

DIN EN ISO 13849-2

ICS 13.110

Entwurf

Einsprüche bis 2010-08-07
Vorgesehen als 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/DIS 13849-2:2010);
Deutsche Fassung prEN ISO 13849-2:2010**

Safety of machinery –
Safety-related parts of control systems –
Part 2: Validation (ISO/DIS 13849-2:2010);
German version prEN ISO 13849-2:2010

Sécurité des machines –
Parties des systèmes de commande relatifs à la sécurité –
Partie 2: Validation (ISO/DIS 13849-2:2010);
Version allemande prEN ISO 13849-2:2010

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2010-06-07 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

- vorzugsweise als Datei per E-Mail an nasg@din.de in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme abgerufen werden;
- oder in Papierform an den Normenausschuss Sicherheitstechnische Grundsätze (NASG) im DIN, 10772 Berlin (Hausanschrift: Burggrafenstr. 6, 10787 Berlin).

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

Gesamtumfang 91 Seiten

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

Beginn der Gültigkeit

Diese Norm gilt ab ...¹⁾

Nationales Vorwort

Dieser Norm-Entwurf enthält sicherheitstechnische Festlegungen im Sinne der 9. Verordnung zum Geräte- und Produktsicherheitsgesetz (GPSG).

Dieses Dokument enthält die Deutsche Fassung des 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-Entwurfs prEN ISO 13849-2:2010. 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 12100-1	siehe	DIN EN ISO 12100-1
ISO 13849-1	siehe	DIN EN ISO 13849-1

Im Verzeichnis „Literaturhinweise“ angegebene Normen

ISO/DIS 4413	siehe	E DIN EN ISO 4413
ISO/DIS 4414	siehe	E DIN EN ISO 4414
ISO 4960	siehe	DIN EN 10140 (modifizierte Übernahme)
ISO 5598	keine nationale Entsprechung	
ISO 11161	siehe	DIN EN ISO 11161
ISO 12100-2	siehe	DIN EN ISO 12100-2
ISO 13850	siehe	DIN EN ISO 13850
ISO 13851	siehe	DIN EN 574
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 (modifizierte Übernahme)
IEC 60269-1	siehe	DIN EN 60269-1
IEC 60529	siehe	DIN EN 60529
IEC 60664-Reihe	siehe	DIN EN 60664-Reihe
IEC 60812	siehe	DIN EN 60812
IEC 60947-Reihe	siehe	DIN EN 60947-Reihe
IEC 61025	siehe	DIN EN 61025

1) Wird bei Herausgabe als Norm festgelegt.

IEC 61078	siehe	DIN EN 61078
IEC 61165	siehe	DIN EN 61165
IEC 61249-2	siehe	DIN EN 61249-2
IEC 61558-Reihe	siehe	DIN EN 61558-Reihe
IEC 61810-Reihe	siehe	DIN EN 61810-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 Verweise;
- 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 Neuaufeilung 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.

Nationaler Anhang NA (informativ)

Literaturhinweise

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

DIN EN 1037:2008-11, *Sicherheit von Maschinen — Vermeidung von unerwartetem Anlauf; Deutsche Fassung EN 1037:1995+A1:2008*

DIN EN 1088:2008-10, *Sicherheit von Maschinen — Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen — Leitsätze für Gestaltung und Auswahl; Deutsche Fassung EN 1088:1995+A2:2008*

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

DIN EN 10140, *Kaltband — Grenzabmaße und Formtoleranzen*

DIN EN 60204-1:2007-06, *Sicherheit von Maschinen — Elektrische Ausrüstung von Maschinen — Teil 1: Allgemeine Anforderungen (IEC 60204-1:2005, modifiziert); Deutsche Fassung EN 60204-1:2006*

DIN EN 602691, *Niederspannungssicherungen — Teil 1: Allgemeine Anforderungen*

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

DIN EN 60664 (alle Teile), *Isolationskoordination für elektrische Betriebsmittel in Niederspannungsanlagen*

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

DIN EN 60947 (alle Teile), *Niederspannungsschaltgeräte*

DIN EN 61025, *Fehlzustandsbaumanalyse*

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

DIN EN 61165, *Anwendung des Markoff-Verfahrens*

DIN EN 61249-2 (alle Teile), *Materialien für Leiterplatten und andere Verbindungsstrukturen*

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

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

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

E 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 12100-1, *Sicherheit von Maschinen — Grundbegriffe, allgemeine Gestaltungsleitsätze — Teil 1: Grundsätzliche Terminologie, Methodologie*

DIN EN ISO 12100-2:2004-04, *Sicherheit von Maschinen — Grundbegriffe, allgemeine Gestaltungsleitsätze — Teil 2: Technische Leitsätze (ISO 12100-2:2003); Deutsche Fassung EN ISO 12100-2:2003*

DIN EN ISO 13849-1:2008-12, *Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen — Teil 1: Allgemeine Gestaltungsleitsätze (ISO 13849-1:2006); Deutsche Fassung EN ISO 13849-1:2008*

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

CEN/TC 114

Datum: 2010-03

prEN ISO 13849-2:2010

CEN/TC 114

Sekretariat: DIN

Sicherheit von Maschinen und Geräten — Sicherheitsbezogene Teile von Steuerungen — Teil 2: Validierung (ISO/DIS 13849-2:2010)

Sécurité des machines — Parties des systèmes de commande relatifs à la sécurité — Partie 2: Validation (ISO/DIS 13849-2:2010)

Safety of machinery — Safety-related parts of control systems — Part 2: Validation (ISO/DIS 13849-2:2010)

ICS:

Deskriptoren

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokument-Stage: CEN-Umfrage
Dokument-Sprache: D

Inhalt

Seite

Vorwort	3
Einleitung.....	4
1 Anwendungsbereich	5
2 Normative Verweisungen.....	5
3 Begriffe	5
4 Validierungsverfahren	5
4.1 Validierungsleitsätze	5
4.2 Validierungsplan	8
4.3 Allgemeine Fehlerlisten	8
4.4 Spezielle Fehlerlisten	8
4.5 Angaben zur Validierung	9
4.6 Validierungsaufzeichnung	11
5 Validierung durch Analyse	11
5.1 Allgemeines.....	11
5.2 Analysentechniken	11
6 Validierung durch Prüfen	12
6.1 Allgemeines.....	12
6.2 Messunsicherheit.....	13
6.3 Höherwertige Festlegungen	13
6.4 Anzahl der Prüflinge.....	13
7 Validierung der Spezifikation der Sicherheitsanforderungen.....	13
8 Validierung der Sicherheitsfunktionen.....	14
9 Validierung der Performance Levels und Kategorien.....	15
9.1 Analyse und Prüfung der Performance Level und Kategorien	15
9.2 Validierung der Festlegungen für Kategorien	15
9.3 Validierung von $MTTF_d$, DC_{avg} und CCF.....	17
9.4 Validierung der Maßnahmen zur Vermeidung systematischer Ausfälle hinsichtlich des Performance Levels und der Kategorie des SRP/CS	18
9.5 Validierung der sicherheitsbezogenen Software	18
9.6 Validierung und Nachweis des Performance Levels	19
9.7 Validierung der Kombination von sicherheitsbezogenen Teile.....	20
10 Validierung der Umgebungsanforderungen	20
11 Validierung der Instandhaltungsanforderungen	21
12 Validierung der technischen Dokumentation und Benutzerinformation	21
Anhang A (informativ) Möglichkeiten zur Validierung mechanischer Systeme	22
Anhang B (informativ) Möglichkeiten zur Validierung pneumatischer Systeme.....	27
Anhang C (informativ) Möglichkeiten zur Validierung hydraulischer Systeme.....	39
Anhang D (informativ) Möglichkeiten zur Validierung elektrischer Systeme	49
Anhang E (informativ) Beispiel der Validierung von Fehlverhalten und Mitteln zur Diagnose.....	64
Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der Richtlinie 2006/42/EG	85
Literaturhinweise	86

Vorwort

Dieses Dokument (prEN ISO 13849-2:2010) wurde vom Technischen Komitee ISO/TC 199 „Safety of machinery“ in Zusammenarbeit mit dem Technische Komitee CEN/TC 114 „Sicherheit von Maschinen und Geräten“, dessen Sekretariat vom DIN gehalten wird, erarbeitet.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Dieses Dokument wird EN ISO 13849-2:2008 ersetzen.

