critical blocks which are subject of greater review and validation effort — planning of the test of the software system design	Input: — SDS Output: — software system design specification (SSDS) including function block modelling — test plan for the SSDS — documentation of review activity
design of the software modules	— review of the software module design against the SSDS. — planning of the test of the software modules	Input: — SSDS Output: — module design specification (MDS) — test plan for the MDS — documentation of review activity
coding aspect: coding of non-existing software modules according to the programming rules (see J.4)	— review of the code against the MDS — verification of functions and compliance with rules	Input: — MDS Output: — reviewed code including Encoding comments in the code — documentation of review activity
NOTE Each test plan contains — correspondence matrix which cross-references specification paragraphs and tests; — test sheets comprising test scenario and comments upon results achieved.		

Table J.1 *(continued)*

Development activity	Lifecycle activity	Associated documentation
validation aspect: — module test	test of the software modules against the MDS according to the test plan for the MDS including — verification of the test coverage — verification of the test results	Input: — reviewed code — MDS — test plan for the MDS Output: — tested software modules — documentation of test activity
validation aspect: — software integration testing	test of the integrated software against the SSDS according to the test plan for the SSDS including — verification of the test coverage — verification of the test results The test may include the final hardware (if possible).	Input: — tested software modules — SSDS — test plan for the MDS Output: — tested integration — documentation of test activity
validation aspect: — validation of the SRP/CS making of test scenarios: — operation aspect of functions — behaviour-on-failure aspect	test of the integrated software and hardware (the SRP/CS) against the SDS according to the test plan for the SDS including — verification of the test coverage — verification of the test results The test may include the final hardware (if possible).	Input: — SDS — test plan for the SDS Output: — validated software (of the SRP/CS) — documentation of test activity
NOTE Each test plan contains — correspondence matrix which cross-references specification paragraphs and tests; — test sheets comprising test scenario and comments upon results achieved.		

J.3 Verification of software specification at different levels (i.e. SDS, SSDS, MDS)

As part of the software safety lifecycle according to Figure 14a, the verification activities at each level of the software specifications consists in reading the specifications so as to verify that all the sensitive points are properly described. The following should be considered when verifying each software function:

a) limiting the cases of erroneous interpretation of the software specifications;

b) avoiding gaps in the specifications resulting in an unknown behaviour of the SRP/CS;

c) precisely defining conditions for activation and de-activation of functions;

d) precisely guaranteeing that all the possible cases are handled;

e) consistency tests;

f) the different parameterizing cases;

g) the reaction following a failure.

J.4 Example of programming rules

In general it should be possible to identify the software version. Modifications should be documented with author, date and type of modification. Concerning the programming rules the following rules can be differentiated.

a) **Programming rules at level of the program structure**

The programming should be structured so as to display a consistent and understandable general skeleton allowing the different processing to be easily localized. This implies

1) use of templates for typical program or function blocks,

2) partitioning of the program into segments in order to identify main parts corresponding to “inputs”, “processing” and “outputs”,

3) comments on each program section in the source of the program to facilitate the updating of the comment in case of modification,

4) description of the role a function block has when calling this block,

5) that memory location should be used only by one single kind of data type and be marked by unique labels, and

6) that the working sequence should not depend on variables such as a jump address calculated at runtime of the program, conditional jumps being authorized.

b) **Programming rules regarding the use of variables**

— The activation or de-activation of any output should take place only once (centralized conditions).

— The program should be structured such that the equations for updating a variable are centralized.

— Each global variable, input or output should have a mnemonic name explicit enough and be described by a comment within the source.

c) **Programming rules at level of a function block**

1) Function blocks that have been validated by the supplier of the SRP/CS should be used. It should be checked that the assumed operating conditions for these validated blocks correspond to the conditions of the program..

2) The size of the coded block should be limited to the following guideline values:

— parameters – maximum eight digital and two integer inputs, one output;

— in function code – maximum 10 local variables, maximum 20 Boolean equations.

3) The function blocks should not modify the global variables.

4) Each value should be compared to expected pre-set benchmarks to ensure its validity.

5) The input parameters of a function block should be checked for inconsistencies.

6) Each fault code should be accessible and allow a clear identification of the original fault.

7) The fault codes and the state of the block after fault detection should be described by comments.

8) The resetting of the block or the restoration of a normal state should be described by comments.

Annex K
(informative)

Numerical representation of Figure 12

See Table K.1.

Table K.1 — Numerical representation of Figure 12

$MTTF_D$ for each channel	Average probability of a dangerous failure per hour, PFH_D (1/h) and corresponding performance level													
	Cat. B		**Cat. 1**	**Cat. 2**		**Cat. 2**		**Cat. 3**		**Cat. 3**		**Cat. 4**		
years	DC_{avg} = none		DC_{avg} = none	DC_{avg} = low		DC_{avg} = medium		DC_{avg} = low		DC_{avg} = medium		DC_{avg} = high		
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			
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			

NOTE 1 If for category 2 the demand rate is less than or equal to 1/25 of the test rate (see 6.1.8), then the PFH_D values stated in the Table K.1 for category 2 multiplied by a factor of 1,1 can be used as a worst-case estimate.

NOTE 2 The calculating of the PFH_D-values was based on following DC_{avg}:

— DC_{avg} = low, calculated with 60 %;

— DC_{avg} = medium, calculated with 90 %;

— DC_{avg} = high, calculated with 99 %.

Table K.1 *(continued)*

$MTTF_D$ for each channel	Average probability of a dangerous failure per hour, PFH_D (1/h) and corresponding performance level																	
	Cat. B		**Cat. 1**		**Cat. 2**		**Cat. 2**		**Cat. 3**		**Cat. 3**		**Cat. 4**	
years	DC_{avg} = none		DC_{avg} = none		DC_{avg} = low		DC_{avg} = medium		DC_{avg} = low		DC_{avg} = medium		DC_{avg} = high	
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
180													$1{,}33 \times 10^{-8}$	e

NOTE 1 If for category 2 the demand rate is less than or equal to 1/25 of the test rate (see 6.1.8), then the PFH_D values stated in the Table K.1 for category 2 multiplied by a factor of 1,1 can be used as a worst-case estimate.

NOTE 2 The calculating of the PFH_D-values was based on following DC_{avg}:

— DC_{avg} = low, calculated with 60 %;

— DC_{avg} = medium, calculated with 90 %;

— DC_{avg} = high, calculated with 99 %.

Table K.1 *(continued)*

$MTTF_D$ for each channel	Average probability of a dangerous failure per hour, PFH_D (1/h) and corresponding performance level						
	Cat. B	**Cat. 1**	**Cat. 2**	**Cat. 2**	**Cat. 3**	**Cat. 3**	**Cat. 4**
years	DC_{avg} = none	DC_{avg} = none	DC_{avg} = low	DC_{avg} = medium	DC_{avg} = low	DC_{avg} = medium	DC_{avg} = high
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

NOTE 1 If for category 2 the demand rate is less than or equal to 1/25 of the test rate (see 6.1.8), then the PFH_D values stated in the Table K.1 for category 2 multiplied by a factor of 1,1 can be used as a worst-case estimate.

NOTE 2 The calculating of the PFH_D-values was based on following DC_{avg}:

— DC_{avg} = low, calculated with 60 %;

— DC_{avg} = medium, calculated with 90 %;

— DC_{avg} = high, calculated with 99 %.

