DEUTSCHE NORM **Februar 2013**

DIN EN ISO 13849-2

DIN

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

Preisgruppe 31
www.din.de
www.beuth.de

1893485

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 —

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN ISO 13849-2

Oktober 2012

ICS 13.110

Ersatz für EN ISO 13849-2:2008

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

Ref. Nr. EN ISO 13849-2:2012 D

Inhalt

Seite

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, Oberflächentemperatur, 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.

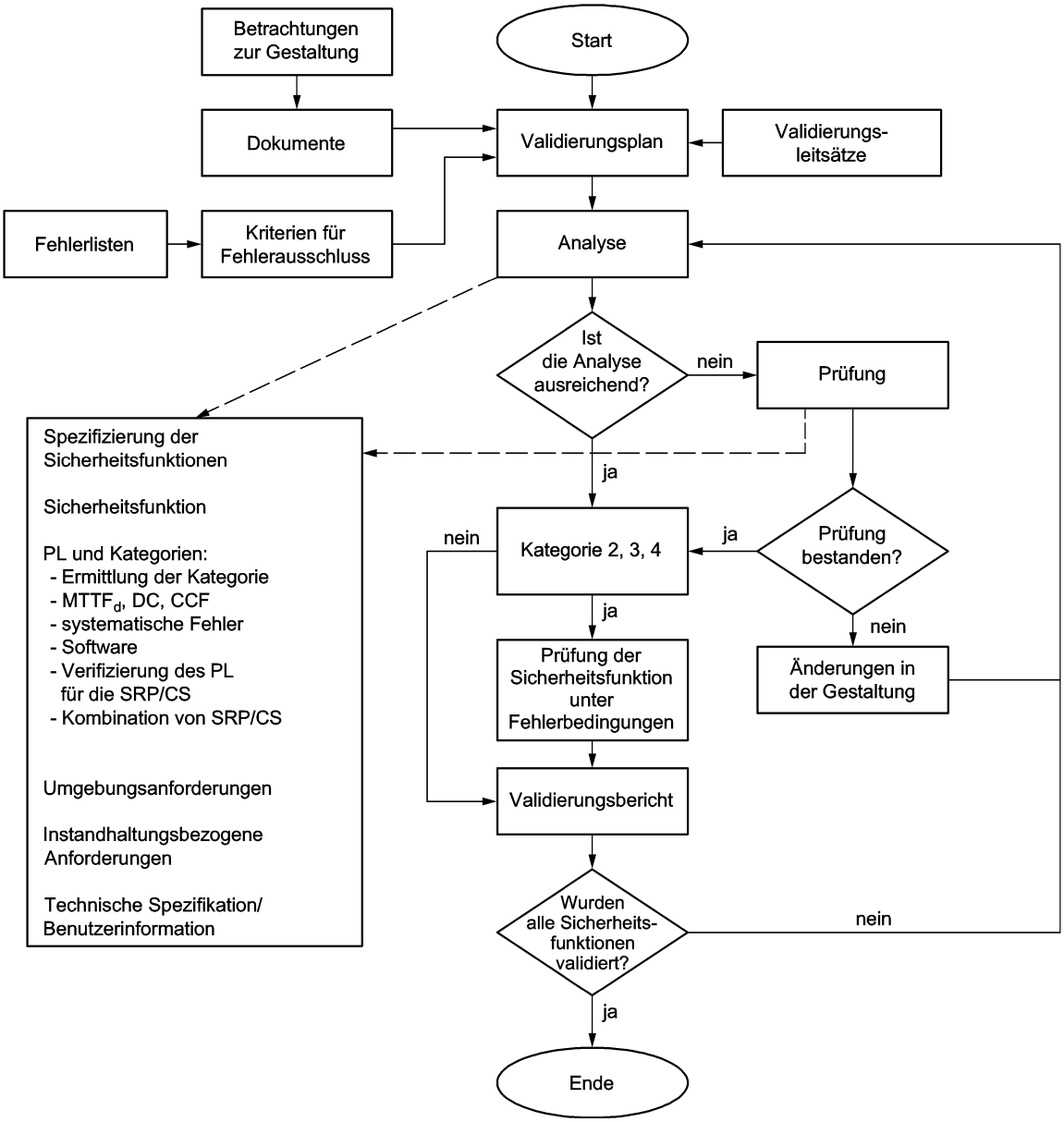


Bild 1 — Übersicht über das Validierungsverfahren

„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 Perfomance Level(s) und/oder Kategorie(n) erfüllen:

a) Festlegung der erforderlichen Eigenschaften jeder Sicherheitsfunktion und ihrer/ihres 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 bestimmbaren 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 Prüfablaufes 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;

— Fehlereingabeprüfungen 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 Ingangsetzung 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.

