

DIN EN ISO 13849-2

ICS 13.110

Ersatz für
DIN EN ISO 13849-2:2008-09
und
DIN EN ISO 13849-2
Berichtigung 1:2009-01

**Sicherheit von Maschinen –
Sicherheitsbezogene Teile von Steuerungen –
Teil 2: Validierung (ISO 13849-2:2012);
Deutsche Fassung EN ISO 13849-2:2012**

Safety of machinery –
Safety-related parts of control systems –
Part 2: Validation (ISO 13849-2:2012);
German version EN ISO 13849-2:2012

Sécurité des machines –
Parties des systèmes de commande relatives à la sécurité –
Partie 2: Validation (ISO 13849-2:2012);
Version allemande EN ISO 13849-2:2012

Gesamtumfang 98 Seiten

Normenausschuss Sicherheitstechnische Grundsätze (NASG) im DIN
Normenausschuss Maschinenbau (NAM) im DIN

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist 2013-02-01.

Nationales Vorwort

Diese Norm enthält sicherheitstechnische Festlegungen im Sinne des Produktsicherheitsgesetzes (ProdSG).

Dieses Dokument enthält die Deutsche Fassung der vom Technischen Komitees ISO/TC 199 „Safety of machinery“ des Internationalen Komitees für Normung (ISO) in Zusammenarbeit mit dem Technischen Komitee CEN/TC 114 „Sicherheit von Maschinen und Geräten“ des Europäischen Komitees für Normung (CEN) entsprechend der Vereinbarung zwischen dem CEN und ISO über die technische Zusammenarbeit (Wiener Vereinbarung) ausgearbeiteten Norm EN ISO 13849-2:2012. Die Sekretariate beider Technischer Komitees werden vom DIN (Deutschland) gehalten.

Die nationalen Interessen bei der Erarbeitung der Norm wurden vom Gemeinschaftsausschuss „Steuerungen“ (NA 095-01-03 GA) des Normenausschusses Sicherheitstechnische Grundsätze (NASG) mit dem NAM und der DKE im DIN wahrgenommen.

Für die in Abschnitt 2 und in den Literaturhinweisen angegebenen Internationalen Normen wird im Folgenden auf die entsprechenden Deutschen Normen hingewiesen. Die Europäischen Normen wurden als Deutsche Normen unter identischer Normnummer veröffentlicht.

In Abschnitt 2 angegebene Normen

ISO 12100	siehe	DIN EN ISO 12100
ISO 13849-1	siehe	DIN EN ISO 13849-1

Im Verzeichnis „Literaturhinweise“ angegebene Normen

ISO 4413	siehe	DIN EN ISO 4413
ISO 4414	siehe	DIN EN ISO 4414
ISO 4960	siehe	DIN EN 10140 (modifizierte Übernahme)
ISO 11161	siehe	DIN EN ISO 11161
ISO 13850	siehe	DIN EN ISO 13850
ISO 13851	siehe	DIN EN 574
ISO 13855	siehe	DIN EN ISO 13855
ISO 13856-Reihe	siehe	DIN EN 1760-Reihe
ISO 14118	siehe	DIN EN 1037
ISO 14119	siehe	DIN EN 1088
IEC 60204-1	siehe	DIN EN 60204-1 (VDE 0113-1) (modifizierte Übernahme)
IEC 60269-1	siehe	DIN EN 60269-1 (VDE 0636-1)
IEC 60529	siehe	DIN EN 60529 (VDE 0470-1)
IEC 60664-Reihe	siehe	DIN EN 60664-Reihe (VDE 0110-Reihe)
IEC 60812	siehe	DIN EN 60812
IEC 60893-1	siehe	DIN EN 60893-1 (VDE 0318-1)
IEC 60947-Reihe	siehe	DIN EN 60947-Reihe (VDE 0660-Reihe)
IEC 61025	siehe	DIN EN 61025
IEC 61078	siehe	DIN EN 61078
IEC 61131-1	siehe	DIN EN 61131-1
IEC 61131-2	siehe	DIN EN 61131-2 (VDE 0411-500)
IEC 61165	siehe	DIN EN 61165
IEC 61249-Reihe	siehe	DIN EN 61249-Reihe
IEC 61508-Reihe	siehe	DIN EN 61508 (VDE 0803-Reihe)
IEC 61558-Reihe	siehe	DIN EN 61558-Reihe (VDE 0570-Reihe)
IEC 61800-5-2	siehe	DIN EN 61800-5-2 (VDE 0160-105-2)
IEC 61810-Reihe	siehe	DIN EN 61810-Reihe (VDE 0435-Reihe)

Änderungen

Gegenüber DIN EN ISO 13849-2:2008-09 und DIN EN ISO 13849-2 Berichtigung 1:2009-01 wurden folgende Änderungen vorgenommen:

- a) Anpassung der Anforderungen und Terminologie an die aktuelle Ausgabe ISO 13849-1:2006;
- b) Aktualisierung der Verweisungen;
- c) Analyse und Prüfung des Performance Levels (PL) nach ISO 13849-1:2006 ergänzt;
- d) teilweise neue Benummerung der Abschnitte durch Aufnahme eines Abschnittes 3 „Begriffe“ und Neuaufteilung und Verschiebung einzelner Abschnitte;
- e) Tabelle 2 „Anforderungen an die Dokumentation für Kategorien als Teil des Performance Levels“ aktualisiert;
- f) Abschnitt 9.2 „Validierung von Kategoriefestlegungen“ nach ISO 13849-1:2006 aktualisiert;
- g) neuer Abschnitt 9.3 „Validierung von $MTTF_d$, DC_{avg} und CCF“ aufgenommen;
- h) neuer Abschnitt 9.4 „Validierung von Maßnahmen zur Vermeidung systematischer Ausfälle hinsichtlich des Performance Levels und der Kategorie des SRP/CS“ ergänzt;
- i) neuer Abschnitt 9.5 „Validierung sicherheitsbezogener Software“ aufgenommen;
- j) neuer Abschnitt 9.6 „Validierung und Nachweis des Performance Levels“ hinzugefügt;
- k) neuer Abschnitt 12 „Validierung der technischen Dokumentation und Benutzerinformation“ aufgenommen;
- l) neuer Anhang E „Beispiel der Validierung von Fehlverhalten und Mitteln zur Diagnose“ ergänzt.

Frühere Ausgaben

DIN EN ISO 13849-2: 2003-12, 2008-09

DIN EN ISO 13849-2 Berichtigung 1: 2009-01

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN 574, *Sicherheit von Maschinen — Zweihandschaltungen — Funktionelle Aspekte — Gestaltungsleitsätze*

DIN EN 1037, *Sicherheit von Maschinen — Vermeidung von unerwartetem Anlauf*

DIN EN 1088, *Sicherheit von Maschinen — Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen — Leitsätze für Gestaltung und Auswahl*

DIN EN 1760 (alle Teile), *Sicherheit von Maschinen — Druckempfindliche Schutzeinrichtungen*

DIN EN 10140, *Kaltband — Grenzabmaße und Formtoleranzen*

DIN EN 60204-1 (VDE 0113-1), *Sicherheit von Maschinen — Elektrische Ausrüstung von Maschinen — Teil 1: Allgemeine Anforderungen*

DIN EN 60269-1 (VDE 0636-1), *Niederspannungssicherungen — Teil 1: Allgemeine Anforderungen*

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

DIN EN 60664 (alle Teile) (VDE 0110-Reihe), *Isolationskoordination für elektrische Betriebsmittel in Niederspannungsanlagen*

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

DIN EN 60893-1 (VDE 0318-1), *Isolierstoffe — Tafeln aus technischen Schichtpressstoffen auf der Basis warmhärtender Harze für elektrotechnische Zwecke — Teil 1: Definitionen, Bezeichnungen und allgemeine Anforderungen*

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

DIN EN 61025, *Fehlzustandsbaumanalyse*

DIN EN 61078, *Techniken für die Analyse der Zuverlässigkeit — Zuverlässigkeitsblockdiagramm und Boole'sche Verfahren*

DIN EN 61131-1, *Speicherprogrammierbare Steuerungen — Teil 1: Allgemeine Informationen*

DIN EN 61131-2 (VDE 0411-500), *Speicherprogrammierbare Steuerungen — Teil 2: Betriebsmittelanforderungen und Prüfungen*

DIN EN 61165, *Anwendung des Markoff-Verfahrens*

DIN EN 61249 (alle Teile), *Materialien für Leiterplatten und andere Verbindungsstrukturen*

DIN EN 61508 (alle Teile) (VDE 0803-Reihe), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme*

DIN EN 61558 (alle Teile) (VDE 0570-Reihe), *Sicherheit von Transformatoren, Netzgeräten, Drosseln und dergleichen*

DIN EN 61800-5-2 (VDE 0160-105-2), *Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl — Teil 5-2: Anforderungen an die Sicherheit — Funktionale Sicherheit*

DIN EN 61810 (alle Teile), *Elektromechanische Elementarrelais*

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

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

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

DIN EN ISO 12100, *Sicherheit von Maschinen — Allgemeine Gestaltungsleitsätze — Risikobeurteilung und Risikominderung*

DIN EN ISO 13849-1, *Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen — Teil 1: Allgemeine Gestaltungsleitsätze*

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

DIN EN ISO 13855, *Sicherheit von Maschinen — Anordnung von Schutzeinrichtungen im Hinblick auf Annäherungsgeschwindigkeiten von Körperteilen*

— Leerseite —

Deutsche Fassung

Sicherheit von Maschinen —
Sicherheitsbezogene Teile von Steuerungen —
Teil 2: Validierung
(ISO 13849-2:2012)

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

Sécurité des machines —
Parties des systèmes de
commande relatives à la sécurité —
Partie 2: Validation
(ISO 13849-2:2012)

Diese Europäische Norm wurde vom CEN am 14. Oktober 2012 angenommen.