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

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

Diese zweite Ausgabe ersetzt die erste Ausgabe (ISO 13849-2:2003), die technisch überarbeitet wurde, um sich an ISO 13849-1:2006 anzupassen. Außerdem gibt der neue Anhang E ein Beispiel für die Validierung von Fehlverhalten und Mitteln zur Diagnose an.

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

— Teil 1: Allgemeine Gestaltungsleitsätze

— Teil 2: Validierung

Die Anhänge A bis D sind informativ und gegliedert wie in Tabelle 1 angegeben.

Tabelle 1 — Gliederung der Abschnitte der Anhänge A bis D

Anhang	Technik	Liste grundlegender Sicherheitsprinzipien	Liste bewährter Sicherheitsprinzipien	Liste bewährter Bauteile	Fehlerlisten und Fehlerausschlüsse
		Abschnitte			
A	Mechanisch	A.2	A.3	A.4	A.5
B	Pneumatisch	B.2	B.3	B.4	B.5
C	Hydraulisch	C.2	C.3	C.4	C.5
D	Elektrisch (enthält Elektronik)	D.2	D.3	D.4	D.5

Dieses Dokument enthält Literaturhinweise.

Anerkennungsnotiz

Der Text von ISO 13849-2:2010 wurde vom CEN als prEN ISO 13849-2:2010 ohne irgendeine Abänderung genehmigt.

Einleitung

Dieses Dokument ist eine Typ-B-Norm, wie in ISO 12100-1 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. Diese Internationale Norm legt das Validierungsverfahren, einschließlich sowohl Analyse als auch Prüfung, für die Sicherheitsfunktionen, Kategorien und Performance Levels von sicherheitsbezogenen Teilen von Steuerungen fest. Die meisten der Verfahren und Bedingungen in dieser Internationalen Norm 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. Wird ein anderes Verfahren angewendet (z.B. das Markov-Modell), können einige Teile dieser Norm möglicherweise nicht angewendet werden und es können zusätzliche Anforderungen notwendig sein. Diese Norm gibt keine Anleitung für den besonderen Fall, wenn andere Verfahren zur Abschätzung des PL angewendet werden.

Beschreibungen der Sicherheitsfunktionen und die Anforderungen für die Kategorien und Performance Levels sind in ISO 13849-1 gegeben, die sich mit den allgemeinen Leitsätzen für die Gestaltung befasst. Einige Anforderungen für die Validierung sind allgemeiner und einige besonderer Art entsprechend der angewendeten Technologie. ISO 13849-2 legt auch die Bedingungen fest, unter welchen die Validierung beim Prüfen der sicherheitsbezogenen Teile von Steuerungen durchgeführt werden sollte.

ISO 13849-1 legt die Sicherheitsanforderungen fest und gibt Anleitung für die Leitsätze bei der Gestaltung (siehe ISO 12100-1) der sicherheitsbezogenen Teile von Steuerungen. Sie legt für diese Teile die Kategorie und den Performance Level fest und beschreibt die Eigenschaften ihrer Sicherheitsfunktionen unabhängig von der verwendeten Energieart.

Das Erreichen der Anforderungen kann durch alle möglichen Kombinationen der Analyse (siehe Abschnitt 5) und der Prüfung (siehe Abschnitt 6) validiert werden. Mit der Analyse sollte so früh wie möglich im Gestaltungsprozess begonnen werden.

1 Anwendungsbereich

Diese Internationale Norm legt die Vorgehensweisen und Bedingungen in Übereinstimmung mit ISO 13849-1 fest, die bei der Validierung durch Analyse und Prüfung zu befolgen sind, für

- die vorgesehenen Sicherheitsfunktionen, und
- die ausgeführten Kategorien, und
- den erreichten Performance Level

der sicherheitsbezogenen Teile der Steuerung (SRP/CS), bei Anwendung der durch den Konstrukteur vorgesehenen sinnvollen Gestaltung.

ANMERKUNG Anforderungen für programmierbare elektronische Systeme einschließlich der damit verbundenen Software sind in ISO 13849-1:2006, 4.6 und in den Normen der Reihe 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 12100-1, *Safety of machinery — Basic concepts, general principles for design — Part 1: Basic terminology, methodology*

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 13849-1.

4 Validierungsverfahren

4.1 Validierungsleitsätze

Der Zweck des Validierungsverfahrens ist, die Spezifizierung und die Konformität der Gestaltung der sicherheitsbezogenen Teile der Steuerung (SRP/CS) innerhalb der Gesamtspezifizierungen für die Sicherheitsanforderungen an der Maschine zu bestätigen.

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

- den festgelegten Sicherheitseigenschaften der Sicherheitsfunktionen für diesen Teil, wie in der sinnvollen Gestaltung realisiert;
- den Anforderungen für den festgelegte Performance Level (siehe ISO 13849-1:2006, 4.5);
- den Anforderungen für die festgelegte Kategorie (siehe ISO 13849-1:2006, 6.2);
- Maßnahmen zur Steuerung und zur Vermeidung systematischer Ausfälle (siehe ISO 13849-1:2006, Anhang G), und
- falls vorhanden, die Anforderungen an die Software (siehe ISO 13849-1:2006, 4.6);
- die Fähigkeit, eine Sicherheitsfunktion unter den erwarteten Umgebungsbedingungen zu leisten.