Table K.1 *(continued)*

$MTTF_D$ for each channel	Average probability of a dangerous failure per hour, PFH_D (1/h) and corresponding performance level							
	Cat. B	**Cat. 1**	**Cat. 2**	**Cat. 2**	**Cat. 3**	**Cat. 3**	**Cat. 4**	
years	DC_{avg} = none	DC_{avg} = none	DC_{avg} = low	DC_{avg} = medium	DC_{avg} = low	DC_{avg} = medium	DC_{avg} = high	
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

NOTE 1 If for category 2 the demand rate is less than or equal to 1/25 of the test rate (see 6.1.8), then the PFH_D values stated in the Table K.1 for category 2 multiplied by a factor of 1,1 can be used as a worst-case estimate.

NOTE 2 The calculating of the PFH_D-values was based on following DC_{avg}:

— DC_{avg} = low, calculated with 60 %;

— DC_{avg} = medium, calculated with 90 %;

— DC_{avg} = high, calculated with 99 %.

Annex L
(informative)

EMC immunity

The following routes provide guidance to fulfil EMC immunity measures for an SRP/CS or subsystems. At least one or more routes should be selected and fully applied:

— Route A: follow the EMC requirements of the relevant product standard (see IEC 61000-6-7:2014, 4.1, 1st sentence). Examples of product standards are IEC 61326 3 1 or 61800-5-2);

— Route B: for PL_r a and b, follow the EMC requirements of IEC 61000-6-2;

— Route C: for PL_r c, d and e implement EMC measures to achieve a score of at least 280 (of possible 400) according to Table "EMC" L.1 (see IEC 61000-6-7, 4.1, Note 1); for PL_r e, this route can only be applied if the requirements of category 4 are additionally fulfilled;

— Route D: follow IEC 61000-6-7 or other generic EMC standards for functional safety.

For electromechanical components with integrated active electronic the effect of EMC on the execution of the safety functions should be analysed and the relevant measures to achieve EMC should be implemented. If route C is selected, the measures listed in Table L.1 should be evaluated according to their effectiveness to avoid or control EMC effects. Engineering judgement should prove (e.g. using FMEA techniques) those typical causes for EMC are reduced as much as reasonably possible. The selected routes/measures should be clearly documented with adequate proof of compliance to the selected route.

Where tests are applied for validation, they should ensure that the safety function is exercised and exposed to the EMC Immunity for an adequate duration to demonstrate no susceptibilities are present.

Table L.1 — Measures to achieve EMC for safety-related components and other electrical/ electronic parts

Measures to achieve EMC	Score[a]
Safety-related sensors and their harness	
application of the measures described in Annex H of IEC 60204-1 and/or IEC 61800-3	10
analog voltage signals, angle encoder shielded and grounded and/or twisted cables for sensors and safety-related input/output-signals (cable shields are flat grounded in low impedance close to the components)	20
harnesses and wiring of low voltage DC between components is in twisted pair cabling	10
Safety-related IO system (central or decentral or integrated in the PLC)	
installed in a shielded and bonded cabinet or components in a shielded and bonded housing	20

NOTE Redundant channels in Table L.1 means functional channel and test channel in category 2 or redundant functional channels in categories 3 and 4.

[a] Where technological measures are not relevant, scores attached to this column can be considered in the comprehensive calculation.

[b] The zones can be located inside one cabinet or separated into several cabinets.

Table L.1 *(continued)*

Measures to achieve EMC	Score[a]
Control system and/or specific components are be divided into zones[b], e.g. a) mains supply and power distribution; b) strong interferers e.g. mains filter, mains chokes, heating components, high power supplies and motor cables: c) sensitive components e.g. low voltage power supplies, PLCs, data busses, sensors and low voltage actuators.	20
PLC as part of SRP/CS	
installed in a shielded and bonded cabinet or components in a shielded and bonded housing	10
category 3/4 for PL_r d/e with diverse PLC in the same enclosure separated with sufficient distance	10
category 3/4 for PL_r d/e with redundant PLC in different enclosures	20
category 3/4 for PL_r d/e with diverse channels (e.g. PLC and discrete logic) or using safety PLC	20
Safety-related actuator and their wire harness	
application of the measures described in Annex H of IEC 60204-1 and/or usage of IEC 61800-3:	10
Other components and wiring with relevant disturbance level	
bonded cables for motors or sinewave filter between motor and inverter or equivalent measures	20
RF-filter, overvoltage and transient protection (e.g. filter, transient-voltage suppression diode, optocoupler, ferrites) for safety-related signals	20
EMC filters (as per manufacturers installation instructions or specifically intended for the application) for power mains (e.g. overvoltage and transient protection)	20
application of the measures described in Annex H of IEC 60204-1 and/or usage of IEC 61800-3	10
Engineering, programming, training, field observation	
components fulfil at minimum, IEC 61000-6-2 (mentioned in manufacturers documentation)	10
risk analysis for EMC (see example in Table L.2) and risk assessment with a final report	20
diverse redundant channels (see Note)	20
Separation of EMC sources and sensitive components e.g. — separate routing and location of power lines and signal lines — separate metal cabinets for power electronics and low power electronics — following the instructions by the manufacturer; if no instructions are available use distance ≥ 20 cm between power components and sensitive components or alternatively use shielded and bonded components in shorter distance with field experience of low EMC influences	30
software/firmware with diagnostic on component or system level, e.g. by plausibility checks, data cross monitoring in case of redundancy, self-tests	20
designers have experience or have been trained (with training documentation, e.g. certificate of training) to understand the causes and consequences of EMC	20
reuse of a specific functional safety system design previously used in a similar electromagnetic environment and found to be highly reliable without known EMC issues	30
Power supply of the SRP/CS	
low voltage AC or DC power supplies with insulated transformers related to IEC 61558, and/or SELV supplies related to IEC 60950, and/or SELV or PELV supplies related to IEC 50178	20

NOTE Redundant channels in Table L.1 means functional channel and test channel in category 2 or redundant functional channels in categories 3 and 4.

[a] Where technological measures are not relevant, scores attached to this column can be considered in the comprehensive calculation.

[b] The zones can be located inside one cabinet or separated into several cabinets.

Table L.1 *(continued)*

Measures to achieve EMC		Score[a]
redundant PLC with separate switching power supply for the SRP/CS of channel 1/2		10
Total score 400	**Measures for EMC immunity** [a]	
280 or better	Meets the requirements	
Less than 280	Process failed ⇒ choose additional measures or select route one or more above mentioned routes	

NOTE Redundant channels in Table L.1 means functional channel and test channel in category 2 or redundant functional channels in categories 3 and 4.

[a] Where technological measures are not relevant, scores attached to this column can be considered in the comprehensive calculation.

[b] The zones can be located inside one cabinet or separated into several cabinets.

Table L.2 — Example of a risk analysis for EMC

Source of disturbance	EMC-phenomenon	Distance source/ sink	Sensitive component	Risk consequence	Solution of problem
power supply	inductive coupling capacitive coupling	<20 cm	signal lines sensor lines	wrong measurement values malfunction	higher distance shielding filtering shielded cable
inverter	capacitive coupling	<40 cm	all cables all sensors programmable logic ADC-converter	sporadic failure malfunction loss of function	higher distance filtering sine filter shielded cable ferrite clamps
power mains	conductive coupling capacitive coupling high power transients	—	sensor programmable logic motor drive	disturbance malfunction damage undefined state	mains filter surge filter twisted cable filtering transient protection
inductive loads	inductive coupling conductive coupling capacitive coupling high power transients	—	all cables all sensors programmable logic ADC-converter motor drive	disturbance malfunction damage undefined state	filtering twisted cable transient protection
All EMC	all couplings	—	all active electronic	—	diagnostic system leads into safe state

Annex M
(informative)

Additional information for safety requirements specification

Table M.1 and Table M.2 list some typical safety functions and their characteristics and safety-related parameters, while making reference to other International Standards whose requirements relate to the safety function, characteristic or parameter.