Tabelle A.1 *(fortgesetzt)*

Grundlegendes Sicherheitsprinzip	Bemerkungen
Begrenzung der Erzeugung und/oder Übertragung der Kraft und ähnlicher Parameter	Beispiele sind Scherstift, Scherplatte, Drehmomenten-Begrenzungskupplung. **WICHTIG — Dieses Prinzip darf nicht angewendet werden, wenn die kontinuierliche Unversehrtheit der Bauteile unerlässlich dafür ist, die erforderliche Steuerungsebene beizubehalten**
Begrenzung des Bereichs der Umgebungsparameter	Beispiele für diese Parameter sind Temperatur, Luftfeuchte, Verunreinigungen am Einbauort. Siehe Abschnitt 10 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 Grenzabmaßen
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. zur Beibehaltung der Energie für Spanneinrichtungen oder zur Sicherung einer Stellung, müssen gesondert betrachtet werden
Vereinfachung	Vermeidung unnötiger Bauteile im sicherheitsbezogenen System
Trennung	Trennung der sicherheitsbezogenen Funktionen von anderen Funktionen
geeignete Schmierung	Beachten der Notwendigkeit von Schmiervorrichtungen, Angaben zu Schmiermitteln und Schmierintervallen
geeigneter Schutz gegen Eindringen von Flüssigkeiten und Staub	Beachten der IP-Schutzart (siehe IEC 60529)

Tabelle A.2 — Bewährte Sicherheitsprinzipien

Bewährtes Sicherheitsprinzip	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 ist stets das Gleiche. Siehe ISO 12100:2010, 6.2.12.3
Überdimensionierung/Sicherheitsfaktor	Es sind die in Normen angegebenen oder auf Erfahrungen mit sicherheitsbezogenen Anwendungen beruhenden Sicherheitsfaktoren anzuwenden.
Gesicherte Position	Das bewegliche Element des Bauteils wird mechanisch in einer sicheren Stellung gehalten (Reibung allein ist nicht ausreichend). Für eine Bewegung aus der gesicherten Position ist das Aufbringen einer Kraft erforderlich
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.
positive mechanisch zwangläufige Wirkung	Um eine mechanisch zwangsläufige Wirkung zu erreichen, müssen alle bewegenden mechanischen Bauteile, die zur Ausführung der Sicherheitsfunktion erforderlich sind, verbundene Bauteile zwangsläufig mitbewegen, z. B. ein Nocken, der die Kontakte eines elektrischen Schalters direkt öffnet statt einer auf einer Feder beruhenden Verbindung (siehe ISO 12100:2010, 6.2.5).
Vervielfachung von Teilen	Verringerung der Auswirkung von Ausfällen durch Anwendung mehrerer gleicher Teile, die parallel zueinander wirken, z. B. wenn ein Ausfall, der an einer von mehreren Federn auftritt, keinen gefährlichen Zustand bewirkt.

Tabelle A.2 *(fortgesetzt)*

Bewährtes Sicherheitsprinzip	Bemerkungen
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 — einen Abstand zwischen den Windungen bei unbelasteter Feder, der kleiner als der Drahtdurchmesser ist; und — eine ausreichende Kraft nach einem Bruch oder nach mehreren Brüchen wird aufrechterhalten (d. h. Bruch/Brüche führen nicht zu einem gefährlichen Zustand). ANMERKUNG Druckfedern werden bevorzugt.
reduzierter Bereich der Kraft und ähnlicher Parameter	Festlegen der notwendigen Begrenzung in Abhängigkeit von Erfahrungen und der jeweiligen Anwendung. Beispiele sind Scherstift, Scherplatte und Drehmomentbegrenzungskupplung **WICHTIG — Dieses Prinzip darf nicht angewendet werden, wenn die kontinuierliche Unversehrtheit der Bauteile unerlässlich dafür ist, die erforderliche Steuerungsebene beizubehalten.**
reduzierter Bereich der Geschwindigkeit und ähnlicher Parameter	Festlegen der notwendigen Begrenzung in Abhängigkeit von Erfahrungen und der jeweiligen Anwendung. Beispiele sind Fliehkraftregler, sichere Überwachung der Geschwindigkeit und Wegbegrenzung.
reduzierter Bereich der Umgebungsparameter	Festlegen der notwendigen Begrenzungen. Beispiele sind Temperatur, Luftfeuchte, Verunreinigung beim Einbau. Siehe Abschnitt 10 und Anwendungshinweise der Hersteller beachten
reduzierter Bereich der Reaktionszeit, Hysteresebegrenzung	Festlegen der notwendigen Begrenzungen. Beachten von z. B. Verringerung der Federkraft, Reibung, Schmierung, Temperatur, Trägheit bei Beschleunigung und Verzögerung, Kombination von Grenzabmaßen