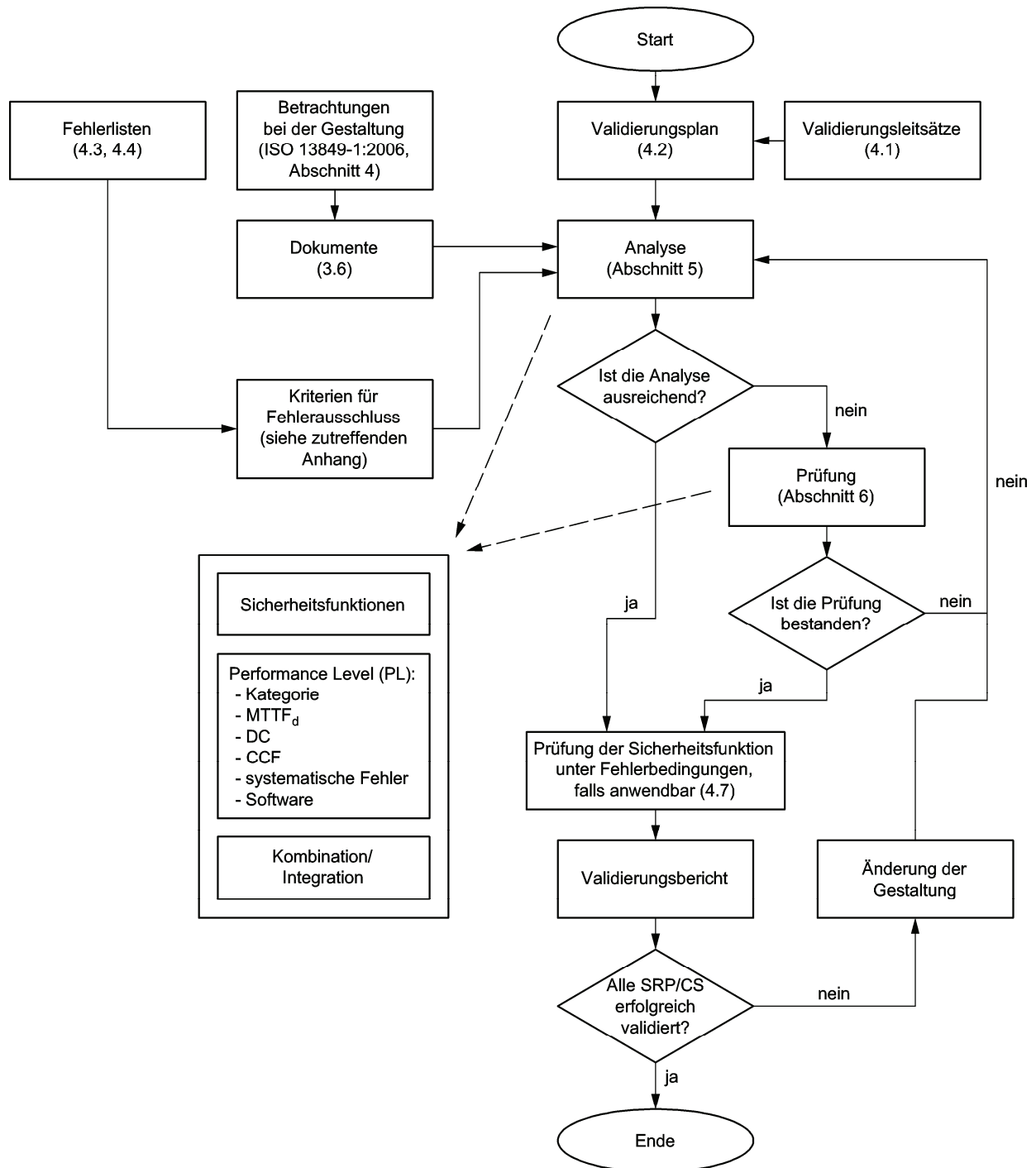
ANMERKUNG Die Validierung der Gestaltung von SRP/CS schließt Überprüfungsmaßnahmen ein. Die Validierung und Überprüfung sollte von Personen mit Ausnahme des Konstrukteurs des entsprechenden Teils ausgeführt werden. Die Überprüfung sollte auf der Spezifizierung der Sicherheitsanforderungen und der Gestaltungsdokumentation beruhen.

Die Validierung besteht aus der Durchführung der Analyse und aus der Durchführung von Funktionsprüfungen unter normalen Bedingungen in Übereinstimmung mit dem Validierungsplan. Bild 1 gibt einen Überblick über das Validierungsverfahren. Die Abwägung zwischen Analyse und Prüfung hängt von der Technologie und dem Performance Level ab. Wo es für die Kategorie 2, 3, und 4 erforderlich ist, muss die Sicherheitsfunktion auch durch Prüfung unter Fehlerbedingungen validiert werden.

Mit der Analyse sollte so früh wie möglich und gleichzeitig mit dem Gestaltungsprozess begonnen werden, so dass Probleme frühzeitig korrigiert werden können, in einem Stadium, in dem sie relativ leicht korrigierbar sind, d. h. im Rahmen der Schritte „Gestaltung und technische Realisierung der Sicherheitsfunktionen“ und „Ermittlung des Performance Levels PL“ (Kästchen 4 und 5 in Bild 3 der ISO 13849-1:2006). Für einige Analysen kann es notwendig sein, sie solange hinauszuschieben, bis die Gestaltung gut entwickelt ist.

Für umfangreiche Systeme können aufgrund der Größe, Komplexität oder integrierten Art (mit der Maschine) der Steuerung spezielle Zusammenstellungen gemacht werden für:

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



ANMERKUNG Der Block „Änderung der Gestaltung“ bezieht sich auf das Gestaltungsverfahren. Wenn die Validierung nicht erfolgreich beendet werden kann, sind Änderungen in der Gestaltung erforderlich. Danach sollte die Validierung der geänderten Teile wiederholt werden. Dieses Verfahren sollte solange wiederholt werden, bis sämtliche Teile erfolgreich validiert sind.

Bild 1 — Übersicht über das Validierungsverfahren

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. Wo es angemessen ist, muss er darlegen:

- a) die Identität der Dokumente für die Festlegungen;
- b) die Betriebs- und Umgebungsbedingungen während der Prüfung;
- c) die anzuwendenden Analysen und Prüfungen;
- d) den Verweis auf anzuwendende Prüfnormen;
- e) die für jeden Teil der Validierung verantwortlichen Personen oder Parteien.

Sicherheitsbezogene Teile, die früher validiert wurden, benötigen nur einen Verweis auf die frühere Validierung.

4.3 Allgemeine Fehlerlisten

Das Validierungsverfahren schließt die Überlegung des Verhaltens von SRP/CS für alle zu berücksichtigenden Fehler ein. Eine Grundlage für die Fehlerbetrachtung ist in den Fehlerlisten der informativen Anhänge (A.5, B.5, C.5 und D.5) zu finden, die sich auf Erfahrungen abstützen. Die allgemeinen Fehlerlisten enthalten:

- die einzubeziehenden Bauteile/Elemente, z. B. Leiter/ Kabel (siehe D.5.2);
- die zu berücksichtigenden Fehler, z. B. Kurzschlüsse zwischen Leitern;
- die erlaubten Fehlerausschlüsse, unter Berücksichtigung von Umgebungs-, Betriebs- und Anwendungsaspekten;
- eine Spalte für Bemerkungen, die die Begründungen für Fehlerausschlüsse enthält.

In den Fehlerlisten sind nur permanente Fehler berücksichtigt.

4.4 Spezielle Fehlerlisten

Eine spezielle auf das Produkt bezogene Fehlerliste muss 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.

Wo diese spezielle auf das Produkt bezogene Fehlerliste auf der (den) allgemeinen Liste(n) aufbaut, muss sie Folgendes bestätigen:

- die aus der/n allgemeinen Liste(n) einbezogenen Fehler;
- alle anderen relevanten einbezogenen Fehler, die nicht in der allgemeinen Liste aufgeführt sind (z. B. Ausfall infolge gemeinsamer Ursache);
- 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 befriedigt sind;

und, ausnahmsweise

- alle anderen Fehler für die die allgemeine(n) Liste(n) einen Ausschluss nicht zulässt, jedoch zusammen mit einer Begründung und sinnvollen Erklärung für ihren Ausschluss (siehe ISO 13849-1:2006, 7.3).

Wo diese Liste nicht auf der/n allgemeinen Liste(n) aufbaut, muss der Konstrukteur eine sinnvolle Erklärung für Fehlerausschlüsse geben.

4.5 Angaben zur Validierung

Die Angaben, die für die Validierung erforderlich sind, unterscheiden sich hinsichtlich der angewendeten Technologie, der Kategorie(n) und des/der Performance Level(s), die aufzuzeigen sind, der sinnvollen Gestaltung des Systems und hinsichtlich des Beitrages der SRP/CS für die Risikoverringerung. Dokumente, die in ausreichendem Maße die Angaben aus unten stehender Liste enthalten, müssen im Validierungsverfahren aufgenommen sein, um den/die erreichten Performance Level(s), Kategorie(n) und die Sicherheitsfunktion(en) der sicherheitsbezogenen Teile aufzuzeigen:

- a) Spezifikation über die erforderliche Leistungsfähigkeit jeder Sicherheitsfunktion und ihre/n erforderliche Kategorie und Performance Level;
- b) Zeichnungen und Festlegungen, z. B. für mechanische, hydraulische und pneumatische Teile, gedruckte Steuerkreisläufe, Montagepläne, interne Verdrahtung, Gehäuse, Werkstoffe, Aufstellung;
- c) Blockdiagramm(e) mit Funktionsbeschreibung der Blöcke;
- d) Steuerkreisdigramm(e) einschließlich ihrer Verknüpfungen/Verbindungen;
- e) Funktionsbeschreibung der Steuerkreisdigramme;
- f) Zeitfolgediagramm(e) für schaltende Bauteile, für Signale, die für die Sicherheit zuständig sind;
- g) Beschreibung der entsprechenden Eigenschaften von früher validierten Bauteilen;
- h) für andere sicherheitsbezogene Teile (ausgenommen der unter g) aufgelisteten) die Bauteillisten mit Stückbezeichnung, Nennwerten, Toleranzen, wesentlichen Betriebsbeanspruchungen, Typ-Bezeichnungen, Daten über Fehlerraten und Bauteilhersteller und alle anderen Daten, die für die Sicherheit maßgebend sind;
- i) Analyse aller relevanten Fehler (siehe auch 4.2), die z. B. in A.5, B.5, C.5 und D.5 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.