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

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

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



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

Management-Zentrum: Avenue Marnix 17, B-1000 Brüssel

Inhalt

Seite

Vorwort	4
Einleitung.....	5
1 Anwendungsbereich	6
2 Normative Verweisungen.....	6
3 Begriffe	6
4 Validierungsverfahren	6
4.1 Validierungsleitsätze	6
4.2 Validierungsplan	9
4.3 Allgemeine Fehlerlisten	9
4.4 Spezielle Fehlerlisten	9
4.5 Angaben zur Validierung	10
4.6 Validierungsaufzeichnung	12
5 Validierung durch Analyse	12
5.1 Allgemeines	12
5.2 Analysetechniken	12
6 Validierung durch Prüfen	13
6.1 Allgemeines	13
6.2 Messgenauigkeit	14
6.3 Höhere Anforderungen	14
6.4 Anzahl der Prüflinge	14
7 Validierung der Spezifikation von Sicherheitsanforderungen an die Sicherheitsfunktionen	15
8 Validierung der Sicherheitsfunktionen.....	15
9 Validierung der Performance Levels und Kategorien.....	16
9.1 Analyse und Prüfung.....	16
9.2 Validierung der Festlegungen von Kategorien.....	17
9.2.1 Kategorie B	17
9.2.2 Kategorie 1	17
9.2.3 Kategorie 2	17
9.2.4 Kategorie 3	18
9.2.5 Kategorie 4	18
9.3 Validierung von $MTTF_d$, DC_{avg} und CCF	19
9.4 Validierung von Maßnahmen zur Vermeidung systematischer Ausfälle hinsichtlich des Performance Levels und der Kategorie des SRP/CS	20
9.5 Validierung der sicherheitsbezogenen Software	20
9.6 Validierung und Verifizierung des Performance Levels	21
9.7 Validierung der Kombination sicherheitsbezogener Teile	22
10 Validierung der Umgebungsanforderungen	22
11 Validierung der Instandhaltungsanforderungen	23
12 Validierung der technischen Dokumentation und Benutzerinformation	23

Anhang A (informativ) Validierungswerkzeuge für mechanische Systeme.....	24
Anhang B (informativ) Validierungswerkzeuge für pneumatische Systeme	30
Anhang C (informativ) Validierungswerkzeuge für hydraulische Systeme	41
Anhang D (informativ) Validierungswerkzeuge für elektrische Systeme.....	50
D.1 Allgemeines	50
D.2 Fehlerausschluss	55
D.2.1 Allgemeines	55
D.2.2 „Zinn-Whiskers“	55
D.2.3 Kurzschlüsse an PCB-montierten Teilen	55
D.2.4 Fehlerausschlüsse und integrierte Schaltkreise	55
Anhang E (informativ) Beispiel für die Validierung von Fehlverhalten und Mitteln zur Diagnose	64
E.1 Allgemeines	64
E.2 Beschreibung der Maschine	64
E.3 Festlegung der Anforderungen an Sicherheitsfunktionen	66
E.4 Gestaltung der SRP/CS.....	68
E.4.1 Allgemeines	68
E.4.2 Sicherheitsfunktion SF 1  Sicherheitsbezogenes Abschalten durch Öffnen der verriegelten trennenden Schutzeinrichtung und Vermeidung von unerwartetem Anlauf, wenn die verriegelte trennende Schutzeinrichtung geöffnet ist	72
E.4.3 Sicherheitsfunktion SF 2  Sicher begrenzte Geschwindigkeit (SLS – en: safely-limited speed)	75
E.4.4 Sicherheitsfunktion SF 3  Selbsttätiger Rückstellungsbetrieb	77
E.5 Validierung	79
E.5.1 Allgemeines	79
E.5.2 Validierung von Fehlverhalten und DC_{avg}	79
E.5.3 FMEA und DC_{avg} für SF 1.0 und SF 1.3.....	80
Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EU-Richtlinie 2006/42/EG	90
Literaturhinweise	91

Vorwort

Dieses Dokument (EN ISO 13849-2:2012) 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 vom DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis April 2013, und etwaige entgegenstehende nationale Normen müssen bis April 2013 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Texte dieses Dokuments Patentrechte berühren können. CEN [und/oder CENELEC] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Dieses Dokument ersetzt EN ISO 13849-2:2008.

Dieses Dokument wurde unter einem Mandat erarbeitet, das die Europäische Kommission und die Europäische Freihandelszone dem CEN erteilt haben, und unterstützt grundlegende Anforderungen der EU-Richtlinien.

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

EN ISO 13849 besteht unter dem allgemeinen Titel *Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen* aus den folgenden Teilen:

- Teil 1: *Allgemeine Gestaltungsleitsätze*;
- Teil 2: *Validierung*.

Die Anhänge A bis D sind informativ und nach Tabelle 1 gegliedert.

Tabelle 1 — Gliederung der Anhänge A bis D dieses Teils der ISO 13849

Anhang	Technik	Liste grundlegender Sicherheitsprinzipien	Liste bewährter Sicherheitsprinzipien	Liste bewährter Bauteile	Fehlerlisten und Fehlerausschlüsse
		Tabelle(n)			
A	Mechanisch	A.1	A.2	A.3	A.4, A.5
B	Pneumatisch	B.1	B.2	—	B.3 bis B.18
C	Hydraulisch	C.1	C.2	—	C.3 bis C.12
D	Elektrisch (enthält Elektronik)	D.1	D.2	D.3	D.4 bis D.21

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

Anerkennungsnotiz

Der Text von ISO 13849-2:2012 wurde vom CEN als EN ISO 13849-2:2012 ohne irgendeine Abänderung genehmigt.

Einleitung

Sicherheitsnormen auf dem Gebiet Maschinen und Geräte sind wie folgt gegliedert:

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

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

Die Anforderungen dieses Dokuments können durch eine Typ-C-Norm ergänzt oder geändert werden.

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

Dieser Teil der ISO 13849 legt das Validierungsverfahren für die Sicherheitsfunktionen, Kategorien und Performance Level von sicherheitsbezogenen Teilen von Steuerungen fest. Sie erkennt an, dass die Validierung von sicherheitsbezogenen Teilen von Steuerungen durch eine Kombination aus Analyse (siehe Abschnitt 5) und Prüfung (siehe Abschnitt 6) erreicht werden kann und legt die bestimmten Umstände fest, unter denen eine Prüfung durchgeführt werden sollte.

Die meisten Verfahren und Bedingungen in diesem Teil der ISO 13849 beruhen auf der Annahme, dass das in ISO 13849-1:2006, 4.5.4, beschriebene vereinfachte Verfahren zur Abschätzung des Performance Level (PL) angewendet wird. Dieser Teil der ISO 13849 gibt keine Anleitung für den besonderen Fall, dass andere Verfahren zur Abschätzung des PL angewendet werden (z. B. das Markov-Modell). Wird ein anderes Verfahren angewendet, können einige Teile dieser Norm möglicherweise nicht angewendet werden und es können zusätzliche Anforderungen notwendig sein.

Eine Anleitung zu den allgemeinen Gestaltungsleitsätzen (siehe ISO 12100) von sicherheitsbezogenen Teilen von Steuerungen wird unabhängig von der Art der angewandten Technik (elektrisch, hydraulisch, pneumatisch, mechanisch usw.) in ISO 13849-1 gegeben. Das umfasst Beschreibungen einiger typischer Sicherheitsfunktionen, die Ermittlung ihres Performance Levels sowie allgemeine Anforderungen an Kategorie und Performance Level.

Innerhalb dieses Teils der ISO 13849 sind einige Anforderungen an die Validierung allgemeiner Art, während andere sich speziell auf die Art der angewandten Technik beziehen.