Tabelle A.3 — Bewährte Bauteile

Bewährtes Bauteil	Bedingungen für „bewährt“	Norm oder Festlegung
Schraube	Alle Faktoren, die auf die Schraubverbindung und die Anwendung einen Einfluss ausüben, sind zu berücksichtigen. Siehe Tabelle A.2.	Mechanische Verbindungen wie Schrauben, Muttern, Unterlegscheiben, Nieten, Stifte, Bolzen usw. sind genormt
Feder	Siehe Tabelle A.2 „Anwendung bewährter Federn“.	Technische Festlegungen für Federstähle und andere Sonderanwendungsfälle sind in ISO 4960 gegeben
Nocken	Alle Faktoren, die auf die Anordnung des Nockens (z. B. als Teil einer Verriegelung) Einfluss nehmen, sind zu berücksichtigen. Siehe Tabelle A.2.	Siehe ISO 14119 (Verriegelungseinrichtungen).
Scherstift	Alle Faktoren, die auf die Anwendung Einfluss nehmen, sind zu berücksichtigen. Siehe Tabelle A.2.	—

Tabelle A.4 — Mechanische Geräte, Bauteile und Elemente (z. B. Nocken, Stößel, Kette, Kupplung, Bremse, Welle, Schraube, Stift, Führung, Lager)

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Verschleiß/Korrosion	Ja, wenn Werkstoff, (Über-)Dimensionierung, Herstellungsverfahren, Behandlungsverfahren und geeignete Schmierung entsprechend der festgelegten Lebensdauer sorgfältig ausgewählt sind (siehe auch Tabelle A.2)	Siehe ISO 13849-1:2006, 7.3
nicht Festziehen/Lösen	Ja, wenn Werkstoff, Herstellungsverfahren, Sicherungselemente und Behandlungsverfahren entsprechend der festgelegten Lebensdauer sorgfältig ausgewählt sind (siehe auch Tabelle A.2)	
Bruch	Ja, wenn Werkstoff, (Über-)Dimensionierung, Herstellungsverfahren, Behandlungsverfahren und geeignete Schmierung entsprechend der festgelegten Lebensdauer sorgfältig ausgewählt sind (siehe auch Tabelle A.2)	
Verformung durch Überbeanspruchung	Ja, wenn Werkstoff, (Über-)Dimensionierung, Herstellungsverfahren und Behandlungsverfahren entsprechend der festgelegten Lebensdauer sorgfältig ausgewählt sind (siehe auch Tabelle A.2)	
Steifheit/Hängenbleiben	Ja, wenn Werkstoff, (Über-)Dimensionierung, Herstellungsverfahren, Behandlungsverfahren und geeignete Schmierung entsprechend der festgelegten Lebensdauer sorgfältig ausgewählt sind (siehe auch Tabelle A.2)	

Tabelle A.5 — Schraubendruckfedern

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Verschleiß/Korrosion	Ja, bei Anwendung bewährter Federn und sorgfältig ausgewählter/n Befestigungsarten (siehe Tabelle A.2).	Siehe ISO 13849-1:2006, 7.3.
Verringerung der Kraft durch bleibende Verformung und Bruch		
Bruch		
Steifheit/Hängenbleiben		
Lösen		
Verformung durch Überbeanspruchung		

Anhang B
(informativ)

Validierungswerkzeuge für pneumatische Systeme

Bei Anwendung pneumatischer Systeme in Verbindung mit anderen Technologien sollte auch Anhang B berücksichtigt werden. Wenn pneumatische Bauteile elektrisch verbunden/gesteuert werden, sollten die entsprechenden Fehlerlisten im Anhang D berücksichtigt werden.

ANMERKUNG Zusätzliche Anforderungen können in nationalen Rechtsvorschriften enthalten sein.

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

Eine Aufzählung bewährter Bauteile ist in diesem Anhang B nicht enthalten. Der Status „bewährt“ ist in erster Linie anwendungsbezogen zu sehen. Bauteile können als „bewährt“ beschrieben werden, falls diese ISO 13849-1:2006, 6.2.2, und ISO 4414:2010, Abschnitte 5 bis 7, entsprechen. Ein für bestimmte Anwendungen bewährtes Bauteil kann für andere Anwendungen ungeeignet sein.

In den Tabellen B.3 bis B.18 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 B.1 — Grundlegende Sicherheitsprinzipien

Grundlegendes Sicherheitsprinzip	Bemerkungen
Anwendung geeigneter Werkstoffe und Herstellungsverfahren	Auswahl der Werkstoffe, 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, Grenzabmaßen und Herstellungsverfahren
Geeignete Auswahl, Kombination, Anordnung, 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 Freischalten von Energie an allen relevanten Einrichtungen 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 Ingangsetzung in ISO 12100:2010, 6.2.11.3. Berücksichtigen von unterschiedlichen Betriebsarten, z. B. Betriebsmodus, Instandhaltungsmodus. Dieses Prinzip darf nicht angewendet werden, wenn durch einen Verlust von pneumatischem Druck eine zusätzliche Gefährdung entstehen würde.
Geeignete Befestigung	Bei der Anwendung von z. B. Schraubensicherungen, Armaturen, Klebungen, Spannringen, Anwendungshinweise des Herstellers beachten. Überbeanspruchung kann durch Anwendung eines geeigneten Drehmomenten-Begrenzungs-Verfahrens vermieden werden.
Druckbegrenzung	Beispiele sind Druckbegrenzungsventile, Druckminder-/Druckregelventile