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

- 1) eine Spezifikation, die klar und eindeutig ist, und die das Erreichen der geforderten sicherheitstechnischen Leistungsfähigkeit der Software bestätigt, und
- 2) den Beweis, dass die Software so gestaltet ist, dass sie den erforderlichen Performance Level erreicht, und
- 3) Einzelheiten über Prüfungen (insbesondere Prüfberichte), die durchgeführt wurden, um zu bestätigen, dass die geforderte sicherheitstechnische Leistungsfähigkeit erreicht wurde.

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

- 1) ein sicherheitsbezogenes Blockdiagramm (siehe ISO 13849-1:2006, Anhang B) oder vorgesehene Architektur (siehe ISO 13849-1:2006, 6.2);
- 2) die Bestimmung von $MTTF_d$ (mittlere Zeit bis zum gefahrbringenden Ausfall), DC_{avg} (durchschnittlicher Diagnosedeckungsgrad) und CCF (Ausfall infolge gemeinsamer Ursache);
- 3) die Bestimmung der Kategorie (siehe Tabelle 2).

Es sind Angaben zur Dokumentation über systematische Aspekte der SRS/CS erforderlich.

Es sind Angaben darüber erforderlich, inwiefern die Kombination verschiedener SRP/CS die Anforderungen an den Performance Level erfüllt.

Tabelle 2 — Anforderungen an die Dokumentation für Kategorien als Teil 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 zu verarbeitenden Werkstoffe	X	X	X	X	X
Leistungsfähigkeit während anderer wesentlicher äußerer Einflüsse	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 Prüfverfahren für die Sicherheitsfunktion(en)	—	—	X	—	—
durchgeführte Diagnosemaßnahmen einschließlich Fehlerreaktion	—	—	X	X	X
Prüfintervalle, wenn festgelegt	—	—	X	X	X
Diagnosedeckungsgrad (DC_{avg})	—	—	X	X	X
bei der Gestaltung berücksichtigte vorhersehbare Einzelfehler und das angewendete Erkennungsverfahren	—	—	X	X	X
die erkannten Fehler gemeinsamer Ursache und wie sie verhindert werden	—	—	X	X	X
die vorhersehbaren ausgeschlossenen Einzelfehler	—	—	—	X	X
Fehler, die zu erkennen sind	—	—	X	X	X
verschiedene Fehleranhäufungen, die bei der Gestaltung zu berücksichtigen sind	—	—	—	—	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 ist erforderlich					
— Dokumentation ist nicht erforderlich					

ANMERKUNG Die in Tabelle 2 erwähnten 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 aller sicherheitstechnischen Anforderungen ersichtlich machen. Es dürfen Querverweise zu vorhergehenden Validierungsaufzeichnungen gemacht werden, vorausgesetzt, sie sind richtig gekennzeichnet.

Für jedes sicherheitsbezogene Teil, das einen Teil des Validierungsverfahrens nicht bestanden hat, muss die Aufzeichnung den Teil (die Teile) beschreiben, die die Validierungsprüfungen und/oder -analysen nicht bestanden haben. Es muss sichergestellt sein, dass sämtliche Teile nach der 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 erkannten Sicherheitsfunktion(en) und den/die erforderlichen Performance Level, die sich bei der Risikoanalyse an der Maschine ergeben (siehe ISO 13849-1:2006, Bild 1 und 3);
- die Zuverlässigkeit ($MTTF_d$, DC_{av} und CCF) (siehe ISO 13849-1:2006, 4.2 bis 4.5);
- die Systemstruktur (z. B. vorgesehene Architektur) (siehe ISO 13849-1:2006, 4.2 bis 4.5, Abschnitt 6);
- die nicht quantifizierbaren qualitativen Aspekte, die Auswirkung auf das Systemverhalten haben (siehe ISO 13849-1:2006, 4.2 bis 4.5);
- 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, Fehlerraten, Erfahrungen bei der Anwendung) basiert. Diese Betrachtung ist abhängig von der Anwendung. Diese und andere Faktoren können die deterministischen Argumente beeinflussen.

ANMERKUNG 2 Deterministische Argumente unterscheiden sich von anderen Beweisführungen dadurch, dass sie zeigen, dass die geforderten Eigenschaften des Systems einem Systemmodell logisch folgen. Solche Argumente können auf der Grundlage einfacher, gut verständlicher Begriffe entwickelt werden, wie z. B. die Genauigkeit einer mechanischen Verriegelung.

5.2 Analysentechniken

Die auszuwählende Analysentechnik hängt von der Zielrichtung der Analyse ab. Es bestehen zwei grundsätzliche Arten von Techniken:

- a) „Top-down“ (deduktive) Techniken sind zur Bestimmung der Ursachen geeignet, die zu den festgestellten Ausgangsereignissen führen können und zur Abschätzung der Wahrscheinlichkeit von Ausgangsereignissen abhängig von der Wahrscheinlichkeit der Ursachen. Sie können auch angewendet werden bei der Untersuchung der Folgen von erkannten Mehrfachfehlern. Beispiele für „top-down“-Techniken sind die Fehlerbaumanalyse (FTA – siehe IEC 61025) und die Ereignisbaumanalyse (ETA).
- b) „Bottom-up“ (induktive) Techniken sind für die Untersuchung der Folgen von festgestellten Einzelfehlern geeignet. Beispiele für „bottom-up“-Techniken sind die Ausfallarten- und Effektanalyse (FMEA - siehe IEC 60812) und die Fehlerarten, Auswirkungs- und kritischen Zustandsanalyse (FMECA).

6 Validierung durch Prüfen

6.1 Allgemeines

Wenn die Validierung durch Analyse nicht überzeugend ist, müssen Prüfungen durchgeführt werden, um die Validierung zu vervollständigen. Eine Prüfung ist immer zusätzlich zur Analyse durchzuführen und ist oft notwendig.

Die Validierung durch Prüfungen muss 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 zu erwartenden Ergebnisse der Prüfungen;
 - 3) die Reihenfolge der Prüfungen.
- b) Prüfaufzeichnungen müssen erstellt werden, die Folgendes beinhalten:
 - 1) den Namen der Person, die die Prüfung durchführt;
 - 2) die Umgebungsbedingungen (siehe Abschnitt 10);
 - 3) die Vorgehensweisen bei der Prüfung und die verwendete Ausrüstung;
 - 4) das Prüfdatum;
 - 5) die Ergebnisse der Prüfung.
- c) Die Prüfaufzeichnungen müssen mit dem Prüfplan verglichen werden, um Gewissheit zu erhalten, dass die festgelegten Funktions- und Leistungsziele erreicht sind.

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

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

Wo angebracht, muss die Validierung von Sicherheitsfunktionen durch Prüfung durchgeführt werden, bei der Signale in verschiedenen Kombinationen in die SRP/CS eingegeben werden. Die korrespondierenden Ausgänge müssen mit den entsprechend festgelegten Ausgangssignalen verglichen werden.