1 Anwendungsbereich

Dieser Teil von ISO 13849 legt die Vorgehensweisen und Bedingungen fest, die bei der Validierung durch Analyse und Prüfung zu befolgen sind, für

- die festgelegten Sicherheitsfunktionen;
- die erreichten Kategorien, sowie
- den erreichten Performance Level

der sicherheitsbezogenen Teile der Steuerung (SRP/CS), die in Übereinstimmung mit ISO 13849-1 entwickelt wurden.

ANMERKUNG Zusätzliche Anforderungen an programmierbare elektronische Systeme einschließlich Embedded-Software sind in ISO 13849-1:2006, 4.6, und in IEC 61508 enthalten.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. 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 13849-1:2006, *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO 12100 und ISO 13849-1.

4 Validierungsverfahren

4.1 Validierungsleitsätze

Der Zweck des Validierungsverfahrens ist es, zu bestätigen, dass die Gestaltung der sicherheitsbezogenen Teile der Steuerung (SRP/CS) die Spezifikation der Sicherheitsanforderungen der Maschinen unterstützt.

Die Validierung muss aufzeigen, dass jedes SRP/CS die Anforderungen von ISO 13849-1 erfüllt, insbesondere bei

- a) den festgelegten Sicherheitseigenschaften der Sicherheitsfunktionen, wie diese bei der sinnvollen Gestaltung vorgesehen wurde;
- b) den Anforderungen für den festgelegte Performance Level (siehe ISO 13849-1:2006, 4.5):
 - 1) den Anforderungen für die festgelegte Kategorie (siehe ISO 13849-1:2006, 6.2),
 - 2) den Maßnahmen zur Beherrschung und zur Vermeidung systematischer Ausfälle (siehe ISO 13849-1:2006, Anhang G),
 - 3) den Anforderungen an die Software, falls vorhanden (siehe ISO 13849-1:2006, 4.6), und
 - 4) der Fähigkeit, eine Sicherheitsfunktion unter den erwarteten Umgebungsbedingungen zu leisten;
- c) der ergonomischen Gestaltung der Benutzerschnittstelle, z. B. damit der Benutzer nicht verleitet wird, in einer gefährlichen Weise zu handeln, indem er z. B. die SRP/CS umgeht (siehe ISO 13849-1:2006, 4.8).

Die Validierung sollte von Personen durchgeführt werden, die unabhängig von der Gestaltung der SRP/CS sind.

ANMERKUNG „Unabhängige Person“ bedeutet nicht unbedingt, dass eine Prüfung durch Dritte erforderlich ist.

Die Validierung besteht aus der Durchführung der Analyse (siehe Abschnitt 5) und aus der Durchführung von Funktionsprüfungen (siehe Abschnitt 6) unter vorhersehbaren Bedingungen in Übereinstimmung mit dem Validierungsplan. Bild 1 gibt einen Überblick über das Validierungsverfahren. Die Abwägung zwischen Analyse und Prüfung hängt von der für die sicherheitsbezogenen Teile angewandten Technik und dem erforderlichen Performance Level ab. Für die Kategorien 2, 3, und 4 muss die Validierung der Sicherheitsfunktion auch Prüfungen unter Fehlerbedingungen beinhalten.

Mit der Analyse sollte so früh wie möglich und gleichzeitig mit dem Gestaltungsprozess begonnen werden, so dass Probleme frühzeitig korrigiert werden können. In folgenden Schritten sind sie noch relativ leicht korrigierbar, „Gestaltung und technische Realisierung der Sicherheitsfunktionen“ und „Ermittlung des Performance Levels PL“ (Kasten 4 und 5 in ISO 13849-1:2006, Bild 3). Für einige Teile der Analyse kann es notwendig sein, sie erst dann auszuführen, wenn die Entwicklung weit fortgeschritten ist.

Falls es aufgrund der Größe des Systems, seiner Komplexität oder der Verknüpfung der Steuerung (mit der Maschine) erforderlich ist, sollten spezielle Zusammenstellungen für:

- die Validierung der SRP/CS getrennt vor dem Einbau einschließlich der Simulation der geeigneten Eingangs- und Ausgangssignale; und
- die Validierung der Auswirkungen bei Integration sicherheitsbezogener Teile in den Rest der Steuerung in Übereinstimmung mit ihrer Anwendung in der Maschine.

gemacht werden.

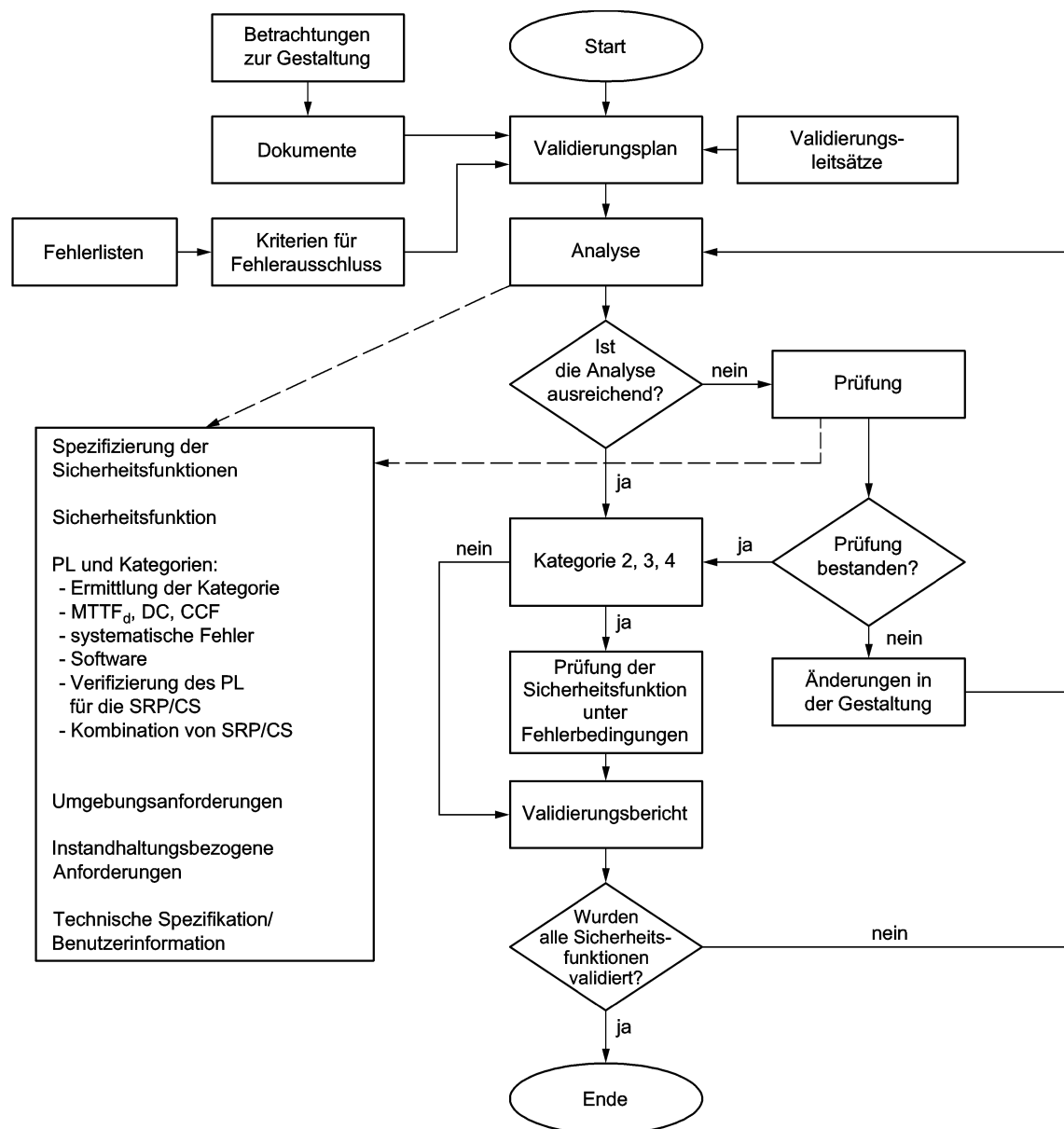


Bild 1 — Übersicht über das Validierungsverfahren

„Änderungen in der Gestaltung“ in Bild 1 bezieht sich auf das Gestaltungsverfahren. Wenn die Validierung nicht erfolgreich abgeschlossen werden kann, sind Änderungen in der Gestaltung erforderlich. Danach sollte die Validierung der geänderten sicherheitsbezogenen Teile wiederholt werden. Dieses Verfahren sollte solange wiederholt werden, bis sämtliche sicherheitsbezogenen Teile der Sicherheitsfunktionen erfolgreich validiert sind.

4.2 Validierungsplan

Der Validierungsplan muss die Anforderungen an die Durchführung des Validierungsverfahrens für die festgelegten Sicherheitsfunktionen, ihre Kategorien und Performance Level bestimmen und beschreiben.