As most of the safety functions referenced in Table M.1 and Table M.2 relate to electrical standards, the applicable requirements need to be adapted when other technologies or energy sources (e.g. hydraulic, pneumatic) are used.

Table M.1 — Examples of International Standards applicable to typical machine safety functions and certain of their characteristics

Safety function/ characteristic	Requirement(s)		For additional information
	This document	ISO 12100:2010	
safety-related stop function	5.2.3.1	3.26, 6.2.11.3	IEC 60204-1:2016, 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
manual reset function	5.2.3.2	—	IEC 62046:2018 ISO 13850:2015
start/restart function	5.2.3.3	5.2.11.3, 5.2.11.4	IEC 60204-1:2016, 9.2.3.2, 9.2.3.3, 9.2.3.10 IEC 62046:2018
local control function	5.2.3.4	5.2.11.8, 5.2.11.10	IEC 60204-1:2016, 10.1.5
muting function	5.2.3.5	—	IEC 62046:2018, 5.7
hold-to-run function		5.2.11.8 b)	IEC 60204-1:2016, 9.2.3.7
enabling device function		—	IEC 60204-1:2016, 9.2.3.9, 10.9
prevention of unexpected start-up	—	5.2.11.4	ISO 14118:2017 IEC 60204-1:2016, 5.4 IEC 61800-5-2:2016
escape and rescue of trapped persons	—	5.3.5.3	ISO 14119:2013, 5.7.5.2
isolation and energy dissipation function	—	5.3.5.4	ISO 14118:2017 IEC 60204-1:2016, 5.3, 6.3.1
operating mode selection	5.2.3.8	5.2.11.8, 5.2.11.10	IEC 60204-1: 2016, 9.2.3.5
interaction between different safety-related parts of control systems	—	5.2.11.1 (last sentence)	IEC 60204-1:2016 ISO 11161:2007 ISO 13850:2015

[a] Complementary protective measure, see ISO 12100:2010.

Table M.1 *(continued)*

Safety function/ characteristic	Requirement(s)		For additional information
	This document	ISO 12100:2010	
monitoring of parameterization of safety-related input values	7.5	—	—
emergency stop function[a]	—	5.3.5.2	ISO 13850:2015 IEC 60204-1:2016, 9.2.3.4.2 IEC 61800-5-2:2016
monitoring or limiting speed; torque; power; position (e.g. position limiting device); movement; momentum; pressure; stopping time; stopping distance	—	—	ISO 10218-1:2011 IEC 61800-5-2:2016 ISO/TS 15066:2016
safe brake control	—	—	IEC 61800-5-2:2016

[a] Complementary protective measure, see ISO 12100:2010.

Table M.2 — Examples of International Standards giving requirements for certain safety functions and safety-related parameters

Safety function/ safety-related parameter	Requirement		For additional information, see:
	This document	ISO 12100:2010	
response time	5.2 13.2	—	ISO 13855:2010, 3.2, A.3, A.4 IEC 62046:2018, 4.4.2.2
safety-related parameter such as speed, temperature, pressure, position or torque	5.2.3.6	5.2.11.7.3	IEC 60204-1:2016, 7.1, 9.3.2 IEC 61800-5-2:201610218-
fluctuations, loss and restoration of power sources	5.2.3.7	5.2.11.4 5.2.11.5	IEC 60204-1:2016, 4.3, 7.1, 7.5 ISO 4413:2010 ISO 4414:2010
indications and alarms	—	5.2.3.6 and 5.2.3.7	ISO 7731:2008 ISO 11428:1996 ISO 11429:1996 IEC 61310-1:2007 IEC 60204-1:2016, 10.3, 10.4 IEC 61131-3:2013 IEC 62061:2015

Annex N
(informative)

Avoiding of systematic failure in software-design

N.1 Selection of fault avoiding measures for the design of safety-related software

The following tables give guidance for the selection of fault avoiding measures for safety-related embedded software (SRESW) or safety-related application software (SRASW). Table N.1 gives an overview for the clustering of the selection measures. Table N.2 should be used for SRASW in LVL, and Table N.3 should be used for SRESW & SRASW in FVL.

Table N.1 — Clustering of cases for the selection of measures

PL_r	Category	Part	Case
a and b	B	Functional channel	Case 1
a, b and c	2	Test channel	
a and b	2	Functional channel	
a and b	3	Pre assessed platform	
a and b	3	Channel 1 AND 2	
a, b and c	3	Channel 1 OR 2	
c	2	Functional channel	Case 2
c	3	Pre assessed platform	
c	3	Channel 1 AND 2	
d	2	Test channel	
d	3 and 4	Channel 1 OR 2	
d	2	Functional channel	Case 3
d	3 and 4	Pre assessed platform	
d	3 and 4	Channel 1 AND 2	
e	3 and 4	Channel 1 OR 2	
e	3 and 4	Pre assessed platform	Case 4[a]
e	3 and 4	Channel 1 AND 2	
[a] The only difference in both lines of case 4 are the requirements for the selection of tools.			

EXAMPLE For a subsystem with PL_r of c and category 2 case 2 is chosen for the functional channel and case 1 is chosen for the test channel.

For Tables N.3 and N.4, the following abbreviations are used:

— r = recommended means that the use of this measure improves the quality of the software, but its use is not mandatory;

— m = mandatory means that this measure should always be used;

— "-" means that this measure is not required.

— channel 1 AND 2 means that SRESW or SRASW is used in both functional channels of category 3 or 4;

— channel 1 OR 2 means that SRESW or SRASW is only used in one of two functional channels of category 3 or 4;

— pre-assessed platform means that the hardware and the internal software (SRESW) is designed for safety applications and already assessed to comply with this document or IEC 61508/62061 for the required performance level.

The fault avoiding measures for SRESW and SRASW in Table N.2 and Table N.3 are graded according to the category and PL:

a) PL a and b are typically realized using a category B structure with software used in the logic block of the functional channel.

b) PL c and d may be realized using a category 2 structure with software used in the logic block of the functional channel or in the test equipment block in the testing channel. For the testing channel the requirements are reduced by one performance level.

c) PL d and e may be realized using a category 3 structure with software used in the logic block of the functional channels. “Channel 1 and channel 2” means that software is only used in one or both functional channels. “Channel 1 or channel 2” means that software is used only in one of both functional channels, in this case the requirements are reduced by one performance level.

d) SRASW in PL d and e may also be realized using a pre-assessed platform (safety-related hardware in combination with operating system and programming tool). In this case, only one application software is used for both functional channels.