Es wird empfohlen, dass die Kombination dieser Eingabesignale systematisch der Steuerung und der Maschine anzupassen ist. Ein Beispiel für diese Logik ist: Energie einschalten, in Betrieb setzen, Arbeitsablauf, Richtungsumkehr, Wiederanlaufen. Wo notwendig, muss eine erweiterte Anzahl Eingangsdaten eingegeben werden, um anormale oder ungewöhnliche Situationen zu berücksichtigen, und um zu sehen, wie die SRP/CS reagieren. Solche Kombinationen von Eingangsdaten müssen vorhersehbare fehlerhafte Abläufe berücksichtigen.

Die Zielstellungen bei der Prüfung werden maßgeblich durch die Umgebungsbedingungen bei dieser Prüfung beeinflusst. Diese Bedingungen können sein:

- a) normale Umgebungsbedingungen bei bestimmungsgemäßer Verwendung; oder
- b) Bedingungen bei besonderen Nennwerten; oder
- c) bestimmte Bandbreiten für Bedingungen, wenn Driften zu erwarten ist.

ANMERKUNG Die Bandbreite für Bedingungen, die als beständig angesehen werden kann und für die Prüfungen gültig sind, sollten zwischen dem Konstrukteur und dem verantwortlichen Prüfpersonal abgestimmt und aufgezeichnet werden.

6.2 Messunsicherheit

Die Messunsicherheiten bei der Validierung durch Prüfen müssen der durchgeführten Prüfung angemessen sein. Im Allgemeinen müssen Messunsicherheiten für Temperaturen innerhalb 5 K liegen und im Folgenden innerhalb 5 % bei:

- a) Zeitmessungen,
- b) Druckmessungen,
- c) Kraftmessungen,
- d) elektrischen Messungen,
- e) Messungen der relativen Feuchte,
- f) Abstandsmessungen.

Abweichungen von diesen Messunsicherheiten müssen begründet werden.

6.3 Höherwertige Festlegungen

Wenn die Steuerung entsprechend der Angaben in den Begleitdokumenten höherwertige Festlegungen als die Anforderungen dieser Norm erfüllt, müssen die höherwertigen Festlegungen zu Grunde gelegt werden.

ANMERKUNG Derartig höherwertige Festlegungen können zu Grunde gelegt werden, wenn die Steuerung besonders ungünstigen Betriebsbedingungen standhalten muss, z. B. raue Handhabung, Einwirkungen von Feuchte, Hydrolyse, Veränderungen bei der Umgebungstemperatur, Auswirkungen von chemischen Mitteln, Korrosion, hohe Intensität elektromagnetischer Felder, z. B. in der Nähe von Sendern.

6.4 Anzahl der Prüflinge

Soweit nicht anderweitig festgelegt, müssen die Prüfungen an einem einzelnen Muster des/der sicherheitsbezogenen Teils/e durchgeführt werden, das allen entsprechenden Prüfungen standhalten sollte.

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

Einige Prüfungen können dauerhaft die Leistungsfähigkeit einiger Bauteile verändern. Wo die dauerhafte Veränderung in den Bauteilen der Grund dafür ist, dass die sicherheitsbezogenen Teile außerhalb der Gestaltungsfestlegung liegen, muss/müssen (ein) weitere(s) Muster für nachfolgende Prüfungen verwendet werden.

Wo eine bestimmte Prüfung zerstörend wirkt und gleichwertige Ergebnisse durch die Prüfung eines getrennten Teiles der SRP/CS erhalten werden können, darf ein Muster dieses Teils anstelle des gesamten Ausrüstungsmusters benutzt werden, um an das Ergebnis für diese Prüfung zu gelangen. Dieses Vorgehen darf nur angewendet werden, wo sich durch Analyse ergeben hat, dass die Prüfung des(r) sicherheitsbezogenen Teile(s) ausreichend ist, um seine sicherheitstechnische Leistungsfähigkeit zu bestätigen.

7 Validierung der Spezifikation der Sicherheitsanforderungen

Vor der Validierung der Gestaltung der SRP/CS oder der Kombination von SRP/CS, die die Sicherheitsfunktion enthält, muss die Spezifikationsanforderung an die Sicherheitsfunktion bestätigt werden.

ANMERKUNG 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 an alle Sicherheitsfunktionen der Maschinensteuerung dokumentiert werden.

Um die Spezifikation zu validieren, sollten geeignete Maßnahmen gegen systematisches Fehler (Versagen, Auslassungen und Unbeständigkeiten) getroffen werden.

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

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

Wo 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 die Betätigung der gestalteten SRP/CS oder Kombination der SRP/CS, die die Sicherheitsfunktion enthalten, den festgelegten Eigenschaften entspricht.

ANMERKUNG 1 Das Versagen der Sicherheitsfunktionen, wenn keine Hardwarefehler vorhanden sind, beruht auf systematischen Fehlern während der Gestaltung und der Anpassungsstufen (z. B. eine Fehlinterpretation der Eigenschaften der Sicherheitsfunktion, ein Fehler in der logischen Gestaltung, ein Fehler innerhalb des Hardwareaufbaus, ein Fehler beim Tippen des Softwarecodes usw.). Einige Fehler werden durch Untersuchungen während des Gestaltungsprozesses entdeckt, aber andere bleiben unbemerkt oder führen zu keinem Fehler, bis die Gestaltung fortgeschritten ist. Zusätzlich ist es ebenfalls möglich, einen Fehler während des Validierungsprozesses zu begehen (z. B. einige Eigenschaften ohne Überprüfung auszulassen).

Die Validierung der festgelegten Eigenschaften der Sicherheitsfunktion muss durch Anwendung geeigneter Maßnahmen der folgenden Liste durchgeführt werden:

- funktionale Analyse der Schaltbilder, Überprüfungen des Programms (siehe 9.5);
ANMERKUNG 2 Wenn eine Maschine komplexe oder eine große Anzahl von Sicherheitsfunktionen hat, kann die Analyse die Anzahl der Funktionsprüfungen verringern.
- Simulation;
- Überprüfung der in die Maschine eingebauten Hardwarebestandteile und der Software, um ihre Übereinstimmung mit der Dokumentation (z. B. Herstellung, Art, Bauart) zu bestätigen;
- Funktionsprüfung der Sicherheitsfunktionen (nach ISO 13849-1:2006, Abschnitt 5) in allen Betriebsarten der Maschine. Die Funktionsprüfung muss sicherstellen, dass alle sicherheitsbezogenen Ausgangssignale über ihren gesamten Bereich umgesetzt sind. Das schließt Überlastungsprüfungen ein. Die Prüffälle werden normalerweise von den Spezifikationen abgeleitet, können jedoch auch einige Fälle enthalten, die aus der Analyse der Schaltbilder oder des Programms abgeleitet sind;
- erweiterte Funktionsprüfung, um vorhersehbare abnormale Signale und Kombinationen von Signalen von irgendeiner Eingangsquelle zu überprüfen, einschließlich Energieunterbrechung, -wiederkehr und fehlerhafte Betätigungen;
- Überprüfung der Betriebsverknüpfung der SRP/CS auf Erfüllung ergonomischer Richtlinien (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 der Performance Level und Kategorien

Die Validierung der Performance Level und Kategorien der SRP/CS oder der Kombination der SRP/CS, die die Sicherheitsfunktion enthalten, muss zeigen, dass die festgelegten erforderlichen Performance Level (PL_r) erfüllt sind. Grundsätzlich sind die folgenden Verfahren anwendbar:

— eine Fehleranalyse der Steuerkreisdigramme (siehe Abschnitt 5);

und wo die Fehleranalyse nicht überzeugend ist:

- bei redundanten Systemen Fehlereingabeprüfungen bei den tatsächlich vorhandenen Steuerkreisen und Fehlersimulation an demselben Typ/Modell der tatsächlich vorhandenen Bauteile, besonders in zweifelhaften Bereichen hinsichtlich der bei der Analyse festgestellten Leistungsfähigkeit (siehe Abschnitt 6);
- eine Simulation des Verhaltens der Steuerung bei Fehlerfällen, z. B. mit Mitteln von Hardware- und/oder Softwaremodellen.