Der Validierungsplan muss auch die Mittel bestimmen, die zu verwenden sind, um die festgelegten Sicherheitsfunktionen, Kategorien und Performance Levels zu validieren. Sofern angemessen, muss er Folgendes darlegen:

- a) die Identität der Dokumente für die Spezifikationen,
- b) die Betriebs- und Umgebungsbedingungen während der Prüfung,
- c) die anzuwendenden Analysen und Prüfungen,
- d) den Verweis auf anzuwendende Prüfnormen, und
- e) die für jeden Schritt im Validierungsprozess verantwortlichen Personen oder Parteien.

Sicherheitsbezogene Teile, die bereits zuvor nach der gleichen Spezifikation validiert wurden, benötigen nur einen Verweis auf die frühere Validierung.

4.3 Allgemeine Fehlerlisten

Das Validierungsverfahren schließt die Berücksichtigung des Verhaltens von SRP/CS für alle anzunehmenden Fehler ein. Eine Grundlage für die Fehlerbetrachtung ist in den Fehlerlistentabellen der Anhänge A bis D zu finden, die auf Erfahrungen basieren und Folgendes enthalten:

- die einzubeziehenden Bauteile/Elemente, z. B. Leiter/ Kabel (siehe Annex D),
- 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 dauerhafte Fehler berücksichtigt.

4.4 Spezielle Fehlerlisten

Falls notwendig muss eine spezielle auf das Produkt bezogene Fehlerliste als Bezugsdokument für das Validierungsverfahren für das/die sicherheitsbezogene(n) Teil(e) erstellt werden. Diese Liste kann auf der/den entsprechenden allgemeinen Liste(n) in den Anhängen beruhen.

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

- a) die aus der/n allgemeinen Liste(n) einzubeziehenden Fehler,
- b) alle anderen maßgeblichen aufzunehmenden Fehler, die nicht in der allgemeinen Liste aufgeführt sind (z. B. Ausfall infolge gemeinsamer Ursache),
- c) die aus der/n allgemeinen Liste(n) entnommenen Fehler, die auf der Grundlage ausgeschlossen werden dürfen, dass die in den allgemeinen Listen enthaltenen (siehe ISO 13849-1:2006, 7.3) Kriterien erfüllt werden, und

ausnahmsweise

- d) alle weiteren Fehler, für die die allgemeine(n) Liste(n) einen Ausschluss nicht zulässt/zulassen, für die jedoch eine Begründung und sinnvollen Erklärung für ihren Ausschluss gegeben wird (siehe ISO 13849-1:2006, 7.3).

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

4.5 Angaben zur Validierung

Die für die Validierung notwendigen Angaben unterscheiden sich hinsichtlich der angewendeten Technologie, der Kategorie(n) und des/der Performance Level(s), um eine sinnvolle Gestaltung des Systems und den Beitrag der SRP/CS für die Risikoverringerung nachzuweisen. Dokumente, die in ausreichendem Maße die Angaben aus der nachfolgenden Liste enthalten, müssen im Validierungsverfahren aufgenommen sein, um nachzuweisen, dass die sicherheitsbezogenen Teile die festgelegten Sicherheitsfunktionen entsprechend des/der erforderlichen Performance Level(s) und/oder Kategorie(n) erfüllen:

- a) Festlegung der erforderlichen Eigenschaften jeder Sicherheitsfunktion und ihrer/ihrer erforderlichen Kategorie und Performance Levels;
- b) Zeichnungen und Festlegungen, z. B. für mechanische, hydraulische und pneumatische Teile, gedruckte Schaltungen, Montagepläne, interne Verdrahtung, Gehäuse, Werkstoffe, Aufstellung;
- c) Blockdiagramm(e) mit einer Funktionsbeschreibung der Blöcke;
- d) Schaltpläne einschließlich ihrer Verknüpfungen/Verbindungen;
- e) Funktionsbeschreibung der Schaltpläne;
- 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 mit Stückbezeichnung, Nennwerten, Grenzabmaßen, maßgeblichen Betriebsbeanspruchungen, Typ-Bezeichnungen, Daten über Fehlerraten und Bauteilhersteller und alle weiteren Daten, die für die Sicherheit maßgebend sind;
- i) Analyse aller maßgeblichen Fehler (siehe auch 4.3 und 4.4), die z. B. in den Tabellen der Anhänge A bis D aufgelistet sind, einschließlich der Begründung aller ausgeschlossenen Fehler;
- j) Analyse des Einflusses der im Verfahren verwendeten Werkstoffe;
- k) Benutzerinformation, 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, und die die sicherheitstechnische Leistungsfähigkeit, die die Software erreichen muss, angibt,
- den Nachweis, dass die Software so gestaltet ist, dass sie den erforderlichen Performance Level erreicht (siehe 9.5), und
- Einzelheiten über Prüfungen (insbesondere Prüfberichte), die durchgeführt wurden, um nachzuweisen, dass die geforderte sicherheitstechnische Leistungsfähigkeit erreicht wurde.

ANMERKUNG Bezüglich Anforderungen siehe ISO 13849-1:2006, 4.6.2 und 4.6.3.

Es sind Angaben darüber erforderlich, wie der Performance Level und die durchschnittliche Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde bestimmt werden. Die Dokumentation der quantitativ bestimmbar Aspekte muss Folgendes enthalten:

- das sicherheitsbezogene Blockdiagramm (siehe ISO 13849-1:2006, Anhang B) oder die vorgesehene Architektur (siehe ISO 13849-1:2006, 6.2),

- die Bestimmung von $MTTF_d$ (mittlere Zeit bis zum gefahrbringenden Ausfall), DC_{avg} (durchschnittlicher Diagnosedeckungsgrad) und CCF (Ausfall infolge gemeinsamer Ursache), und
- die Bestimmung der Kategorie (siehe Tabelle 2).

In der Dokumentation sind Angaben erforderlich, wie systematische Aspekte der SRP/CS berücksichtigt wurden.

Es sind Angaben darüber erforderlich, inwiefern die Kombination mehrerer SRP/CS einen Performance Level erreicht, der dem geforderten Performance Level entspricht.

Tabelle 2 — Anforderungen an die Dokumentation für Kategorien unter Berücksichtigung des Performance Levels

Anforderungen an die Dokumentation	Kategorie, für die eine Dokumentation erforderlich ist				
	B	1	2	3	4
grundlegende Sicherheitsprinzipien	X	X	X	X	X
zu erwartende Betriebsbeanspruchungen	X	X	X	X	X
Einfluss der verwendeten Werkstoffe	X	X	X	X	X
Leistungsfähigkeit bei anderen maßgeblichen äußeren Einflüssen	X	X	X	X	X
bewährte Bauteile	—	X	—	—	—
bewährte Sicherheitsprinzipien	—	X	X	X	X
mittlere Zeit bis zum gefahrbringenden Ausfall ($MTTF_d$) jeden Kanals	X	X	X	X	X
das Testverfahren für die Sicherheitsfunktion(en)	—	—	X	—	—
durchgeführte Diagnosemaßnahmen einschließlich Fehlerreaktion	—	—	X	X	X
Testintervalle, wenn festgelegt	—	—	X	X	X
Diagnosedeckungsgrad (DC_{avg})	—	—	X	X	X
bei der Gestaltung berücksichtigte vorhersehbare Einzelfehler und die angewendete Diagnosemaßnahme	—	—	X	X	X
die erkannten Ausfälle infolge gemeinsamer Ursache (CCF) und wie sie verhindert werden	—	—	X	X	X
die vorhersehbaren ausgeschlossenen Einzelfehler	—	—	—	X	X
Fehler, die zu erkennen sind	—	—	X	X	X
wie die Sicherheitsfunktion in jedem Fehlerfall aufrechterhalten bleibt	—	—	—	X	X
wie die Sicherheitsfunktion bei allen Fehlerkombinationen aufrechterhalten bleibt	—	—	—	—	X
Maßnahmen gegen systematische Fehler	X	X	X	X	X
Maßnahmen gegen Softwarefehler	X	—	X	X	X
X Dokumentation erforderlich — Dokumentation nicht erforderlich					
ANMERKUNG Die Kategorien entsprechen denen, die in ISO 13849-1:2006 angegeben sind.					

4.6 Validierungsaufzeichnung

Die Validierung durch Analyse und Prüfung muss aufgezeichnet werden. Die Aufzeichnung muss das Validierungsverfahren für alle sicherheitstechnischen Anforderungen ersichtlich machen. Es dürfen Querverweise zu vorhergehenden Validierungsaufzeichnungen gemacht werden, vorausgesetzt, sie sind ordnungsgemäß gekennzeichnet.

Für jedes sicherheitsbezogene Teil, das ein Bestandteil des Validierungsverfahrens nicht bestanden hat, muss die Aufzeichnung beschreiben, welche Bestandteile der Validierungsanalyse/-prüfung nicht bestanden wurden. Es muss sichergestellt sein, dass sämtliche sicherheitsbezogenen Teile nach einer Veränderung erfolgreich neu validiert werden.