Table N.2 — Selection of measures for SRASW in LVL

	Description: r = recommended, m = mandatory (with low, medium or high effectiveness), “-“ = not required				
	Case	**Case 1**	**Case 2**	**Case 3**	**Case 4**
1	These basic measures should be applied:				
a)	Development lifecycle with verification and validation activities, see Figure 14a and Figure 14b	m	m	m	m
b)	Documentation of specification and design				
c)	Modular and structured programming				
d)	Functional testing; (e.g. black box testing)				
e)	Appropriate development activities after modifications				
2	The safety-related software specification should be reviewed (see also Annex J), made available to every person involved in the lifecycle of the V-modell and should contain the description of:				
a)	Safety functions with required PL and associated operating modes	-	m	m	m
b)	Performance criteria, e.g. reaction times,				
c)	Hardware architecture with external signal interfaces, and				
d)	Detection and control of hardware failure.				
3	Selection of tools, libraries, languages:				
a)	Tools should be suitable for the application.	-	m	m	m
b)	For PL e achieved with one component and its tool, the tool should comply with the appropriate safety standard. * If two diverse components with diverse tools are used, confidence from use may be sufficient (for PL e).	-	-	-	m[a]
c)	Technical features which detect conditions that could cause systematic error (such as data type mismatch, ambiguous dynamic memory allocation, incomplete called interfaces, recursion, pointer arithmetic) should be used.	-	m	m	m
d)	Checks should mainly be carried out during compile time and not only at runtime. Tools should enforce language subsets and coding guidelines or at least supervise or guide the developer using them.				

Table N.2 *(continued)*

	Description: r = recommended, m = mandatory (with low, medium or high effectiveness), "-" = not required				
	Case	**Case 1**	**Case 2**	**Case 3**	**Case 4**
e)	Whenever reasonable and practicable, validated function block (FB) libraries should be used – either safety-related FB libraries provided by the tool manufacturer or validated application specific FB libraries and in conformity with this part of ISO 13849.	-	r	r	r
f)	A justified LVL-subset suitable for a modular approach should be used, e.g. accepted subset of IEC 61131-3 languages.				
4	Software design should feature:				
a)	Semi-formal methods to describe data and control flow, e.g. state diagram or program flow chart,	-	m	m	m
b)	Modular and structured programming predominantly realized by function blocks deriving from safety-related validated function block libraries or other modularity structure to achieve easy code reading and testability,				
c)	Function blocks of limited size of coding,				
d)	Code execution inside function block which should have one entry and one exit point,				
e)	Architecture model of three stages, Inputs → Processing → Outputs (see Figure 10 and Annex J),				
f)	Assignment of a safety output at only one program location, and				
g)	use of techniques for detection of hardware failure and for defensive programming within input, processing and output blocks which lead to safe state.				
5	Where SRASW and non-SRASW are combined in one component:				
a)	SRASW and non-SRASW should be coded in different function blocks with well-defined data links;	-	m	m	m
b)	There should be no logical combination of non-safety-related and safety-related data which could lead to downgrading of the integrity of safety-related signals, for example, combining safety-related and non-safety-related signals by a logical "OR" where the result controls safety-related signals.				
6	Software implementation/coding:				
a)	Code should be readable, understandable and testable and, because of this symbolic variables (instead of explicit hardware addresses) should be used;	-	m	m	m
b)	Justified or accepted coding guidelines should be used (see also Annex J);				
c)	Data integrity and plausibility checks (e.g. range checks.) available on application layer (defensive programming) should be used;	-	r	r	r
d)	Code should be tested by simulation;				
e)	Verification should be by control and data flow analysis for PL d or e.	-	-	r	r
7	Testing:				
a)	The appropriate validation method is black-box testing of functional behaviour and performance criteria (e.g. timing performance);	-	m	m	m
b)	I/O testing should ensure that safety-related signals are correctly used within SRASW.				
c)	Test planning is recommended and should include test cases with completion criteria and required tools;	-	r	r	r
d)	For PL d or e, test case execution from boundary value analysis is recommended;	-	-	r	r
8	Documentation:				

Table N.2 *(continued)*

	Description: r = recommended, m = mandatory (with low, medium or high effectiveness), "-" = not required				
	Case	**Case 1**	**Case 2**	**Case 3**	**Case 4**
a)	All lifecycle and modification activities should be documented;	-	m	m	m
b)	Documentation should be complete, available, readable and understandable;				
c)	Code documentation within source text should contain module headers with legal entity, functional and I/O description, version and version of used library function blocks, and sufficient comments of networks/statement and declaration lines.				
9	Validation (only necessary for application-specific code, and not for validated library functions)				
	Validation should be performed by review, inspection, walkthrough or other appropriate activities.	-	m	m	m
10	Configuration management:				
	It is highly recommended that procedures and data backup be established to identify and archive documents, software modules, verification/validation results and tool configuration related to a specific SRASW version.	-	m	m	m
11	Modifications:				
	After modifications of SRASW, impact analysis should be performed to ensure specification. Appropriate lifecycle activities should be performed after modifications. Access rights to modifications should be controlled and modification history should be documented. NOTE 1 Modification does not affect systems already in use.	-	m	m	m

Table N.3 — Selection of measures for SRESW and/or SRASW in FVL

	Description: r = recommended, m = mandatory, "-" = not required				
	Case	**Case 1**	**Case 2**	**Case 3**	**Case 4**
1	These basic measures should be applied:				
a)	Software safety lifecycle with verification and validation activities, see Figure 14a	m	m	m	m [a]
b)	Documentation of specification and design, e.g. software design specification, software system design specification, module design specification, code listings including comments;				
c)	Modular and structured design and coding, e.g. hierarchy and limitation of functionality, clear program structure, definition of interfaces, well-structured call-graph, avoidance of interrupts, use of coding guidelines;				
d)	Control of systematic failures, e.g. program sequence monitoring, controlling errors in the data communication process (see G.2);				
e)	Where using software-based measures for control of random hardware failures, verification of correct implementation, e.g. correct implementation of diagnostic measures, RAM/ROM/CPU tests, hardware tests, plausibility checks;				
f)	Functional testing, e.g. black box testing, e.g. verification of correct output data based on input data (valid, invalid and border values), compatibility of interfaces, timing;				
g)	Appropriate software safety lifecycle activities after modifications, e.g. based on an impact analysis.				
2	These additional measures should be applied:				

[a] When using diversity in specification, design and coding, for the two channels used in SRP/CS with category 3 or 4, PL_r e can be achieved with the above-mentioned basic and additional measures for PL_r of c or d.

NOTE 2 For SRESW with diversity in design and coding, for components used in SRP/CS with category 3 or 4, the effort involved in taking measures to avoid systematic failures can be reduced by, for example, reviewing parts of the software only by considering structural aspects instead of checking each line.

Table N.3 *(continued)*

	Description: r = recommended, m = mandatory, "-" = not required				
	Case	**Case 1**	**Case 2**	**Case 3**	**Case 4**
a)	Project management and quality management system comparable to, e.g. IEC 61508, e.g. definition of workflow, responsibilities, configuration management, use of tools;	-	m (see Note 2)	m (see Note 2)	m[a]
b)	Documentation of all relevant activities during software safety lifecycle, e.g. documentation of reviews, testing, validation and verification;				
c)	Configuration management to identify all configuration items and documents related to a SRESW release, e.g. version control of code listings, modules, design documents, test plans, release control, archiving;				
d)	Structured specification with safety requirements and design;				
e)	Use of suitable programming languages and computer-based tools with confidence from use, e.g. programmers are trained to use the tools;				
f)	Modular and structured programming, separation from non-safety-related software, limited module sizes with fully defined interfaces, use of design and coding standards;				
g)	Coding verification by walk-through/review with control flow analysis (to check for faults, quality of comments, compliance with coding guidelines, clarity, readability, completeness);				
h)	Extended functional testing, e.g. grey box testing, performance testing or simulation, e.g. using input unspecified data, extreme environmental conditions, full load, testing based on knowledge of internal coding;				
i)	Impact analysis and appropriate software safety lifecycle activities after modifications.				
j)	SRESW for components with PL_r = e should comply with IEC 61508-3:2010, Clause 7, appropriate for SIL 3.	-	-	-	m[a]

[a] When using diversity in specification, design and coding, for the two channels used in SRP/CS with category 3 or 4, PL_r e can be achieved with the above-mentioned basic and additional measures for PL_r of c or d.