Tabelle B.1 *(fortgesetzt)*

Grundlegendes Sicherheitsprinzip	Bemerkungen
Begrenzung/Verringerung der Geschwindigkeit	Ein Beispiel ist die Geschwindigkeitsbegrenzung eines Kolbens durch ein Stromventil oder eine Drossel.
ausreichende Maßnahmen zur Vermeidung von Verunreinigung des Fluids	Berücksichtigen von Filtration und Abtrennung von Feststoffen und Wasser im Fluid.
geeigneter Schaltzeitbereich	Berücksichtigen von z. B. der Länge der Rohrleitung, Druck, Entlüftungskapazität, Kraft, Verringerung der Federkraft, Reibung, Schmierung, Temperatur, Trägheit bei Beschleunigung und Verzögerung und Zusammenwirken von Grenzabmaßen.
Beständigkeit gegen Umgebungsbedingungen	Gestalten der Einrichtung, dass sie in allen für den Einsatz zu erwartenden Umgebungen und bei allen vorhersehbaren ungünstigen Bedingungen, z. B. für Temperatur, Feuchte, Schwingungen, Verunreinigungen, arbeiten kann. Siehe Abschnitt 10 und Spezifikationen/Anwendungshinweise des Herstellers beachten.
Schutz gegen unerwarteten Anlauf	Berücksichtigen von unerwartetem Anlauf, verursacht durch gespeicherte Energie und nach Wiederherstellung der Energieversorgung, für unterschiedliche Betriebsarten, z. B. Betriebsmodus, Instandhaltungsmodus. Eine besondere Einrichtung zum Ablassen der gespeicherten Energie kann erforderlich sein (siehe ISO 14118:2000, 5.3.1.3). Spezielle Anwendungen (z. B. Beibehaltung der Energie für Spanneinrichtungen oder Sicherung einer Stellung) benötigen eine getrennte Betrachtungsweise.
Vereinfachung	Vermeiden von unnötigen Bauteilen im sicherheitsbezogenen System
geeigneter Temperaturbereich	Dieser ist überall im gesamten System zu berücksichtigen.
Trennung	Trennung der sicherheitsbezogenen Funktionen von anderen Funktionen (z. B. logische Trennung)

Tabelle B.2 — Bewährte Sicherheitsprinzipien

Bewährtes Sicherheitsprinzip	Bemerkungen
Überdimensionierung/Sicherheitsfaktor	Der Sicherheitsfaktor ist in Normen angegeben oder beruht auf Erfahrungen mit sicherheitsbezogenen Anwendungen.
gesicherte Position	Das bewegliche Element des Bauteils wird mechanisch in einer der möglichen Positionen gehalten (Reibung allein ist nicht ausreichend). Um die Position zu verändern, ist das Aufbringen von Kraft notwendig.
erhöhte AUS-Kraft	Eine Lösung kann sein, dass das Flächenverhältnis für die Bewegung eines Ventilschiebers in die sichere Position (AUS-Stellung) gegenüber dem Flächenverhältnis für die Bewegung des Ventilschiebers in die EIN-Stellung wesentlich größer ist (ein Sicherheitsfaktor).
durch den Lastdruck schließendes Ventil	Dies sind im Allgemeinen Sitzventile, z. B. Kegelsitzventile, Kugelventile. Berücksichtigen, wie der Lastdruck aufzubringen ist, um das Ventil auch dann geschlossen zu halten, wenn z. B. die Schließfeder des Ventils bricht.
mechanisch zwangläufige Wirkung	Die mechanisch zwangläufige Wirkung wird für die beweglichen Teile innerhalb der pneumatischen Bauteile angewendet. Siehe auch Tabelle A.2.
Vervielfachung von Teilen	Siehe Tabelle A.2.
Anwendung bewährter Federn	Siehe Tabelle A.2.
Begrenzung/Verringerung der Geschwindigkeit durch einen Widerstand zum Erreichen eines festgelegten Volumenstroms	Beispiele sind Festblende und Festdrossel.
Begrenzung/Verringerung der Kraft	Dies kann erreicht werden durch ein bewährtes Druckbegrenzungsventil, das z. B. mit einer bewährten Feder ausgestattet und korrekt bemessen und ausgewählt ist.
geeigneter Bereich für die Betriebsbedingungen	Die Eingrenzung der Betriebsbedingungen, z. B. Druck-, Volumenstrom- und Temperaturbereich, sollte berücksichtigt werden.
geeignetes Vermeiden einer Verunreinigung des Fluids	Berücksichtigen der Notwendigkeit von hoch wirksamer Filtration und Abscheidung von Feststoffen und Wasser im Fluid.
ausreichend große positive Überdeckung in Schieberventilen	Die positive Überdeckung sichert die Stopp-Funktion und verhindert unzulässige Bewegungen.
Hysteresebegrenzung	Die Hysterese erhöht sich z. B. durch stärkere Reibung. und durch das Zusammenwirken von Grenzabmaßen.