5 Validierung durch Analyse

5.1 Allgemeines

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

- die bei der Risikoanalyse erkannten Sicherheitsfunktion(en), ihre Eigenschaften und der/die erforderliche(n) Performance Level(s) (siehe ISO 13849-1:2006, Bilder 1 und 3);
- die quantifizierbaren Aspekte ($MTTF_d$, DC_{avg} und CCF);
- die Systemstruktur (z. B. vorgesehene Architektur) (siehe ISO 13849-1:2006, Abschnitt 6);
- die nicht quantifizierbaren qualitativen Aspekte, die das Systemverhalten beeinträchtigen (gegebenenfalls Software-Aspekte);
- deterministische Argumente.

Bei der Validierung der Sicherheitsfunktionen durch Analyse ist weit mehr als bei der Prüfung die Festlegung von deterministischen Argumenten erforderlich.

ANMERKUNG 1 Ein deterministisches Argument ist ein Argument, das auf qualitativen Gesichtspunkten (z. B. Qualität bei der Herstellung, Erfahrungen bei der Anwendung) basiert. Diese Betrachtung ist abhängig von der Anwendung, welche zusammen mit andere Faktoren können die deterministischen Argumente beeinträchtigen.

ANMERKUNG 2 Deterministische Argumente unterscheiden sich von anderen Beweisführungen dadurch, dass sie zeigen, dass die geforderten Eigenschaften des Systems einem Systemmodell logisch folgen. Derartige Argumente können auf der Grundlage einfacher, gut verständlicher Begriffe entwickelt werden.

5.2 Analysetechniken

Die Auswahl einer Analysetechnik hängt von dem jeweiligen Analysegegenstand ab. Es gibt zwei grundsätzliche Techniken:

- a) „Top-down“-(deduktive) 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 „Top-down“-Analysetechniken sind die Fehlerbaumanalyse (FTA – siehe IEC 61025) und die Ereignisbaumanalyse (ETA);

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

BEISPIEL „Bottom-up“-Techniken sind die Fehlerzustandsart- und -auswirkungsanalyse (FMEA — siehe IEC 60812) sowie die Fehlzustandsart-, -auswirkungs- und -kritizitätsanalyse (FMECA).

6 Validierung durch Prüfen

6.1 Allgemeines

Wenn die Validierung durch Analyse nicht schlüssig ist, müssen Prüfungen durchgeführt werden, um die Validierung zu vervollständigen. Eine Prüfung als Ergänzung zur Analyse ist oft notwendig.

Die Validierungsprüfungen müssen geplant und in logischer Weise ausgeführt werden. Insbesondere:

- a) vor Beginn der Prüfungen muss ein Prüfplan ausgearbeitet werden, der Folgendes beinhalten muss:
 - 1) die Prüfspezifikationen,
 - 2) die für die Übereinstimmung erforderlichen Ergebnisse der Prüfungen,
 - 3) die zeitliche Abfolge der Prüfungen,
- b) Prüfaufzeichnungen müssen erstellt werden, die folgende Angaben enthalten:
 - 1) den Namen der Person, die die Prüfung durchführt,
 - 2) die Umgebungsbedingungen (siehe Abschnitt 10),
 - 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 sicher zu stellen, dass die festgelegten Funktions- und Leistungsziele erreicht sind.

Die Prüfung am Prüfling muss so nah wie möglich in der vorgesehenen endgültigen Betriebskonfiguration, d. h. mit allen peripheren Geräten und angebrachten Abdeckungen, durchgeführt werden.

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

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

Es wird empfohlen, die Kombination dieser Eingangssignale systematisch in die Steuerung und Maschine einzugeben. Ein Beispiel für diese Logik ist: Energie einschalten, in Betrieb setzen, Arbeitsablauf, Richtungsänderungen, Wiederanlaufen. Falls notwendig, muss ein erweiterter Umfang von Eingangsdaten eingegeben werden, um anormale oder ungewöhnliche Situationen zu berücksichtigen, und um zu sehen, wie die SRP/CS reagieren. Derartige Kombinationen von Eingangsdaten müssen vorhersehbare fehlerhafte Bedienungen berücksichtigen.

Das Ziel der Prüfung ist die Festlegung der Umgebungsbedingungen für die Prüfung, welche die eine oder andere der folgenden sein können:

- die Umgebungsbedingungen bei der beabsichtigten Verwendung;
- die Bedingungen bei besonderen Nennwerten;
- ein bestimmter Bereich von Bedingungen, wenn Driften zu erwarten ist.

Die Bandbreite von Bedingungen, die als stabil angesehen werden kann und über die die Prüfungen gültig sind, sollte zwischen dem Konstrukteur und dem verantwortlichen Prüfpersonal vereinbart und aufgezeichnet werden.

6.2 Messgenauigkeit

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

- a) Zeitmessungen;
- b) Druckmessungen;
- c) Kraftmessungen;
- d) elektrische Messungen;
- e) Messungen der relativen Feuchte;
- f) Längenmessungen.

Abweichungen von diesen Messgenauigkeiten sind zu begründen.

6.3 Höhere Anforderungen

Wenn die in den Begleitdokumenten gestellten Anforderungen an die SRP/CS über die Anforderungen dieses Teils der ISO 13849 hinausgehen, müssen die höheren Anforderungen zu Grunde gelegt werden.

ANMERKUNG Höhere Anforderungen können zu Grunde gelegt werden, wenn die Steuerung besonders ungünstigen Betriebsbedingungen standhalten muss, z. B. grobe Handhabung, Einwirkungen von Feuchte, Hydrolyse, Schwankungen der Umgebungstemperatur, Auswirkungen von chemischen Mitteln, Korrosion, hohe Intensität elektromagnetischer Felder — z. B. aufgrund der Nähe zu Sendern.

6.4 Anzahl der Prüflinge

Soweit nicht anders festgelegt, müssen die Prüfungen an einem einzelnen Produktionsmuster des zu prüfenden sicherheitsbezogenen Teils durchgeführt werden.

(Ein) sicherheitsbezogene(s) Teil(e), das/die sich in der Prüfung befindet/n, darf/dürfen während des Prüf- ablaufes nicht verändert werden.

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

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

7 Validierung der Spezifikation von Sicherheitsanforderungen an die Sicherheitsfunktionen

Vor der Validierung der Gestaltung der SRP/CS oder der Kombination von SRP/CS, die die Sicherheitsfunktion enthält, muss die Spezifikation der Anforderungen für die Sicherheitsfunktion verifiziert werden, um die Übereinstimmung und Vollständigkeit für ihren vorgesehenen Verwendungszweck sicherzustellen.

Die Spezifikation der Sicherheitsanforderungen sollte analysiert werden, bevor mit der Gestaltung begonnen wird, da jede andere Tätigkeit auf diesen Anforderungen beruht.

Es muss sichergestellt sein, dass die Anforderungen für alle Sicherheitsfunktionen der Maschinensteuerung dokumentiert wurden.

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

Die Validierung darf anhand von Prüfungen und Inspektionen der Sicherheitsanforderungen und Gestaltungsspezifikation(en) der SRP/CS durchgeführt werden; insbesondere, um nachzuweisen, dass sämtliche Aspekte von

- den vorgesehenen Anwendungsanforderungen und Sicherheitserfordernissen, und
- den Betriebs- und Umgebungsbedingungen sowie möglichem menschlichen Versagen (z. B. Missbrauch) berücksichtigt wurden.

Wenn eine Produktnorm die Sicherheitsanforderungen für die Gestaltung eines SRP/CS festlegt (z. B. ISO 11161 für integrierte Fertigungssysteme oder ISO 13851 für Zweihandschaltungen), müssen diese berücksichtigt werden.

8 Validierung der Sicherheitsfunktionen

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

ANMERKUNG 1 Ein Verlust der Sicherheitsfunktion, wenn kein Hardwarefehler vorliegt, beruht auf einem systematischen Fehler, der durch Fehler während der Gestaltung und der Integration verursacht worden sein kann (durch eine Fehlinterpretation der Eigenschaften der Sicherheitsfunktion, einen Fehler in der logischen Gestaltung, einen Fehler innerhalb des Hardwareaufbaus, einen Fehler beim Tippen des Softwarecodes usw.). Einige dieser systematischen Fehler werden während des Gestaltungsprozesses entdeckt, während andere während des Validierungsvorgangs erkannt werden oder unbemerkt bleiben. Zusätzlich ist es ebenfalls möglich, einen Fehler während des Validierungsprozesses zu begehen (z. B. Nicht-Überprüfung einer Eigenschaft).

Die Validierung der festgelegten Eigenschaften der Sicherheitsfunktionen muss durch Anwendung geeigneter Maßnahmen der folgenden Liste durchgeführt werden.

- funktionale Analyse der Schaltpläne, Überprüfungen der Software (siehe 9.5).