NOTE 2 For SRESW with diversity in design and coding, for components used in SRP/CS with category 3 or 4, the effort involved in taking measures to avoid systematic failures can be reduced by, for example, reviewing parts of the software only by considering structural aspects instead of checking each line.

N.2 Example for software validation

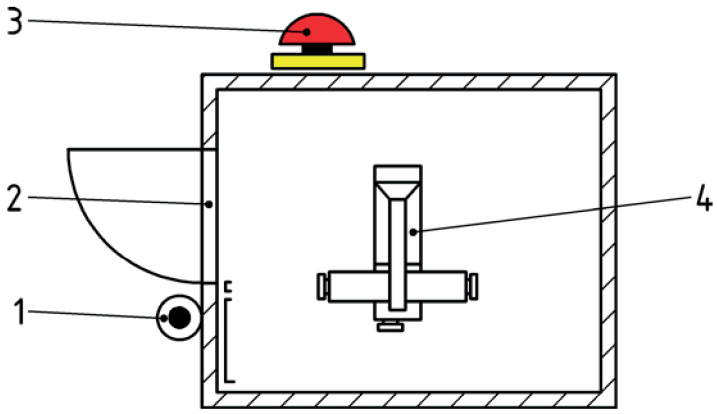
N.2.1 Example for Software validation

In this validation example pre-assessed software modules are used. The validation is done by test cases at the inputs of the pre-assessed software modules to check their usage in the context of the whole application software. The number of test cases do not claim completeness.

N.2.2 Coding guidelines

Coding should be done according to the coding guidelines required by the manufacturer of the software platform, if relevant, or according to an "in house guideline" but not being in contradiction with those coding guidelines of the software platform used by the user.

N.2.3 Specification of safety functions



Key

1 ACK1 - acknowledge button of interlocking guard door 1 (accessible)
2 GD1 - interlocking guard door 1
3 ES1 - emergency stop 1
4 M1- motor 1 stopped with STO (safe torque off) in PL d (over safety bus PL e)

Figure N.1 — Safety functions

The safety function and complementary operate as follows:

— If the interlocking guard door 1 (GD1) is opened (accessible area) then M1 will be switched off (STO is realised in PL d). GD1 is acknowledged with the button ACK1. Acknowledgement only possible when GD1 is closed.

— Emergency Stop (ES1) initiate an STO of motor M1 (PL_r = PL d).

If all safety-relevant requirements of the manufacturer of the safety PLC used are complied with, the simplified V-model is sufficient, see table N.4.

Table N.4 — General architecture model of the software

sensor	programmable Safety PLC			actuator
GD1 (redundant switch off of the interlocking guard (RESET interlocking guard) **ES1** (emergency stop)	Input (block) — Logic (block) — Output (block)			**M1** (drive with STO in PL d)
	Collection of the information for the various safety sensors through the inputs	Processing of the safety-related signals	Actuation of the drive elements through safety output	

N.2.4 Verification procedure of DC measures to be implemented in SRASW

N.2.4.1 General

To prove the DC value it is recommended to divide the software into blocks:

1) evaluation of the interlocking safety guard;

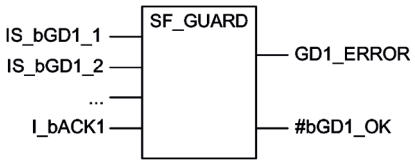
2) evaluation of emergency stop;

3) evaluation of enable / switch off of motor M1.

N.2.4.2 Evaluation of the interlocking safety guard

Table N.5 — FMEA of the interlocking safety guard

Relevant inputs				
description	I/O	Type	Info	description
GD1 Ch1: IS_bGD1_1	E 1.1	Bool	Discrepancy time to Ch 2 500 msec	Interlocking guard NC (positive opening)
GD1 Ch2: IS_bGD1_2	E 1.2	Bool	Discrepancy time to Ch 1 500 msec	Interlocking guard NC (positive opening)
ACK1: I_bACK1	E 1.3	Bool	NO	Acknowledgment interlocking guard GD1
Relevant Flags				
description	O	Type	Info	description
#bGD1_OK	O 1.1	Bool	NO	This release flag is used for subsequent processing.
GD1_ERROR	O 1.2	Bool	NO	This error flag is used for subsequent processing.

software blocks used			
Name	pre-assessed block of the SW platform	description	Info
SF_Guard	yes	pre-assessed software block for monitoring of the interlocking guard in PL d: When a fault is detected GD1_ERROR flag changes to High	

Prove of implemented DC measures by test cases (fault cause and effect analysis)			
Nr.	Fault injection	Safe state and fault reaction	Expected result

0	With no fault injection and no expected fault reaction:
	When the safety function is requested (by opening the interlocking guard door) IS_bGD1_1=LOW and IS_bGD1_2=LOW.
		#bGD1_OK = LOW and
		GD1_ERROR = LOW
			Yes/No

NOTE 1 Error-free state (initial situation / normal state before tests are performed, interlocking guard door is closed).			
1	Permanent HIGH Signal on IS_bGD1_1 (E 1.1) When the safety function is requested (by opening the interlocking guard door) IS_bGD1_2 changing of the signal	Safe state with #bGD1_OK = LOW and initiated fault reaction GD1_ERROR = LOW changes to GD1_ERROR = HIGH	Yes/No
NOTE 2 Message error E 1.1, block cannot be acknowledged. If the door is closed again, the block can be acknowledged again.			
2	Permanent HIGH signal on IS_bGD1_2 (E 1.2). When the safety function is requested (by opening the interlocking guard door) IS_bGD1_1 changing of signal	Safe state with #bGD1_OK = LOW and initiated fault reaction GD1_ERROR = LOW changes to GD1_ERROR = HIGH	Yes/No
NOTE 3 Message error E 1.2, block cannot be acknowledged. If the door is closed again, the block can be acknowledged again.			

Table N.5 *(continued)*

3	LOW signal on IS_bGD1_1 (E 1.1)	Safe state with #bGD1_OK = LOW and initiated fault reaction GD1_ERROR = LOW changes to GD1_ERROR = HIGH	Yes/No
NOTE 4 Message Error E 1.1, module cannot be acknowledged due to the closed-circuit current principle, even if the interlocking guard door is closed again.			
4	LOW Signal on IS_bGD1_2 (E 1.2)	Safe state with #bGD1_OK = LOW and initiated fault reaction GD1_ERROR = LOW changes to GD1_ERROR = HIGH	Yes/No
NOTE 5 Message Error E 1.2, module cannot be acknowledged due to the closed-circuit current principle, even if the interlocking guard door is closed again.			
5	IS_bGD1_1 changes the signal state outside the set discrepancy time to IS_bGD1_2	Safe state with #bGD1_OK = LOW and initiated fault reaction GD1_ERROR = LOW changes to GD1_ERROR = HIGH	Yes/No
NOTE 6 This diagnostic function is for protection against manipulation. The discrepancy error with GD1 module cannot be acknowledged. If the door is closed again, the module can be acknowledged.			
6	IS_bGD1_2 changes the signal state outside the set discrepancy time to IS_bGD1_1	Safe state with #bGD1_OK = LOW and initiated fault reaction GD1_ERROR = LOW changes to GD1_ERROR = HIGH	Yes/No
NOTE 7 This diagnostic function is for protection against manipulation. The discrepancy error with GD1 module cannot be acknowledged. If the door is closed again, the module can be acknowledged.			
7	ACK1 (E 1.3) permanent High Signal and GD1_ERROR = True	Even if the error is corrected, the block cannot be reset	Yes/No
NOTE 8 Acknowledgement is edge-controlled and not level-controlled. This diagnostic function is prevention measurement against manipulation.			
8	ACK1 (E 1.3) permanent Low Signal and GD1_ERROR = True	Even if the error is corrected, the block cannot be reset	Yes/No
NOTE 9 Acknowledgement is edge-controlled and not level-controlled. This diagnostic function is prevention measurement against manipulation.			