Tabelle B.3 — Fehler und Fehlerausschlüsse — Wegeventile

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Veränderung der Schaltzeiten	Ja, bei mechanisch zwangläufiger Betätigung (siehe Tabelle A.2) der beweglichen Bauteile, sofern die Betätigungskraft ausreichend groß ist.	—
Nichtschalten (Hängenbleiben in der End- oder Nulllage) oder nicht vollständiges Schalten (Hängenbleiben in einer beliebigen Zwischenstellung)	Ja, bei mechanisch zwangläufiger Betätigung (siehe Tabelle A.2) der beweglichen Bauteile, sofern die Betätigungskraft ausreichend groß ist.	
selbsttätige Veränderung der Ausgangs-Schaltstellung (ohne Eingangssignal)	Ja, bei mechanisch zwangläufiger Betätigung (siehe Tabelle A.2) der beweglichen Bauteile, sofern die Haltekraft ausreichend groß ist, oder wenn bewährte Federn angewendet werden (siehe Tabelle A.2) und wenn übliche Einbau- und Betriebsbedingungen vorliegen (siehe Bemerkung), oder bei Schieberventilen mit elastischer Abdichtung und wenn übliche Einbau- und Betriebsbedingungen vorliegen (siehe Bemerkung).	Übliche Einbau- und Betriebsbedingungen liegen vor, wenn — die vom Hersteller vorgegebenen Bedingungen befolgt werden und — sich die Gewichtskraft des bewegenden Bauteils sicherheitstechnisch nicht ungünstig auswirkt (z. B. horizontaler Einbau), und — sich keine Massenträgheitskräfte nachteilig auf die bewegenden Bauteile auswirken (z. B. Bewegungsrichtung des Ventilbauteils berücksichtigt Größe und Richtung der Trägheitskräfte, und — keine extremen Schwingungs- und Schockbeanspruchungen auftreten.
Leckage	Ja, bei Schieberventilen mit elastischer Abdichtung, sofern eine ausreichende positive Überdeckung vorhanden ist [siehe Bemerkung 1)], und wenn übliche Betriebsbedingungen vorliegen und die Druckluft ausreichend aufbereitet und filtriert ist, oder bei Sitzventilen, wenn übliche Betriebsbedingungen vorliegen [siehe Bemerkung 2)] und die Druckluft ausreichend aufbereitet und filtriert ist.	1) Bei Schieberventilen mit elastischer Abdichtung können Effekte durch eine Leckage in der Regel ausgeschlossen werden. Über eine längere Dauer kann jedoch eine geringe Leckage auftreten. 2) Übliche Betriebsbedingungen liegen vor, wenn die vom Hersteller vorgegebenen Bedingungen befolgt werden.
Veränderung des Leckagevolumenstroms über eine lange Einsatzdauer	Nein	—
Bersten des Ventilgehäuses oder Bruch des/der bewegten Bauteils/Bauteile sowie Bruch der Befestigungs- oder Gehäuseschrauben	Ja, wenn Konstruktion, Dimensionierung und Einbau bewährten technischen Erfahrungen entsprechen.	
für Servo- und Proportionalventile: Pneumatische Fehler, die unkontrolliertes Verhalten bewirken	Ja, bei Servo- und Proportionalwegeventilen, wenn sie bedingt durch ihre konstruktive Ausführung sicherheitstechnisch wie konventionelle Wegeventile beurteilt werden können.	—
Werden Steuerfunktionen durch individuelle Einzelfunktionen mehrerer Ventile realisiert, sollte eine Fehlerbetrachtung für jedes Ventil durchgeführt werden. Bei vorgesteuerten Ventilen sollte ebenso vorgegangen werden.		

Tabelle B.4 — Fehler und Fehlerausschlüsse — Absperrventile/Rückschlagventile/Schnellentlüftungsventile/Wechselventile usw.