ANMERKUNG 2 Wenn eine Maschine komplexe oder eine große Anzahl von Sicherheitsfunktionen aufweist, kann eine Analyse die Anzahl der erforderlichen Funktionsprüfungen verringern.

- Simulation.
- 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.

- Funktionsprüfung der Sicherheitsfunktionen in allen Betriebsarten der Maschine, um festzustellen, ob sie mit den festgelegten Eigenschaften übereinstimmen (siehe ISO 13849-1:2006, Abschnitt 5 bezüglich Spezifikationen einiger typischer Sicherheitsfunktionen). 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.
- erweiterte Funktionsprüfung, um vorhersehbare anormale Signale oder Kombinationen von Signalen aus irgendeiner Eingangsquelle zu überprüfen, einschließlich Energieunterbrechung, -wiederkehr und fehlerhafte Betätigungen.
- Überprüfung der Bedieneroberfläche der SRP/CS auf Erfüllung ergonomischer Prinzipien (siehe ISO 13849-1:2006, 4.8).

ANMERKUNG 3 Weitere Maßnahmen gegen systematische Fehler, die in 9.4 erwähnt werden (z. B. Diversität, Fehlererkennung durch automatische Prüfungen) können ebenfalls zur Erkennung von Funktionsfehlern beitragen.

9 Validierung der Performance Levels und Kategorien

9.1 Analyse und Prüfung

Für das SRP/CS oder eine Kombination von SRP/CSs, das/die die Sicherheitsfunktion(en) bietet, muss die Validierung nachweisen, dass die in der Spezifikation der Sicherheitsanforderungen geforderten Performance Levels (PL_r) und Kategorien erfüllt werden. Grundsätzlich erfordert dies eine Fehleranalyse an Hand von Schaltplänen (siehe Abschnitt 5) und, falls die Fehleranalyse nicht schlüssig ist:

- Prüfungen durch Fehlersimulationen in den tatsächlich vorhandenen Steuerkreisen und Fehlerauslösung an tatsächlich vorhandenen Bauteilen, insbesondere in Teilen des Systems, bei denen es Zweifel hinsichtlich der bei der Fehleranalyse ermittelten Ergebnisse gibt (siehe Abschnitt 6);
- eine Simulation des Verhaltens der Steuerung beim Auftreten von Fehlern, z. B. mittels Hardware- und/oder Softwaremodellen.

Bei einigen Anwendungen kann es notwendig sein, die verbundenen sicherheitsbezogenen Teile in mehrere Funktionsgruppen zu trennen und diese Gruppen und ihre Verknüpfungen Fehlersimulationsprüfungen zu unterziehen.

Bei der Validierung durch Prüfen sollten die Prüfungen, soweit erforderlich, Folgendes enthalten:

- Prüfungen durch Fehlersimulationen an einem Produktionsmuster;
- Prüfungen durch Fehlersimulationen an einem Hardwaremodell;
- Softwaresimulation von Fehlern; und
- Subsystemfehler, z. B. Energieversorgung.

Der genaue Zeitpunkt, zu dem ein Fehler in ein System eingegeben wird, kann kritisch 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 kritischen Zeitpunkt einzugeben.

9.2 Validierung der Festlegungen von Kategorien

9.2.1 Kategorie B

SRP/CSs der Kategorie B müssen in Übereinstimmung mit den grundlegenden Sicherheitsprinzipien validiert werden (siehe Tabellen A.1, B.1, C.1 und D.1), indem aufgezeigt wird, dass die Spezifikation, die Gestaltung, der Bau und die Wahl der Bauteile mit ISO 13849-1:2006, 6.2.3, übereinstimmen. Es muss nachgewiesen sein, dass die $MTTF_d$ des Kanals mindestens drei Jahre beträgt. Durch Prüfung muss nachgewiesen werden, dass die SRP/CS in Übereinstimmung mit ihren Spezifikationen sind, wie in den Dokumenten für die Validierung beschrieben (siehe 4.5). Für die Validierung der Umgebungsbedingungen siehe 6.1.

ANMERKUNG In bestimmten Fällen können höhere Werte für $MTTF_d$ erforderlich sein — z. B. wenn $PL_r = b$ ist.

9.2.2 Kategorie 1

SRP/CSs der Kategorie 1 müssen validiert werden, indem aufgezeigt wird, dass:

- a) sie die Anforderungen der Kategorie B erfüllen;
- b) die Bauteile bewährt sind (siehe Tabellen A.3 und D.3) und mit mindestens einer der folgenden Bedingungen übereinstimmen:
 - 1) sie sind in der Vergangenheit in zahlreichen Fällen mit erfolgreichen Ergebnissen bei ähnlichen Anwendungen benutzt worden;
 - 2) sie sind nach Prinzipien hergestellt und verifiziert worden, die ihre Eignung und Zuverlässigkeit für sicherheitsbezogene Anwendungen aufzeigen;
- c) bewährte Sicherheitsprinzipien (sofern anwendbar, siehe Tabellen A.2, B.2, C.2 und D.2) richtig umgesetzt wurden und wenn neu entwickelte Prinzipien angewendet wurden, muss validiert werden
 - 1) wie die zu erwartenden Ausfallarten vermieden wurden, und
 - 2) wie Fehler vermieden oder ihre Wahrscheinlichkeit auf einen angemessenen Grad verringert wurde.

Maßgebende Bauteilnormen dürfen benutzt werden, um die Übereinstimmung mit diesem Unterabschnitt aufzuzeigen (siehe Tabellen A.3 und D.3). Es muss nachgewiesen sein, dass die $MTTF_d$ des Kanals mindestens 30 Jahre beträgt.

9.2.3 Kategorie 2

SRP/CSs der Kategorie 2 müssen validiert werden, indem aufgezeigt wird, dass:

- a) sie die Anforderungen der Kategorie B erfüllen;
- b) die angewendeten bewährten Sicherheitsprinzipien (sofern anwendbar) die Anforderungen von 9.2.2 c) erfüllen;
- c) die Testeinrichtung alle maßgeblichen Fehler erkennt, die nacheinander während des Prüfablaufs angewendet werden, und eine angemessene Reaktion der Steuerung bewirkt, die:
 - 1) einen sicheren Zustand einleitet, oder wenn das nicht möglich ist,
 - 2) eine Warnung vor der Gefährdung vorsieht;
- d) die mit der Prüfeinrichtung durchgeführte(n) Prüfung(en) nicht zu einem unsicheren Zustand führen;

e) die Einleitung der Tests durchgeführt wird:

- 1) beim Anlauf der Maschine und vor der Einleitung einer gefährlichen Situation; und
- 2) periodisch während des Betriebs in Übereinstimmung mit der Gestaltungsspezifikation und wenn die Risikobeurteilung und die Art des Betriebs zeigen, dass dies notwendig ist;

ANMERKUNG 1 Die Notwendigkeit und der Umfang von Tests während des Betriebs werden durch die Risikobeurteilung des Konstrukteurs und die Art der notwendigen Handlungen bestimmt.

f) die $MTTF_d$ des funktionellen Kanals ($MTTF_{d,L}$) mindestens drei Jahre beträgt;

g) die $MTTF_{d,TE}$ des Testkanals größer ist als die Hälfte der $MTTF_{d,L}$;

h) die Testrate $\geq 100 \times$ der erwarteten Anforderungsrate ist;

i) der DC_{avg} mindestens 60 % beträgt;

j) die Ausfälle infolge gemeinsamer Ursache (siehe ISO 13849-1:2006, Anhang F) ausreichend verringert wurden.

ANMERKUNG 2 In besonderen Fällen können höhere Werte der $MTTF_d$ und/oder DC_{avg} erforderlich sein — zum Beispiel aufgrund eines hohen PL_r .

9.2.4 Kategorie 3

SRP/CSs der Kategorie 3 müssen validiert werden, indem aufgezeigt wird, dass:

- a) sie die Anforderungen der Kategorie B erfüllen;
- b) die bewährten Sicherheitsprinzipien (wenn anwendbar) die Anforderungen von 9.2.2 c) erfüllen;
- c) ein Einzelfehler nicht zum Verlust der Sicherheitsfunktion führt;
- d) Einzelfehler (einschließlich Fehler gemeinsamer Ursache) in Übereinstimmung mit der sinnvollen Gestaltung und der angewendeten Technologie erkannt werden;
- e) die $MTTF_d$ jedes Kanals mindestens drei Jahre beträgt;
- f) der DC_{avg} mindestens 60 % beträgt;
- g) die Ausfälle infolge gemeinsamer Ursache (siehe ISO 13849-1:2006, Anhang F) ausreichend verringert wurden.

ANMERKUNG In besonderen Fällen können höhere Werte der $MTTF_d$ und/oder DC_{avg} erforderlich sein — zum Beispiel aufgrund eines hohen PL_r .