In einigen Anwendungsfällen kann es notwendig sein, die verbundenen sicherheitsbezogenen Teile in verschiedene Funktionsgruppen zu trennen und diese Gruppen und ihre Verknüpfungen Fehlersimulationsprüfungen zu unterziehen.

Bei der Durchführung der Validierung durch Prüfen können die Prüfungen, sofern angemessen, enthalten:

- Fehlereingabeprüfungen an einem Produktionsmuster;
- Fehlereingabeprüfungen an einem Hardwaremodell;
- Softwaresimulation von Fehlern;
- Subsystemfehler, z. B. Energieversorgung.

Der genaue Zeitpunkt, bei dem ein Fehler in ein System eingegeben wird, kann kritisch sein. Die Auswirkung im schlimmsten Fall (en: worst case effect) bei einer Fehlereingabe sollte anhand einer Analyse bestimmt werden und der Fehler sollte entsprechend dieser Analyse zu diesem geeigneten kritischen Zeitpunkt eingegeben werden, um diese Auswirkung zu prüfen.

9.2 Validierung der Festlegungen für Kategorien

9.2.1 Kategorie B

Die SRP/CS der Kategorie B müssen in Übereinstimmung mit den grundlegenden Sicherheitsprinzipien validiert werden (siehe A.2, B.2, C.2 und D.2), indem aufgezeigt wird, dass die Spezifikation, die Gestaltung, Konstruktion und 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. Das muss durch Prüfung so erreicht werden, dass die SRP/CS, so wie in den Dokumenten für die Validierung vorgesehen, in Übereinstimmung mit ihren Spezifikationen sind (siehe 4.5). Für die Validierung der Umgebungsbedingungen siehe 6.1.

9.2.2 Kategorie 1

SRP/CS der Kategorie 1 müssen validiert werden, um aufzuzeigen, dass:

- a) sie die Anforderungen der Kategorie B erfüllen;
- b) die Bauteile bewährt sind (siehe A.4 und D.4) unter mindestens einer der folgenden Bedingungen:
 - 1) sie sind in zahlreichen Fällen mit erfolgreichen Ergebnissen bei ähnlichen Anwendungen benutzt worden;
 - 2) sie sind nach Prinzipien hergestellt worden, die ihre Eignung und Zuverlässigkeit für sicherheitsbezogene Anwendungen aufzeigen;
- c) bewährte Sicherheitsprinzipien (wo anwendbar, siehe A.3, B.3, C.3 und D.3) richtig einbezogen wurden. Wo neu entwickelte Prinzipien angewendet wurden, muss Folgendes validiert werden:
 - 1) wie die zu erwartenden Ausfallarten vermieden wurden;
 - 2) wie Fehler vermieden oder ihre Wahrscheinlichkeit reduziert wurde.

Entsprechende Bauteilnormen dürfen benutzt werden, um die Übereinstimmung mit diesem Unterabschnitt aufzuzeigen (siehe A.4 bis D.4). Es muss nachgewiesen sein, dass die $MTTF_d$ des Kanals mindestens 30 Jahre beträgt.

9.2.3 Kategorie 2

SRP/CS der Kategorie 2 müssen validiert werden, um aufzuzeigen, 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 Prüfeinrichtung alle relevanten Fehler erkennt, die nacheinander während des Prüfablaufs berücksichtigt 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 durchgeführten Prüfungen nicht in einen unsicheren Zustand führen;
- e) die Einleitung der Prüfung durchgeführt wird:
 - 1) beim Anlauf der Maschine und vor der Einleitung einer gefährlichen Situation, und
 - 2) periodisch während des Betriebs, wenn die Risikobeurteilung und die Art des Betriebs zeigen, dass dies notwendig ist.
- f) die $MTTF_d$ des funktionellen Kanals ($MTTF_{d,L}$) mindestens drei Jahre beträgt;
- g) die $MTTF_{d,TE}$ größer ist als die Hälfte der $MTTF_{d,L}$;
- h) die Anforderungsrate $\leq$ Testrate/100 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 In besonderen Fällen können höhere Werte der $MTTF_d$ erforderlich sein, zum Beispiel wegen eines hohen PL_r .

9.2.4 Kategorie 3

SRP/CS der Kategorie 3 müssen validiert werden, um aufzuzeigen, 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 $MTTF_d$ jeden 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 $MTTF_d$ erforderlich sein, zum Beispiel wegen eines hohen PL_r .

9.2.5 Kategorie 4

SRP/CS der Kategorie 4 müssen validiert werden, um aufzuzeigen, 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;
- e) wenn d) nicht möglich ist, 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 $MTTF_d$ jeden Kanals mindestens 30 Jahre beträgt;
- g) der DC_{avg} mindestens 99 % beträgt;
- h) die 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. gegen ISO 13849-1:2006, Anhang C). Beispielsweise muss die Dokumentation des Ursprungs dieser Werte überprüft werden.

Der $MTTF_d$ jeden Kanals der SRP/CS, einschließlich Symmetrisierung, muss auf die richtige Berechnung überprüft werden.

Die DC-Werte von Bauteilen oder Blöcken müssen auf umfassende Dokumentation überprüft werden (z. B. nach ISO 13849-1:2006, Anhang E). Die korrekte Durchführung (Hardware und Software) von Überprüfungen und Diagnosen einschließlich angemessene Fehlerreaktion muss validiert werden, indem unter 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. nach ISO 13849-1:2006, Anhang F). Typische Validierungsmaßnahmen sind eine statische Hardwareanalyse und Funktionsprüfungen unter Umgebungsbedingungen.

ANMERKUNG Für die Berechnung der $MTTF_d$ -Werte elektronischer Bauteile wird eine Umgebungstemperatur von +40 °C als Grundlage genommen. Während der Validierung ist es wichtig, sicherzustellen, dass die als Grundlage angenommenen Umgebungs- und Funktionsbedingungen (besonders die Temperatur) für $MTTF_d$ -Werte erfüllt sind. Wenn eine Vorrichtung oder ein Bauteil deutlich über der festgelegten Temperatur von +40 °C betrieben wird (z. B. bei mehr als 15 °C), wird es notwendig, $MTTF_d$ -Werte für die gestiegene Umgebungstemperatur zu verwenden.

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

Die Validierung von Maßnahmen zur Vermeidung systematischer Ausfälle (Begriff siehe ISO 13849:2006, 3.1.7) hinsichtlich des Performance Levels und der Kategorie jeder SRP/CS kann üblicherweise erhalten werden durch:

- Überprüfung von Dokumenten zur Gestaltung, die die Gültigkeit bestätigen von:
 - grundlegenden und bewährten Sicherheitsprinzipien (siehe Anhänge A bis D);
 - weitere Maßnahmen zur Vermeidung systematischer Ausfälle (siehe ISO 13849-1:2006, G.3), und
 - weitere Maßnahmen für die Steuerung systematischer Ausfälle wie Diversität der Hardware (siehe ISO 13849-1:2006, G.2), Schutz vor Änderung oder Programmierung zur Fehlererklärung;
- Fehleranalyse (z. B. FMEA);
- Fehlereingabeproofungen/Fehlerstimulierung;
- Überprüfung und Prüfung von Datenkommunikation, wo verwendet;
- Überprüfung, dass ein Qualitätsmanagementsystem Ursachen systematischer Ausfälle während des Herstellungsprozesses vermeidet.