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Veränderung der Schaltzeiten	Nein	—
Nichtöffnen, nicht vollständiges Öffnen, Nichtschließen oder nicht vollständiges Schließen (Hängenbleiben in einer Endlage oder in einer beliebigen Zwischenstellung)	Ja, wenn das Führungssystem für das/die bewegte(n) Bauteil(e) etwa denen eines nicht gesteuerten Kugelsitzventils ohne ein Dämpfungssystem entsprechen (siehe Bemerkung) und wenn bewährte Federn angewendet sind (siehe Tabelle A.2).	Für ein nicht gesteuertes Kugelsitzventil ohne ein Dämpfungssystem ist das Führungssystem im Allgemeinen so gestaltet, dass ein Hängenbleiben des bewegten Bauteils unwahrscheinlich ist.
selbsttätige Veränderung der Ausgangs-Schaltstellung (ohne Eingangssignal)	Ja, wenn übliche Einbau- und Betriebsbedingungen vorliegen (siehe Bemerkung) und eine ausreichende Schließkraft aufgrund der vorliegenden Drücke und Flächen vorhanden ist.	Übliche Einbau- und Betriebsbedingungen werden eingehalten, wenn — die vom Hersteller festgelegten Bedingungen befolgt werden, und — keine besonderen Massenträgheitskräfte die bewegten Bauteile beeinträchtigen, z. B. Bewegungsrichtung berücksichtigt die Orientierung der beweglichen Maschinenteile, und — keine extremen Schwingungs- und Schockbeanspruchungen auftreten.
für Wechselventile: gleichzeitiger Verschluss beider Eingangsanschlüsse	Ja, wenn bedingt durch Konstruktion und Ausführung des bewegten Bauteils der gleichzeitige Verschluss unwahrscheinlich ist.	—
Leckage	Ja, wenn übliche Betriebsbedingungen vorliegen (siehe Bemerkung) und die Druckluft ausreichend aufbereitet und filtriert ist.	Übliche Betriebsbedingungen liegen vor, wenn die vom Hersteller vorgegebenen Bedingungen befolgt werden.
Veränderung des Leckagevolumenstroms über eine lange Einsatzdauer	Nein	—
Bersten des Ventilgehäuses oder Bruch des/der bewegten Bauteils/Bauteile sowie Bruch der Befestigungs- oder Gehäuseschrauben	Ja, wenn Konstruktion, Dimensionierung und Einbau bewährten technischen Erfahrungen entsprechen.	

Tabelle B.5 — Fehler und Fehlerausschlüsse — Stromregelventile

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Veränderung des Volumenstroms ohne Veränderung der Verstelleinrichtung	Ja, bei Stromregelventilen ohne bewegte Bauteile [siehe Bemerkung 1)], z. B. Drosselventile, wenn übliche Betriebsbedingungen vorliegen [siehe Bemerkung 2)] und die Druckluft ausreichend aufbereitet und filtriert ist.	1) Die Verstelleinrichtung wird nicht als bewegtes Bauteil betrachtet. Veränderungen des Volumenstroms durch Änderung der Druckdifferenz sind bei diesem Ventiltyp physikalisch begrenzt und nicht Gegenstand dieser Fehlerannahme. 2) Übliche Betriebsbedingungen liegen vor, wenn die vom Hersteller festgelegten Bedingungen befolgt werden.
Veränderung des Volumenstroms bei nicht einstellbaren, kreisförmigen Blenden und Düsen	Ja, wenn der Durchmesser $\geq$ 0,8 mm ist, übliche Betriebsbedingungen vorliegen [siehe Bemerkung 2)] und, wenn die Druckluft ausreichend aufbereitet und filtriert ist.	
bei Proportionalstromventilen: Veränderung des Volumenstroms durch unbeabsichtigte Veränderung des Einstellwertes	Nein	—
selbsttätige Veränderung der Verstelleinrichtung	Ja, bei einer wirksamen und dem Einsatzfall angepassten Sicherung der Verstelleinrichtung unter Beachtung (der) sicherheitstechnischer/n Festlegung(en).	
unbeabsichtigtes Lösen (Herausdrehen) des Stellteils/der Stellteile der Verstelleinrichtung	Ja, wenn eine wirksame formschlüssige Sicherung gegen das Lösen (Herausdrehen) vorhanden ist.	
Bersten des Ventilgehäuses oder Bruch des/der bewegten Bauteils/Bauteile sowie Bruch der Befestigungs- oder Gehäuseschrauben	Ja, wenn Konstruktion, Dimensionierung und Einbau bewährten technischen Erfahrungen entsprechen.	