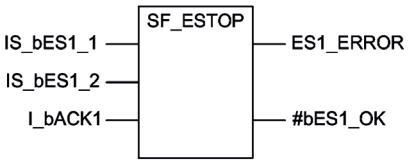
N.2.4.3 Evaluation of emergency stop

Table N.6 — FMEA of the emergency stop

Relevant inputs				
description	I/O	Type	Info	description
ES1 Ch1: IS_bES1_1	E 1.4	Bool	Discrepancy time to Ch 2 500 msec	Emergency stop NC (positive opening)
ES1 Ch2: IS_bES1_2	E 1.5	Bool	Discrepancy time to Ch 1 500 msec	Emergency stop NC (positive opening)
ACK1: I_bACK1	E 1.3	Bool	NO	Acknowledgment Emergency stop ES1
Relevant outputs/flags				

Table N.6 *(continued)*

description	O	Type	Info	description
#bES1_OK	O 1.3	Bool	NO	This release flag is used for subsequent processing.
ES1_ERROR	O 1.4	Bool	NO	This error flag is used for subsequent processing.

software blocks used			
Name	pre-assessed block of the SW platform	description	Info
SF_ESTOP	yes	pre-assessed software block for monitoring a two-channel signal In case of an error ES1_ERROR is set to High	

Prove of implemented DC measures by test cases (fault cause and effect analysis)			
Nr.	Fault injection	Safe state and fault reaction	Expected result

0	With no fault injection and no expected fault reaction:
	when the safety function is requested (actuation of the emergency stop) IS_bES1_1=LOW and IS_bES1_2=LOW.
		#bES1_OK = LOW and
		ES1_ERROR = LOW
			Yes/No

NOTE 1 Error-free state (initial situation / normal state before tests are performed, emergency stop is not requested).			
1	Permanent HIGH signal on IS_bES1_1 (E 1.4) when the safety function is requested (actuation of the emergency stop) and IS_bES1_2 changes signal NOTE 2 Message error E 1.4, block cannot be acknowledged. If the emergency stop is unlocked again, the block can be acknowledged again.	Safe state with #bES1_OK = LOW and initiated fault reaction ES1_ERROR = LOW changes to HIGH	Yes/No
NOTE 3 Message error E 1.4, block cannot be acknowledged. If the emergency stop is unlocked again, the block can be acknowledged again.			
2	permanent HIGH Signal on IS_bES1_2 (E 1.5). When the safety function is requested (actuation of the emergency stop) and IS_bES1_1 changes signal	Safe state with #bES1_OK = LOW and initiated fault reaction ES1_ERROR = LOW changes to HIGH	Yes/No
NOTE 4 Message error E 1.5, block cannot be acknowledged. If the emergency stop is unlocked again, the block can be acknowledged again.			
3	LOW Signal on IS_bES1_1 (E 1.4).	Safe state with #bES1_OK = LOW and initiated fault reaction ES1_ERROR = LOW changes to HIGH	Yes/No
NOTE 5 Message Error E 1.4, module cannot be acknowledged due to the closed-circuit current principle, even if the emergency stop is unlocked again.			
4	LOW Signal on IS_bES1_2 (E 1.5).	Safe state with #bES1_OK = LOW and initiated fault reaction ES1_ERROR = LOW changes to HIGH	Yes/No

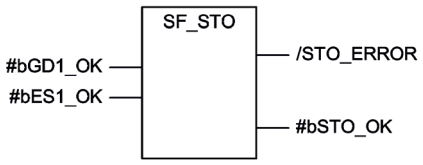
Table N.6 *(continued)*

NOTE 6 Message Error E 1.5, module cannot be acknowledged due to the closed-circuit current principle, even if the emergency stop is unlocked again.			
5	IS_bES1_1 (E 1.4) changes the signal state outside the set discrepancy time to IS_bES1_2	Safe state with #bES1_OK = LOW and initiated fault reaction ES1_ERROR = LOW changes to HIGH	Yes/No
NOTE 7 This diagnostic function is used to check the emergency stop operating element.			
6	IS_bES1_2 (E 1.5) changes the signal state outside the set discrepancy time to IS_bES1_1	Safe state with #bES1_OK = LOW and initiated fault reaction ES1_ERROR = LOW changes to HIGH	Yes/No
NOTE 8 This diagnostic function is used to check the emergency stop operating element.			

N.2.4.4 Evaluation of enable / switch off of motor M1

Table N.7 — FMEA of enable / switch off of motor M1

Relevant inputs / Relevant Flags				
description	I/O	Type	Info	description
#bGD1_OK	Flag GD1	Bool	NO	This release flag is used for subsequent processing.
#bES1_OK	Flag ES1	Bool	NO	This release flag is used for subsequent processing.

Software blocks used			
Name	pre-assessed block of the SW platform	description	Info
SF_STO	yes	This block has been pre-assessed to activate the STO via a BOOL. The feedback is automatically given in the block. If an error occurs, /STO_ERROR is set to Low.	

Relevant outputs/flags				
description	O	Type	Info	description
#bSTO_OK	O 1.5	BUS	pre-assessed according to PL d	via safety bus to inverter 1, activates STO
/STO_ERROR	O 1.6	Bool	NO	This error flag is used for subsequent processing.

Prove of implemented DC measures by test cases (fault cause and effect analysis)			
Nr.	Assumption	effect	Expected result
1	GD1_ERROR = High	#bGD1_OK = Low #bSTO_OK = Low /STO_ERROR = Low	Yes/No
NOTE 1 If error GD1_ ERROR is present then the inverter (FU) should also switch off.			
2	ES1_ERROR = High	#bES1_OK = Low #bSTO_OK = Low /STO_ERROR = Low	Yes/No
NOTE 2 If error ES1_ERROR is present then the inverter (FU) should also switch off.			

Table N.7 *(continued)*

3	#bGD1_OK = High and #bES1_OK = High	#bSTO_OK = High /STO_ERROR = High	Yes/No
remark: This is the error-free state.			
4	#bGD1_OK = High and #bES1_OK = Low	#bSTO_OK = Low /STO_ERROR = Low	Yes/No
remark:			
5	#bGD1_OK = Low and #bES1_OK = High	#bSTO_OK STO_IN = Low /STO_ERROR = Low	Yes/No
remark:			
6	#bGD1_OK = Low and #bES1_OK = Low	#bSTO_OK = Low /STO_ERROR = Low	Yes/No
remark:			
7	Error bus communication	#bSTO_OK = Low /STO_ERROR = High	Yes/No
NOTE 3 Serious error (e.g. in case of a serious error the controller should be restarted)			

In addition to prove of the DC, the following should be documented:

— Date: YYYYY-MM-DD (currently valid version/changes)

— Name: (responsible person)

— Software signature

— Hardware signature

— significant reaction times of the safety functions (possibly delay times).

ATTENTION — With safety software, the required PL_r should not be reduced by an OR function.