9.5 Validierung der sicherheitsbezogenen Software

Die Validierung sowohl von sicherheitsbezogener eingebauter (en: embedded) Software (SRESW) als auch von Anwendungssoftware (SRASW) muss Folgendes enthalten:

- das festgelegte Funktionsverhalten und Leistungskriterien (z. B. Zeitsteuerungsleistung) der Software, wenn sie auf der Zielhardware ausgeführt wird;
- den festgelegten PL_r für die SRP/CS, an denen die Software verwendet wird,
- während der Softwareentwicklung unternommene Maßnahmen und Tätigkeiten zur Vermeidung von systematischen Softwareausfällen.

Als erster Schritt ist zu überprüfen, dass eine Dokumentation der Festlegung und Gestaltung der sicherheitsbezogenen Software vorhanden ist. Diese Dokumentation ist nachzuprüfen, um ihre Vollständigkeit sowie das Nichtvorhandensein von fehlerhaften Auslegungen, Unterlassungen und Unbeständigkeiten zu überprüfen.

ANMERKUNG Im Fall von kleinen Programmen kann eine Programmanalyse durch Nachprüfungen oder Durchläufe des Kontrollflusses, der Verfahren usw. ausreichend sein, indem die Softwaredokumentation (Kontrollflussdiagramm, Quellcodes von Modulen oder Blöcken, I/O und verschiedene Zuweisungslisten, 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-Test oder Grey-Box-Test 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 enthalten:

- Black-Box-Test des funktionellen Verhaltens und der Leistungsfähigkeit (z. B. Zeitsteuerungsleistung);
- zusätzlich erweiterte Prüffälle, die auf Grenzwertanalysen beruhen, empfohlen für PL d oder e;
- I/O-Prüfungen, um sicherzustellen, dass die sicherheitsbezogenen Eingangs- und Ausgangssignale angemessen verwendet werden;
- Prüffälle, die Fehler simulieren, die vorher analytisch festgelegt werden, wie auch die erwartete Reaktion, um die Eignung der auf der Software beruhenden Maßnahmen für die Steuerung der Ausfälle zu bewerten.

Einzelne Softwarefunktionen, die offensichtlich bereits validiert wurden, müssen nicht erneut validiert werden. Wo eine Anzahl solcher Sicherheitsfunktionsblöcke für ein besonderes Projekt kombiniert wurde, muss jedoch die sich daraus ergebende gesamte Sicherheitsfunktion validiert werden.

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

Die Maßnahmen zur Softwareanwendung 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 Anwendung untersucht werden.

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

9.6 Validierung und Nachweis des Performance Levels

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

- Überprüfung der genauen Bestimmung des PL von der Kategorie, dem DC_{avg} und der $MTTF_d$ nach ISO 13849-1:2006, 4.5.4 und Anhang K);
- Nachweis, dass der von den SRP/CS erreichte PL mit dem erforderlichen PL_r übereinstimmt, der aus der Risikobeurteilung erhalten wurde:

$$PL \geq PL_r$$

Wenn andere Verfahren angewendet werden, um den erreichten Performance Level abzuschätzen, der auf der durchschnittlichen Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde beruht, muss die Validierung Folgendes berücksichtigen:

- den $MTTF_d$ -Wert für jedes Baudteil;
- den DC;
- den CCF;
- die Struktur;

und die Dokumentation, Anwendung und Berechnung müssen auf ihre Richtigkeit überprüft werden.

9.7 Validierung der Kombination von sicherheitsbezogenen Teile

Wo die Sicherheitsfunktion durch zwei oder mehrere sicherheitsbezogene Teile ausgeführt ist, muss die Validierung der Kombination (durch Analyse und, wenn nötig, durch Prüfung) durchgeführt werden, um zu bestätigen, dass die Kombination die bei der Gestaltung spezifizierte sicherheitstechnische Leistungsfähigkeit erreicht. Vorhandene Validierungsergebnisse von sicherheitsbezogenen Teilen können dabei berücksichtigt werden. Die folgenden Validierungsschritte müssen durchgeführt werden:

- Überprüfung der Gestaltungsdokumente, die die gesamte(n) Sicherheitsfunktion(en) beschreiben;
- Überprüfen der korrekten Festlegung des Gesamt-PL, der auf dem PL der kombinierten SRP/CS beruht (nach ISO 13849-1:2006, 6.3);

ANMERKUNG Eine Summierung der durchschnittlichen Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde aller kombinierten SRP/CS kann als Alternative zu Tabelle 11 in ISO 13849-1:2006 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 Angaben, Signallevel;
- Fehleranalyse hinsichtlich der Kombination/Integration, z. B. durch FMEA;
- für redundante Systeme Fehlereingabeprüfungen hinsichtlich der Kombination/Integration.

10 Validierung der Umgebungsanforderungen

Die bei der Gestaltung festgelegte Leistungsfähigkeit der SRP/CS muss unter Berücksichtigung der festgelegten 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 ab von den sicherheitsbezogenen Teilen, 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 Umgebungsnormen (z. B. für die Wasserdichtigkeit, Schutz vor Schwingung) können den Validierungsprozess unterstützen.

Wo 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 Feuchte);
- elektromagnetische Verträglichkeit (Immunität).

Wenn es durch die Prüfung notwendig ist, 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 der gesamten Durchführung 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 Richtlinien für die Instandhaltungsanforderungen, wie sie in ISO 13849-1:2006, Abschnitt 9, Absatz 2, festgelegt sind, einbezogen wurden.

ANMERKUNG Die Validierung der Instandhaltungsanforderungen kann folgendermaßen durchgeführt werden:

- Überprüfen der Benutzerinformationen, um zu bestätigen, dass:
 - die Instandhaltungsanleitungen vollständig sind [einschließlich Verfahren, erforderlicher Werkzeuge, Häufigkeit der Überprüfungen, Zeitintervalle für den Austausch von Bestandteilen, die Gegenstand von Abnutzung sind (T_{10d}) usw.], und dass sie verständlich sind;
 - falls zutreffend, dass Richtlinien vorhanden sind, dass die Instandhaltung nur durch sachkundiges Instandhaltungspersonal durchgeführt werden darf;
- Überprüfen der Anwendung von Maßnahmen zur Erleichterung der Instandhaltung (z. B. Bereitstellung von Diagnosewerkzeugen zur Hilfe bei der Fehlererkennung und Reparatur).

Zusätzlich können folgende Maßnahmen angewendet werden:

- Maßnahmen zur Vermeidung von Fehlern während der Instandhaltung (z. B. Erkennung falscher Eingangsdaten durch Überprüfungen der Plausibilität);
- Maßnahmen gegen Veränderung (z. B. ein Passwort, 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, mit einbezogen wurden.

Der Validierungsprozess muss nachweisen, dass die Anforderungen an die Benutzerinformation, wie in ISO 13849-1:2006, Abschnitt 11 festgelegt, mit einbezogen wurden.

Anhang A (informativ)

Möglichkeiten zur Validierung mechanischer Systeme

Inhalt

Anhang A (informativ) Möglichkeiten zur Validierung mechanischer Systeme	22
A.1 Einleitung.....	22
A.2 Liste der grundlegenden Sicherheitsprinzipien	22
A.3 Liste bewährter Sicherheitsprinzipien.....	23
A.4 Liste der bewährten Bauteile.....	25
A.5 Fehlerlisten und Fehlerausschlüsse.....	25
A.5.1 Einleitung.....	25
A.5.2 Verschiedene mechanische Geräte, Bauteile und Elemente	26
A.5.3 Schraubendruckfedern	26

A.1 Einleitung

Bei Anwendung mechanischer Systeme in Verbindung mit anderen Technologien sollten auch die zutreffenden Tabellen für grundlegende und bewährte Sicherheitsprinzipien berücksichtigt werden. Für weitere Fehlerausschlüsse siehe 4.3.