Tabelle B.6 — Fehler und Fehlerausschlüsse — Druckventile

<table>
<tr><th>Betrachteter Fehler</th><th>Fehlerausschluss</th><th>Bemerkungen</th></tr>
<tr><td>Nichtöffnen oder nicht ausreichendes Öffnen bei Überschreiten des Einstelldruckes (Hängenbleiben oder Schwergängigkeit des bewegten Bauteils) [siehe Bemerkung 1)]</td><td rowspan="2">Ja, wenn:
— das Führungssystem für das/die bewegte(n) Bauteil(e) etwa denen eines nicht gesteuerten Kugelsitz- oder Membranventils entsprechen [siehe Bemerkung 2)], z. B. bei einem Druckminderventil mit Sekundärdruckentlastung, und
— die eingebauten Federn bewährte Federn sind (siehe Tabelle A.2).</td><td rowspan="3">1) Diese Fehlerannahme gilt nur, wenn das/die Druckventil(e) für Kraftwirkungen, z. B. zum Spannen, angewendet wird. Diese Fehlerannahme gilt nicht für die übliche Funktion eines Druckventils in Pneumatiksystemen, z. B. Druckminderung, Druckbegrenzung.
2) Für ein nicht gesteuertes Kugelsitz- oder Membranventil ist das Führungssystem im Allgemeinen so gestaltet, dass ein Hängenbleiben des bewegten Bauteils unwahrscheinlich ist.</td></tr>
<tr><td>Nichtschließen oder nicht vollständiges Schließen bei Unterschreiten des Einstelldruckes (Hängenbleiben oder Schwergängigkeit des bewegten Bauteils) [siehe Bemerkung 1)]</td></tr>
<tr><td>Veränderung des Druck-Regelverhaltens ohne Veränderung der Verstelleinrichtung [siehe Bemerkung 1)]</td><td>Ja, bei direkt betätigten Druckbegrenzungsventilen sowie Druckschaltventilen, wenn (eine) bewährte Feder(n) eingebaut ist/sind (siehe Tabelle A.2).</td></tr>
<tr><td>für Proportional-Druckventile: Veränderung des Druck-Regelverhaltens durch unbeabsichtigte Veränderung des Einstellwertes [siehe Bemerkung 1)]</td><td>Nein</td><td rowspan="2">—</td></tr>
<tr><td>selbsttätige Veränderung der Verstelleinrichtung</td><td>Ja, bei einer wirksamen Sicherung der Verstelleinrichtung entsprechend den Anforderungen der Anwendung, z. B. Plombierung.</td></tr>
<tr><td>unbeabsichtigtes Herausdrehen des Stellteils der Verstelleinrichtung</td><td>Ja, wenn eine wirksame formschlüssige Sicherung gegen das Herausdrehen vorhanden ist.</td><td rowspan="2">—</td></tr>
<tr><td>Leckage</td><td>Ja, für Sitzventile, Membranventile und Schieberventile mit elastischer Abdichtung, bei üblichen Betriebsbedingungen (siehe Bemerkung) und wenn die Druckluft ausreichend aufbereitet und filtriert ist.</td><td>Übliche Betriebsbedingungen liegen vor, wenn die vom Hersteller festgelegten Bedingungen befolgt werden.</td></tr>
<tr><td>Veränderung des Leckage-Volumenstroms über eine lange Einsatzdauer</td><td>Nein</td><td rowspan="2">—</td></tr>
<tr><td>Bersten des Ventilgehäuses oder Bruch des/der bewegten Bauteils/Bauteile sowie Bruch der Befestigungs- oder Gehäuseschrauben</td><td>Ja, wenn Konstruktion, Dimensionierung und Einbau bewährten technischen Erfahrungen entsprechen.</td></tr>
</table>

Tabelle B.7 — Fehler und Fehlerausschlüsse — Rohrleitungen

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Bersten und Leckage	Ja, wenn Dimensionierung, Auswahl der Werkstoffe und Befestigung bewährten technischen Erfahrungen entsprechen (siehe Bemerkung).	Bei Anwendung von Kunststoffrohren sind die Herstellerangaben zu beachten, insbesondere bezüglich der Umgebungseinflüsse während des Betriebs, z. B. thermische Einflüsse, chemische Einflüsse oder Einflüsse durch Strahlung. Bei Anwendung von Stahlrohren, die nicht mit einem korrosionshemmenden Mittel behandelt wurden, ist es besonders wichtig, die Druckluft ausreichend zu trocknen.
Fehler am Verbindungselement (z. B. Abreißen/Ausreißen, Leckage)	Ja, wenn Schneidringverschraubungen oder Gewinderohre (d. h. Stahlverschraubungen, Stahlrohre) angewendet werden und wenn Dimensionierung, Auswahl der Werkstoffe, Herstellung, Anordnung und Befestigung bewährten technischen Erfahrungen entsprechen.	—
Zusetzen (Verstopfen)	Ja, bei Rohrleitungen im Leistungskreis Ja, bei Steuer- und Messrohrleitungen, wenn die Nennweite ≥ 2 mm ist.	
Abknicken von Kunststoffrohren mit geringer Nennweite	Ja, wenn die Kunststoffrohre in geeigneter Weise geschützt und verlegt und die entsprechenden Herstellerangaben berücksichtigt werden, z. B. minimaler Biegeradius.	