9.2.5 Kategorie 4

SRP/CSs der Kategorie 4 müssen validiert werden, indem aufgezeigt wird, dass:

- a) sie die Anforderungen der Kategorie B erfüllen;
- b) die bewährten Sicherheitsprinzipien (wenn anwendbar) die Anforderungen von 9.2.2 c) erfüllen;
- c) ein Einzelfehler (einschließlich Fehler gemeinsamer Ursache) nicht zum Verlust der Sicherheitsfunktion führt;

- d) die Einzelfehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt werden, was mit einem DC_{avg} von mindestens 99 % erreicht wird;
- e) wenn ein Einzelfehler mit einem DC_{avg} von mindestens 99 % nicht erkannt wird, eine Anhäufung von Fehlern nicht zum Verlust der Sicherheitsfunktion(en) führt. Der in Betracht gezogene Umfang der Anhäufung von Fehlern muss in Übereinstimmung mit der sinnvollen Gestaltung sein;
- f) die $MTTF_d$ jedes Kanals mindestens 30 Jahre beträgt;
- g) Ausfälle infolge gemeinsamer Ursachen (siehe ISO 13849-1:2006, Anhang F) ausreichend verringert wurden.

9.3 Validierung von $MTTF_d$, DC_{avg} und CCF

Die Validierung von $MTTF_d$, DC_{avg} und CCF wird üblicherweise durch Analyse und Sichtprüfung durchgeführt.

Die $MTTF_d$ -Werte für Bauteile (einschließlich B_{10d} , T_{10d} und n_{op} -Werte) müssen auf ihre Plausibilität überprüft werden (z. B. durch Vergleich mit ISO 13849-1:2006, Anhang C). Beispielsweise muss der Wert, der auf dem Datenblatt des Lieferanten angegeben ist, mit ISO 13849-1:2006, Anhang C, verglichen 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, weshalb das Bauteil nicht zur Berechnung der $MTTF_d$ des Kanals beiträgt.

ANMERKUNG 2 Für die Ermittlung des B_{10d} -Wertes siehe z. B. IEC 60947-4-1:2010, Anhang K.

Der $MTTF_d$ jedes Kanals der SRP/CS, einschließlich Anwendung der Symmetrisierungsgleichung (siehe ISO 13849-1:2006, Anhang D) bei unterschiedlichen redundanten Kanälen, muss auf die richtige Berechnung überprüft werden. Es ist sicherzustellen, dass der $MTTF_d$ einzelner Kanäle auf höchstens 100 Jahre begrenzt wurde, bevor die Symmetrisierungsgleichung angewendet wird.

Die DC-Werte von Bauteilen und/oder logischen Blöcken müssen auf Plausibilität überprüft werden (z. B. durch Vergleich mit Maßnahmen nach ISO 13849-1:2006, 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.

Der DC_{avg} der SRP/CS ist auf richtige Berechnung zu überprüfen.

Die richtige Durchführung ausreichender Maßnahmen gegen Ausfälle aufgrund gemeinsamer Ursache muss validiert werden (z. B. durch Vergleich mit ISO 13849-1:2006, Anhang F). Typische Validierungsmaßnahmen sind eine statische Hardwareanalyse und Funktionsprüfungen unter Umgebungsbedingungen.

ANMERKUNG 3 Für die Berechnung der $MTTF_d$ -Werte elektronischer Bauteile wird eine Umgebungs-temperatur 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 (z. B. mehr als 15 °C Abweichung), wird es notwendig, $MTTF_d$ -Werte für die abweichende Umgebungstemperatur zu verwenden.

9.4 Validierung von Maßnahmen zur Vermeidung systematischer Ausfälle hinsichtlich des Performance Levels und der Kategorie des SRP/CS

Die Validierung von Maßnahmen zur Vermeidung systematischer Ausfälle (definiert in ISO 13849-1:2006, 3.1.7) hinsichtlich der Performance Level und Kategorien jedes SRP/CS kann üblicherweise durchgeführt werden durch

- a) Überprüfungen von Entwicklungsdokumenten, die die Übereinstimmung mit den
 - 1) grundlegenden und bewährten Sicherheitsprinzipien (siehe Anhänge A bis D),
 - 2) weiteren Maßnahmen zur Vermeidung systematischer Ausfälle (siehe ISO 13849-1:2006, G.3), und
 - 3) weiteren Maßnahmen für die Steuerung systematischer Ausfälle wie Diversität der Hardware (siehe ISO 13840-1:2006, Anhang G), Schutz vor Änderung oder Failure Assertion Programmierung bestätigen;
- b) Fehleranalyse (z. B. FMEA);
- c) Tests durch Fehlereingabe/Fehlerauslösung;
- d) Inspektion und Prüfung von Datenkommunikation, sofern verwendet;
- e) Überprüfung, ob durch ein Qualitätsmanagementsystem Ursachen systematischer Ausfälle während des Herstellungsprozesses vermieden werden.

9.5 Validierung der sicherheitsbezogenen Software

Die Validierung sowohl von sicherheitsbezogener Embedded-Software (SRESW) als auch von sicherheitsbezogener Anwendungssoftware (SRASW) muss Folgendes beinhalten:

- das festgelegte Funktionsverhalten und die Leistungskriterien (z. B. Zeitverhalten) der Software, wenn sie auf der Zielhardware ausgeführt wird,
- eine Verifizierung, ob die Softwaremaßnahmen für den festgelegten PL_r der Sicherheitsfunktion ausreichen, und
- angewandte Maßnahmen und Methoden zur Vermeidung von systematischen Softwarefehlern während der Softwareentwicklung.

Als erster Schritt ist zu überprüfen, dass eine Dokumentation der Spezifikation und Gestaltung der sicherheitsbezogenen Software vorhanden ist. Diese Dokumentation ist zu untersuchen, um ihre Vollständigkeit sowie die Vermeidung von fehlerhaften Auslegungen, Unterlassungen und Widersprüchen zu überprüfen.

ANMERKUNG Im Fall von kleinen Programmen kann eine Programmanalyse durch Nachprüfungen oder Analyse des Kontrollflusses (en: walk trough), der Prozeduren usw. ausreichend sein, indem die Softwaredokumentation (Kontrollflussdiagramm, Quellcodes von Modulen oder Blöcken, I/O und Variablenzuweisungslisten, Querverweislisten) verwendet wird.

Im Allgemeinen kann die Software als „black box“ oder „grey box“ (siehe ISO 13849-1:2006, 4.6.2) betrachtet und entsprechend durch Black-Box- bzw. Grey-Box-Prüfungen validiert werden.

In Abhängigkeit vom PL_r [ISO 13849-1:2006, 4.6.2 (für SRESW) und 4.6.3 (für SRASW)] sollten die Prüfungen Folgendes beinhalten:

- Black-Box-Prüfung des funktionellen Verhaltens und der Leistungsfähigkeit (z. B. Zeitverhalten),
- zusätzlich erweiterte Prüffälle, die auf Grenzwertanalysen beruhen, empfohlen für PL d oder 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 auf der Software beruhenden Maßnahmen zur Fehlerbeherrschung zu bewerten.

Einzelne Softwarefunktionen, die bereits validiert wurden, brauchen nicht erneut validiert zu werden. Wenn eine Anzahl derartiger Sicherheitsfunktionsblöcke für ein besonderes Projekt kombiniert wird, muss jedoch die sich daraus ergebende gesamte Sicherheitsfunktion validiert werden.

Die Softwaredokumentation muss überprüft werden, um nachzuweisen, dass ausreichende Maßnahmen und Methoden gegen systematische Softwareausfälle in Übereinstimmung mit dem vereinfachten V-Modell (ISO 13849-1:2006, Bild 6) angewendet wurden.

Die Maßnahmen zur Softwareimplementierung nach ISO 13849-1:2006, 4.6.2 (für SRESW) und 4.6.3 (für SRASW), 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.

9.6 Validierung und Verifizierung des Performance Levels

Für das vereinfachte Verfahren zur Abschätzung des PL der SRP/CS nach ISO 13849-1:2006, 4.5.4 und ISO 13849-1:2006, Anhang B bis F und Anhang K, sind die folgenden Schritte zur Verifizierung und Validierung durchzuführen:

- Überprüfung der ordnungsgemäßen Beurteilung des PL bezüglich der Kategorie, des DC_{avg} und der $MTTF_d$ (nach ISO 13849-1:2006, 4.5.4 und Anhang K);
- Verifizierung, dass der von den SRP/CS erreichte PL mit dem erforderlichen Performance Level PL_r übereinstimmt, der in der Spezifikation der Sicherheitsanforderungen für die Maschine festgelegt ist: $PL \geq PL_r$.

Wenn andere Verfahren zur Beurteilung des erreichten PL angewendet werden, der auf der abgeschätzten durchschnittlichen Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde beruht, muss die Validierung Folgendes berücksichtigen:

- den $MTTF_d$ -Wert für jedes Bauteil,
- den DC,
- den CCF,
- die Struktur, und
- die Dokumentation, Anwendung und Berechnung, welche auf ihre Richtigkeit überprüft werden müssen.