A.2 Liste der grundlegenden Sicherheitsprinzipien

Tabelle A.1 — Grundlegende Sicherheitsprinzipien

Grundlegende Sicherheitsprinzipien	Bemerkungen
Anwendung geeigneter Werkstoffe und Herstellungsverfahren	Auswahl des Werkstoffs, der Herstellungs- und Behandlungsverfahren unter Berücksichtigung von z. B. Spannungen, Haltbarkeit, Elastizität, Reibung, Verschleiß, Korrosion, Temperatur.
richtige Dimensionierung und Formgebung	Berücksichtigen z. B. von Spannung, Dehnung, Ermüdung, Oberflächenrauheit, Toleranzen, Hängenbleiben, Herstellungsverfahren.
geeignete Auswahl, Kombination, Anordnungen, Zusammenbau und Einbau der Bauteile/des Systems	Berücksichtigen von Anwendungshinweisen des Herstellers, z. B. Katalogblätter, Einbauanweisungen, Festlegungen, sowie von Erfahrungen mit ähnlichen Bauteilen/Systemen.
Anwendung des Prinzips der Energietrennung	Der sichere Zustand wird durch Abtrennung von der Energiequelle erreicht. Siehe Primärmaßnahme zum Anhalten in ISO 12100-2:2003, 4.11.3. Zum Ingangsetzen der Bewegung eines Mechanismus wird Energie benötigt. Siehe Primärmaßnahme zum Ingangsetzen in ISO 12100-2:2003, 4.11.3. Berücksichtigen von unterschiedlichen Betriebsarten, z. B. Betriebsmodus, Instandhaltungsmodus. Dieses Prinzip darf bei speziellen Anwendungen nicht benutzt werden, z. B., wenn die Energie für Spannungseinrichtungen aufrecht zu halten ist.

Tabelle A.1 (fortgesetzt)

Grundlegende Sicherheitsprinzipien	Bemerkungen
geeignete Befestigung	Bei der Anwendung von Schraubensicherungen die Anwendungshinweise des Herstellers beachten. Überbeanspruchung kann durch Anwendung eines geeigneten Drehmomenten-Begrenzungs-Verfahrens vermieden werden.
Begrenzung der Erzeugung und/oder Weiterleitung der Kraft und ähnlicher Parameter	Beispiele sind Scherstift, Scherplatte, Drehmomenten-Begrenzungskupplung.
Begrenzung des Bereichs der Umgebungsparameter	Diese Parameter sind z. B. Temperatur, Luftfeuchte, Verunreinigungen am Einbauort. Siehe Abschnitt 8 und Anwendungshinweise des Herstellers beachten.
Begrenzung der Geschwindigkeit und ähnlicher Parameter	Beachten von z. B. Geschwindigkeit, Beschleunigung, Verzögerung, die durch die Anwendung erforderlich sind.
geeignete Reaktionszeit	Beachten von z. B. Verringerung der Federkraft, Reibung, Schmierung, Temperatur, Trägheit bei Beschleunigung und Verzögerung, Kombination von Toleranzen.
Schutz gegen unerwarteten Anlauf	Berücksichtigen von unerwartetem Anlauf, verursacht durch gespeicherte Energie und nach Wiederherstellung der Energieversorgung, für unterschiedliche Betriebsarten wie Betriebsmodus, Instandhaltungsmodus usw. Eine besondere Einrichtung zum Ablassen der gespeicherten Energie kann notwendig sein. Besondere Anwendungen, z. B. Beibehaltung der Energie für Spanneinrichtungen oder Sicherung einer Stellung, benötigen eine getrennte Betrachtungsweise.
Vereinfachung	Verringern der Anzahl der Bauteile in sicherheitsbezogenen Systemen.
Trennung	Trennung der sicherheitsbezogenen Funktionen von anderen Funktionen.
geeignete Schmierung	–
geeigneter Schutz gegen Eindringen von Flüssigkeiten und Staub	Beachten der IP-Schutzart (siehe IEC 60529).

A.3 Liste bewährter Sicherheitsprinzipien

Tabelle A.2 — Bewährte Sicherheitsprinzipien

Bewährte Sicherheitsprinzipien	Bemerkungen
Anwendung sorgfältig ausgewählter Werkstoffe und Herstellungsverfahren	Auswahl der für die jeweilige Anwendung geeigneten Werkstoffe sowie zweckdienlicher Herstellungs- und Behandlungsverfahren.
Anwendung von Bauteilen mit festgelegtem Ausfallverhalten	Das überwiegend auftretende Ausfallverhalten eines Bauteils ist im Voraus bekannt und stets das Gleiche, siehe ISO 12100-2:2003, 4.12.2.
Überdimensionierung/Sicherheitsfaktor	Die Sicherheitsfaktoren werden in Normen angegeben oder beruhen auf Erfahrungen mit sicherheitsbezogenen Anwendungen.

Tabelle A.2 (fortgesetzt)

Bewährte Sicherheitsprinzipien	Bemerkungen
Gesicherte Position	Das bewegliche Element eines Bauteils wird mechanisch in einer der möglichen Position gehalten (Reibung allein ist nicht ausreichend). Um die Position zu verändern, ist das Aufbringen von Kraft notwendig.
erhöhte AUS-Kraft	Eine sichere Stellung/ein sicherer Zustand wird dadurch erreicht, dass die AUS-Kraft gegenüber der EIN-Kraft erhöht wird.
Sorgfältige(r) Auswahl, Kombination, Anordnung, Zusammenbau und Einbau von Bauteilen/Systemen für die jeweilige Anwendung	–
sorgfältige Auswahl der Befestigungsart für die jeweilige Anwendung	Vermeiden einer Befestigung nur durch Reibung.
zwangsläufige mechanische Wirkung/Betätigung	Der abhängige Betrieb (z. B. Parallelbetrieb) mehrerer Teile wird durch ein formschlüssiges mechanisches Verbindungsglied (oder mehrere) erreicht. Das/die Verbindungsglied(er) sollten keine Federn und ähnliche „flexible“ Elemente enthalten (siehe ISO 12100-2:2003, 4.5).
Vervielfachung von Teilen	Verringerung der Fehlerwirkung durch Anwendung mehrerer gleicher Teile, wobei z. B. ein Fehler, der an einer Feder (von vielen Federn) auftritt, keinen gefährlichen Zustand bewirkt.
Anwendung bewährter Federn (siehe auch Tabelle A.3)	Eine bewährte Feder erfordert: — Anwendung sorgfältig ausgewählter Werkstoffe, Herstellungsverfahren (z. B. vor Anwendung vorgenommenes statisches und dynamisches Setzen) und Behandlungsverfahren (z. B. Walzen und Kugelstrahlen); — ausreichende Führung der Feder und — ausreichender Sicherheitsfaktor bei Dauerbeanspruchung (d. h. mit hoher Wahrscheinlichkeit tritt kein Bruch auf). Bewährte Schraubendruckfedern dürfen auch gestaltet werden durch: — Anwendung sorgfältig ausgewählter Werkstoffe, Herstellungsverfahren (z. B. vor Anwendung vorgenommenes statisches und dynamisches Setzen) und Behandlungsverfahren (z. B. Walzen und Kugelstrahlen); — ausreichende Führung der Feder und — eines Abstandes zwischen den Windungen bei unbelasteter Feder, der kleiner als der Drahtdurchmesser ist, und — einer ausreichenden Kraft nach einem Bruch oder nach mehreren Brüchen (d. h. Bruch/Brüche führ(t)en nicht zu einem gefährlichen Zustand).
reduzierter Bereich der Kraft und ähnlicher Parameter	Festlegen der notwendigen Begrenzung in Abhängigkeit von Erfahrungen und der jeweiligen Anwendung. Beispiele für Begrenzungen sind Scherstift, Scherplatte, Drehmomentbegrenzungskupplung.