Annex O
(informative)

Safety-related values of components or parts of control systems

O.1 Definition of device types

O.1.1 General

Devices vary in terms of technology, application, availability and use of diagnostic mechanism and diagnostic information. As a result, different device types will be defined at this point.

Devices can generally be distinguished by the following features:

— device that can be used directly as a SRP/CS or subsystem element in a safety function because the manufacturer has already developed the device for this specific application (device type 1 and device type 4);

— device that is only defined and assessed as a SRP/CS or subsystem element through the user's design process (device type 2 and device type 3).

NOTE A safety function normally uses a variety of device types.

Table O.1 — Characteristic values of device types

Characteristic value	Device type				Comment
	1	2	3	4	
PL	X				ISO 13849-1
SIL					IEC 62061
PFH_D	X				ISO 13849-1 and IEC 62061
Category	X	X	X		ISO 13849-1 and IEC 62061
HFT					one of the characteristic values is required
$MTTF_D$		X			ISO 13849-1 and IEC 62061
λ_D					one of the characteristic values is required
MTTF					
MTBF					
B_{10d}			X		ISO 13849-1 and IEC 62061
B_{10}					one of the characteristic values is required
RDF		O[b]	O[b]		ISO 13849-1
SFF					IEC 62061[a]
T_{10d}	X	X		X	ISO 13849-1 and IEC 62061
T_M					Exactly one of the characteristic values is required.
X mandatory O optional					

[a] SFF (safe failure fraction) is defined as fraction of the overall failure rate of a subsystem that does not result in a dangerous failure in IEC 52061, 3.2.5.4.

[b] If there is no determined safety value from the manufacture (MTTFD or B10d).

O.1.2 Device type 1

Device type 1 has the highest integration level. Pre-designed safety systems with integrated diagnostics are typical. This type is SIL or PL-classified in line with the intended use. The manufacturer of the device specifies the classification.

Devices of this type are developed in accordance with safety standards (e.g. IEC 61508).

NOTE 1 Examples for device type 1: Safety light curtain, safety light grid, safety-related control system components, safe drives/drive functions, safety relays.

NOTE 2 Parameters may depend on other application-specific data (e.g. limitation of the maximum switching frequency).

O.1.3 Device type 2

Additional application data (circuit structure, diagnostic coverage (DC) and consideration of common cause failure (CCF)) are needed in order for the user to assess a safety function.

Devices of this type are not necessarily developed in accordance with safety standards; however, this does not exclude application in accordance with this document.

EXAMPLE For device type 2: Non-safety-related electronics, e.g. operational amplifier, proximity switch, pressure sensor, hydraulic valve.

O.1.4 Device type 3

Type 3 devices are components with a failure mode, which depends on the operating cycles.

Additional application data (number of operations, number of activations, circuit structure, diagnostic coverage (DC) and consideration of common cause failure (CCF)) are needed in order for the user to assess a safety function.

Devices of this type are not necessarily developed in accordance with safety standards; however, this does not exclude application in accordance with this document.

EXAMPLE For device type 3: Electromechanical components that are subject to wear, e.g. power contactors, switches, pneumatic valves, interlocking devices, control devices.

O.1.5 Device type 4

Device type 4 is a special case of device type 1. This type has non-random failures which lead to a dangerous fault, which means the probability of a dangerous fault occurring near PFH_D = 0. For components of this type, either one of the following applies for each potential fault:

— fault exclusion is in accordance with this document,

or

— fault always leads to a safe condition.

Where architectural requirements or other considerations impose a restriction on sole (single-channel) use, a maximum achievable PL and SIL must be specified for single channel use.

In order to provide the above information, devices must be assessed in accordance with safety standards (e.g. IEC 61508).

O.2 Software

O.2.1 General

In case of software is used within the component, the device manufacture should give information about the suitability of the software corresponding to the PL.

O.2.2 Basic safety principles

For components from category B up to category 4, the device manufacture should give information if the component is designed and manufactured according to basic safety principles.

O.2.3 Well-tried safety principles

For components from category 1 up to category 4, the device manufacture should give information if the component is designed and manufactured according to well-tried safety principles.

Annex ZA
(informative)

Relationship between this European Standard and the essential requirements of EU Directive 2006/42/EC aimed to be covered

This European Standard has been prepared under a Commission's standardization request M/396 Mandate to CEN and CENELEC for Standardisation in the field of machinery" to provide one voluntary means of conforming to essential requirements of Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast).

Once this standard is cited in the Official Journal of the European Union under that Directive, compliance with the normative clauses of this standard given in Table ZA.1 confers, within the limits of the scope of this standard, a presumption of conformity with the corresponding essential requirements of that Directive, and associated EFTA regulations.

Table ZA.1 — Correspondence between this European Standard and Directive 2006/42/EC

The relevant essential Requirements of Directive 2006/42/EC	Clause(s)/subclause(s) of this EN	Remarks/Notes
1.1.6	9	
1.2.1	6, 7, 10	
1.2.3	5.2.2.3	This subclause only deals with the restart function
1.2.4.1	5.2.2.1	This subclause only deals with those safety-related stop function achieving stop category 0 or 1.
1.2.4.2	5.2.2.1	This subclause only deals with those safety-related stop function achieving stop category 2.
1.2.4.3	5.2.1	This subclause only deals with the safety requirements specification of an emergency stop function
1.2.5	5.2.2.8	
1.2.6	5.2.1.3 item i), 5.2.2.7	
1.6.1	11	
1.6.2	11	
1.6.4	11	
1.7.4.2 (e, g, i, r, s)	13	This subclause only deals with the instruction for safety functions.

WARNING 1 — Presumption of conformity stays valid only as long as a reference to this European Standard is maintained in the list published in the Official Journal of the European Union. Users of this standard should consult frequently the latest list published in the Official Journal of the European Union.

WARNING 2 — Other Union legislation may be applicable to the product(s) falling within the scope of this standard.

Bibliography

Publications on programmable electronic systems

[1] IEC 61496-1:2014, *Safety of machinery — Electro-sensitive protective equipment — Part 1: General requirements and tests*

[2] IEC 61496-2:2014, *Safety of machinery — Electro-sensitive protective equipment — Part 2: Particular requirements for equipment using active opto-electronic protective devices*

[3] IEC 61496-3:2019, *Safety of machinery — Electro-sensitive protective equipment — Part 3: Particular requirements for active opto-electronic protective devices responsive to diffuse reflection (AOPDDR)*

[4] IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements*

[5] 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*

[7] IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations*

[8] IEC 61508-5:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 5: Examples of methods for the determination of safety integrity levels*

[9] 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*

[10] IEC 61508-7:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures*

Further publications

[11] ISO 11161:2007, *Safety of machinery — Integrated manufacturing systems — Basic requirements*

[12] ISO 13850:2015, *Safety of machinery — Emergency stop function — Principles for design*

[13] ISO 13851:2019, *Safety of machinery — Two-hand control devices — Principles for design and selection*

[14] ISO 13856-1:2013, *Safety of machinery — Pressure-sensitive protective devices — Part 1: General principles for design and testing of pressure-sensitive mats and pressure-sensitive floors*

[15] ISO 13856-2:2013, *Safety of machinery — Pressure-sensitive protective devices — Part 2: General principles for design and testing of pressure-sensitive edges and pressure-sensitive bars*

[16] ISO 11428:1996, *Ergonomics — Visual danger signals — General requirements, design and testing*