9.7 Validierung der Kombination sicherheitsbezogener Teile

Wenn die Sicherheitsfunktion durch zwei oder mehrere sicherheitsbezogene Teile ausgeführt wird, muss die Validierung der Kombination — durch Analyse und, wenn nötig, durch Prüfung — durchgeführt werden, um zu bestätigen, dass die Kombination den bei der Gestaltung festgelegten Performance Level erreicht. Vorhandene aufgezeichnete Validierungsergebnisse von sicherheitsbezogenen Teilen können dabei berücksichtigt werden. Die folgenden Validierungsschritte müssen durchgeführt werden:

- Überprüfung der Entwicklungsdokumente, die die gesamte(n) Sicherheitsfunktion(en) beschreiben;
- Überprüfen, ob der Gesamt-PL der SRP/CS-Kombination auf der Grundlage des PL jedes einzelnen sicherheitsbezogenen Teils richtig beurteilt wurde (nach ISO 13849-1:2006, 6.3);

ANMERKUNG Eine Addition der durchschnittlichen Wahrscheinlichkeit von gefahrbringenden Ausfällen je Stunde aller kombinierten SRP/CS kann als Alternative zu ISO 13849-1:2006, Tabelle 11 verwendet werden. Es ist wichtig, die nicht quantifizierbaren Beschränkungen von systematischen architektonischen und CCF-Aspekten, die den Gesamt-Performance Level auf niedrigere Werte verringern können, zu überprüfen.

- Berücksichtigung von Schnittstelleneigenschaften, z. B. Spannung, Strom, Druck, Datenformat der Signale, Signalpegel;
- Fehleranalyse hinsichtlich der Kombination/Integration, z. B. durch FMEA;
- Fehlereingabeproofungen für redundante Systeme in Abhängigkeit der Kombination/Integration.

10 Validierung der Umgebungsanforderungen

Die bei der Gestaltung festgelegte Leistungsfähigkeit der SRP/CS muss hinsichtlich der spezifizierten Umgebungsbedingungen für die Steuerung validiert werden.

Die Validierung muss durch Analyse durchgeführt werden und wenn nötig, durch Prüfung. Der Umfang der Analyse und Prüfung hängt von den sicherheitsbezogenen Teilen ab, von dem System, in dem sie eingebaut sind, der angewendeten Technologie und der/den Umgebungsbedingung(en), die validiert werden. Die Anwendung von Betriebszuverlässigkeitsdaten des Systems oder seiner Bauteile, oder die Bestätigung der Übereinstimmung mit den entsprechenden Normen für die Umgebungsbedingungen (z. B. für die Wasserdichtigkeit, Schutz vor Schwingung) können diesen Validierungsprozess unterstützen.

Sofern anwendbar, muss sich die Validierung beziehen auf

- zu erwartende mechanische Beanspruchungen durch Schock, Schwingung, das Eindringen von Verschmutzungen,
- mechanische Haltbarkeit,
- elektrische Nennwerte und Energieversorgungen,
- klimatische Bedingungen (Temperatur und Luftfeuchte), und
- elektromagnetische Verträglichkeit (Immunität).

Wenn eine Prüfung notwendig ist, um die Übereinstimmung mit den Umgebungsanforderungen zu bestimmen, müssen die Vorgehensweisen, wie sie in den entsprechenden Normen beschrieben sind, befolgt werden, soweit es für die Anwendung erforderlich ist.

Nach dem Abschluss der Validierung durch Prüfung müssen die Sicherheitsfunktionen weiterhin in Übereinstimmung mit den Festlegungen für die sicherheitstechnischen Anforderungen sein, oder die SRP/CS müssen einen Ausgang/Ausgänge für einen sicheren Zustand erzeugen.

11 Validierung der Instandhaltungsanforderungen

Das Validierungsverfahren muss aufzeigen, dass die Anforderungen für die Instandhaltung, wie sie in ISO 13849-1:2006, Abschnitt 9, Absatz 2, festgelegt sind, umgesetzt wurden.

Die Validierung der Instandhaltungsanforderungen muss, sofern anwendbar, Folgendes enthalten:

- a) eine Durchsicht der Benutzerinformationen, um zu bestätigen, dass
 - 1) die Instandhaltungsanleitungen [einschließlich Verfahren, erforderlicher Werkzeuge, Häufigkeit der Überprüfungen, Zeitintervalle für den Austausch von Verschleißteilen (T_{10d}) usw.] vollständig und verständlich sind,
 - 2) falls zutreffend, Anweisungen vorhanden sind, dass die Instandhaltung nur durch sachkundiges Instandhaltungspersonal durchgeführt werden darf;
- b) eine Überprüfung, dass Maßnahmen zur Erleichterung der Instandhaltung (z. B. Bereitstellung von Diagnosewerkzeugen zur Hilfe bei der Fehlererkennung und Reparatur) angewendet wurden.

Zusätzlich sind folgende Maßnahmen aufzunehmen, sofern sie angewendet werden:

- Maßnahmen zur Vermeidung von Fehlern während der Instandhaltung (z. B. Erkennung falscher Eingangsdaten durch Überprüfungen der Plausibilität);
- Maßnahmen gegen Änderungen (z. B. ein Passwortschutz, um nicht berechtigte Personen am Zugang zum Programm zu hindern).

12 Validierung der technischen Dokumentation und Benutzerinformation

Der Validierungsprozess muss nachweisen, dass die Anforderungen an die technische Dokumentation, wie in ISO 13849-1:2006, Abschnitt 10 festgelegt sowie an die Benutzerinformation, wie in ISO 13849-1:2006, Abschnitt 11, festgelegt, umgesetzt wurden.

Anhang A (informativ)

Validierungswerkzeuge für mechanische Systeme

Wenn mechanische Systeme in Verbindung mit anderen Technologien verwendet werden, sollte ebenfalls Anhang A berücksichtigt werden.

Die Tabellen A.1 und A.2 enthalten grundlegende und bewährte Sicherheitsprinzipien.

Tabelle A.3 führt bewährte Bauteile für eine sicherheitsbezogene Anwendung auf, die auf der Anwendung bewährter Sicherheitsprinzipien und/oder einer Norm für deren besondere Anwendung basieren. Ein für bestimmte Anwendungen bewährtes Bauteil kann für andere ungeeignet sein.

In den Tabellen A.4 und A.5 werden Fehlerausschlüsse und die zugehörigen Begründungen angegeben. Für weitere Ausschlüsse siehe 4.4.

Der genaue Zeitpunkt, zu dem ein Fehler auftritt, kann kritisch sein (siehe 9.1).

Tabelle A.1 — Grundlegende Sicherheitsprinzipien

Grundlegendes Sicherheitsprinzip	Bemerkungen
Anwendung geeigneter Werkstoffe und angemessener Herstellungsverfahren	Auswahl des Werkstoffs, der Herstellungs- und Behandlungsverfahren unter Berücksichtigung von z. B. Spannungen, Haltbarkeit, Elastizität, Reibung, Verschleiß, Korrosion, Temperatur
ordnungsgemäße Dimensionierung und Formgebung	Berücksichtigen z. B. von Spannung, Dehnung, Ermüdung, Oberflächenrauheit, Grenzabmaßen, Hängenbleiben, Herstellungsverfahren
geeignete Auswahl, Kombination, Anordnungen, Zusammenbau und Einbau der Bauteile/des Systems	Berücksichtigen von Anwendungshinweisen des Herstellers, z. B. Katalogblätter, Einbauanweisungen, Festlegungen, sowie Anwendung bewährter technischer Erfahrungen mit ähnlichen Bauteilen/Systemen
Anwendung des Prinzips der Energietrennung	Der sichere Zustand wird durch Freischaltung von Energie erreicht. Siehe maßgeblicher Vorgang zum Stillsetzen in ISO 12100:2010, 6.2.11.3. Zum Ingangsetzen der Bewegung eines Mechanismus wird Energie zugeführt. Siehe maßgeblicher Vorgang zur Inangsetzung in ISO 12100:2010, 6.2.11.3. Berücksichtigen von unterschiedlichen Betriebsarten, z. B. Betriebsmodus, Instandhaltungsmodus. WICHTIG — Dieses Prinzip darf nicht angewendet werden, wenn durch einen Energieverlust eine Gefährdung entstehen würde, z. B. Freigabe eines Werkzeuges durch den Verlust der Spannkraft.
geeignete Befestigung	Bei der Anwendung von Schraubensicherungen die Anwendungshinweise des Herstellers beachten. Durch Anwendung eines geeigneten Drehmomenten-Begrenzungs-Verfahrens kann Überbeanspruchung vermieden und ein angemessener Widerstand gegen das Lösen der Verbindung erreicht werden.