[17] ISO 9001:2013, *Quality management systems — Requirements*

[18] ISO 9355-1:1999, *Ergonomic requirements for the design of displays and control actuators — Part 1: Human interactions with displays and control actuators*

[19] ISO 9355-2:1999, *Ergonomic requirements for the design of displays and control actuators — Part 2: Displays*

[20] ISO 9355-3:2006, *Ergonomic requirements for the design of displays and control actuators — Part 3: Control actuators*

[21] ISO 11429:1996, *Ergonomics — System of auditory and visual danger and information signals*

[22] ISO 7731:2008, *Ergonomics — Danger signals for public and work areas — Auditory danger signals*

[23] ISO 4413:2010, *Hydraulic fluid power — General rules and safety requirements for systems and their components*

[24] ISO 4414:2010, *Pneumatic fluid power — General rules and safety requirements for systems and their components*

[25] ISO 14118:2017, *Safety of machinery — Prevention of unexpected start-up*

[26] ISO 14119:2013, *Safety of machinery — Interlocking devices associated with guards — Principles for design and selection*

[27] ISO 19973 (all parts), *Pneumatic fluid power — Assessment of component reliability by testing*

[28] ISO/TR 22100-2:2013, *Safety of machinery — Relationship with ISO 12100 — Part 2: How ISO 12100 relates to ISO 13849-1*

[29] ISO/TR 22100-4:2020, *Safety of machinery — Relationship with ISO 12100 — Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects*

[30] IEC 60204-1:2019, *Safety of machinery — Electrical equipment of machines — Part 1: General requirements*

[31] IEC 60447:2017, *Basic and safety principles for man-machine interface (MMI) — Actuating principles*

[32] IEC 60529:1989+AMD2:2013, *Degrees of protection provided by enclosures (IP code)*

[33] IEC 60812:2018, *Analysis techniques for system reliability — Procedure for failure mode and effects analysis (FMEA)*

[34] IEC 60947 (all parts), *Low-voltage switchgear and controlgear*

[35] IEC 61000-1-2:2016, *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*

[36] IEC 61000-6-2:2016, *Electromagnetic compatibility (EMC) — Part 6-2: Generic standards — Immunity for industrial environments*

[37] 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*

[38] IEC 61078:2016, *Reliability block diagrams*

[39] IEC 61326-3-1:2017, *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*

[40] IEC 61800-3:2017, *Adjustable speed electrical power drive systems — Part 3: EMC requirements and specific test methods*

[41] IEC 61800-5-2:2016, *Adjustable speed electrical power drive systems — Part 5-2: Safety requirements — Functional*

[42] IEC 61810 (all parts), *Electromagnetic elementary relays*

[43] IEC 61300 (all parts), *Fibre optic interconnecting devices and passive components — Basic test and measurement procedures*

[44] IEC 61310 (all parts), *Safety of machinery — Indication, marking and actuation*

[45] IEC 61131-3:2013, *Programmable controllers — Part 3: Programming languages*

[46] IEC 60050-192:2015, *International electrotechnical vocabulary — Chapter 191: Dependability and quality of service. Amended by IEC 60050-191-am1:1999 and IEC 60050-191-am2:2002:1999*

[47] EN 614-1:2006, *Safety of machinery — Ergonomic design principles — Part 1: Terminology and general principles*

[48] EN 1005-3:2002, *Safety of machinery — Human physical performance — Part 3: Recommended force limits for machinery operation*

[49] IEC 61810-3:2015, *Electromechanical elementary relays - Part 3: Relays with forcibly guided (mechanically linked) contacts*

[51] Goble W.M. *Control systems Safety Evaluation and Reliability*. 3rd Edition:2010 (ISBN-101934394807)

[52] 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, free download in the Internet: www.dguv.de/ifa/13849e

[53] IEC 61506:1997, *Documentation of software for process control systems and facilities*

[54] ISO/IEC/IEEE 26512:2018, *Systems and software engineering — Requirements for acquirers and suppliers of information for users*

[55] ISO/TR 14121-2:2012, *Safety of machinery — Risk assessment — Part 2: Practical guidance and examples of methods*

[56] ISO 10218-1:2011, *Robots and robotic devices — Safety requirements for industrial robots — Part 1: Robots*

[57] ISO 10218-2:2011, *Robots and robotic devices — Safety requirements for industrial robots — Part 2: Robot systems and integration*

[58] Chinniah Yuvin2015) , Analysis and prevention of serious and fatal accidents related to moving parts of machinery, Safety Science **75** (2015) 163–173

[59] 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

[60] ANSI B11.26 - 2018*Functional Safety for Equipment: General Principles for the Design of Safety Control Systems Using ISO 13849-1*

[61] EN 50495:2010, *Safety devices required for the safe functioning of equipment with respect to explosion risks; German version*

[62] VDMA 66413:2012 *Functional Safety - Universal data format for safety-related values of components or parts of control system*

[63] VDMA 24584:2020, *Safety functions of regulated and unregulated (fluid) mechanical systems*

[64] IFA. "*SISTEMA Cookbook 6: Definition of safety functions: what is important?*" (https://www.dguv.de/medien/ifa/en/pra/softwa/sistema/kochbuch/sistema_cookbook6_en.pdf)

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

[66] ISO 60947-4-1:2018, *Low-voltage switchgear and controlgear - Part 4-1: Contactors and motor-starters - Electromechanical contactors and motor-starters*

[67] ISO 60947-5-1:2020, *Low-voltage switchgear and controlgear - Part 5-1: Control circuit devices and switching elements - Electromechanical control circuit devices*

[66] ISO 60947-5-5:2017, *Low-voltage switchgear and controlgear - Part 5-5: Control circuit devices and switching elements - Electrical emergency stop device with mechanical latching function*

[66] ISO 60947-5-8:2008, *Low-voltage switchgear and controlgear -Part 5-8: Control circuit devices and switching elements - Three-position enabling switches*

[67] ISO 61810-2-1:2017, *Electromechanical elementary relays - Part 2-1: Reliability - Procedure for the verification of B_{10} values*

[68] ISO 8573-1:2010, *Compressed air — Part 1: Contaminants and purity classes*

[69] IEC/TR 63074:2021, *Safety of machinery - Security aspects related to functional safety of safety-related control systems*

[70] ISO 16090-1:2017, *Machine tools safety — Machining centres, Milling machines, Transfer machines — Part 1: Safety requirements*

[71] ISO 23125:2015, *Machine tools — Safety — Turning machines*

[72] ISO/TS 10566:2017, *Robots and robotic devices - Collaborative robots*

[73] IEC 61310-1:2007, *Safety of machinery - Indication, marking and actuation - Part 1: Requirements for visual, acoustic and tactile signals*

Databases

[74] IEC 61709:2017[2)], *Electric components — Reliability — Reference conditions for failure rates and stress models for conversion*

[75] *Reliability Prediction of Electronic Equipment, MIL-HDBK-217E*, Notice-2, Department of Defense, Washington, DC, 1995

[76] *Reliability Prediction Procedure for Electronic Equipment*, Telcordia SR-332, Issue 04, 2016 (https://www.ericsson.com/en)

[77] *British Handbook for Reliability Data for Components used in Telecommunication Systems*, British Telecom (HRD5, last issue)

[78] Chinese Military Standard GJB/Z 299C-2006 *Reliability prediction handbook for electronic equipment (English Version*)

[79] *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 (www.ifm.com/obj/EMC-Pocket-Guide-ZVEI-english.pdf)

2) Identical to RDF 2000/*Reliability Data Handbook*, UTE C 80-810, Union Technique de l'Electricité et de la Communication.