Tabelle B.8 — Fehler und Fehlerausschlüsse — Schlauchleitungen

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Bersten, Ausreißen aus/Abreißen an der Einbindung und Leckage	Ja, wenn Schlauchleitungen aus Schläuchen nach ISO 4079-1 oder aus ähnlichen Schläuchen (siehe Bemerkung) und den zugehörigen Schlaucharmaturen angewendet werden.	Ein Fehlerausschluss wird nicht angenommen, wenn — die vorgesehene Verwendungsdauer überschritten ist, — die Druckträger (die Verstärkungseinlage) durch Ermüdung versagen kann, — eine äußere Beschädigung unvermeidbar ist.
Zusetzen (Verstopfen)	Ja, bei Schlauchleitungen im Leistungskreis sowie bei Steuer- und Messschlauchleitungen, wenn die Nennweite ≥ 2 mm ist.	—

Tabelle B.9 — Fehler und Fehlerausschlüsse — Verbindungselemente

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Bersten, Schraubenbruch oder Ausreißen von Gewinden	Ja, wenn Dimensionierung, Auswahl der Werkstoffe, Herstellung, Anordnung und Verbindung zur Leitung und/oder zu den Rohr-/Schlaucharmaturen bewährten technischen Erfahrungen entsprechen.	—
Leckage (Verlust der Dichtwirkung)	Nein	Durch Verschleiß, Alterung, Nachlassen der Elastizität usw. ist kein Fehlerausschluss für eine lange Zeitdauer möglich. Ein plötzliches, weitgehendes Versagen der Dichtwirkung wird nicht angenommen.
Zusetzen (Verstopfen)	Ja, bei Anwendungen im Leistungskreis und bei Steuer- und Messverbindungselementen, wenn die Nennweite $\geq$ 2 mm ist.	—

Tabelle B.10 — Fehler und Fehlerausschlüsse — Druckübersetzer und Druckmittelumrichter

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Verlust oder Veränderung der Luft-/Öl-Dichtwirkung der Druckräume	Nein	—
Bersten der Druckräume sowie Bruch von Befestigungs- oder Deckelschrauben	Ja, wenn Dimensionierung, Auswahl der Werkstoffe, Anordnung und Befestigung bewährten technischen Erfahrungen entsprechen	

Tabelle B.11 — Fehler und Fehlerausschlüsse — Filter

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Zusetzen/Verstopfen des Filterelements	Nein	—
Bruch oder teilweiser Bruch des Filterelements	Ja, wenn das Filterelement eine ausreichende Druckfestigkeit hat	
Ausfall der Filterzustands-Anzeigeeinrichtung oder Überwachungseinrichtung	Nein	
Bersten des Filtergehäuses oder Bruch der Deckel- oder Verbindungselemente	Ja, wenn Dimensionierung, Auswahl der Werkstoffe, Anordnung im System und Befestigung bewährten technischen Erfahrungen entsprechen	

Tabelle B.12 — Fehler und Fehlerausschlüsse — Öler

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Veränderung des Einstellwertes (Ölvolumen je Zeiteinheit) ohne Veränderung der Verstelleinrichtung	Nein	—
selbsttätige Veränderung der Verstelleinrichtung	Ja, wenn eine wirksame, an den jeweiligen Einsatzfall angepasste Sicherung der Verstelleinrichtung vorhanden ist.	
unbeabsichtigtes Herausdrehen des Stellteils der Verstelleinrichtung	Ja, wenn eine wirksame formschlüssige Sicherung gegen das Herausdrehen vorhanden ist.	
Bersten des Gehäuses oder Bruch der Deckel-, Befestigungs- oder Verbindungselemente	Ja, wenn Dimensionierung, Auswahl der Werkstoffe, Anordnung im System und Befestigung bewährten technischen Erfahrungen entsprechen.	

Tabelle B.13 — Fehler und Fehlerausschlüsse — Schalldämpfer

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Zusetzen (Verstopfen) des Schalldämpfers	Ja, wenn Konstruktion und Ausführung des Schalldämpferelementes die Bemerkung erfüllen.	Das Verstopfen des Schalldämpferelementes und/oder eine Erhöhung des Staudruckes in der Abluft über einen kritischen Wert hinaus ist unwahrscheinlich, wenn der Schalldämpfer einen entsprechend großen Querschnitt hat und so konstruiert ist, dass er die Betriebsbedingungen erfüllt.

Tabelle B.14 — Fehler und Fehlerausschlüsse — Energiespeicher und Druckbehälter

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Bruch/Bersten des Energiespeichers/ Druckbehälters oder der Verbindungselemente oder Ausreißen der Gewinde von Befestigungsschrauben	Ja, wenn Konstruktion, Auswahl der Ausrüstung, Auswahl der Werkstoffe und Anordnung im System bewährten technischen Erfahrungen entsprechen.	—

Tabelle B.15 — Fehler und Fehlerausschlüsse — Sensoren

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
fehlerhafter Sensor (siehe Bemerkung)	Nein	Sensoren in dieser Tabelle schließen die Signalerfassung, -verarbeitung und -ausgabe besonders für Druck, Volumenstrom, Temperatur usw. ein.
Veränderung der Erfassungs- oder Ausgabeeigenschaften	Nein	—

Tabelle B.16 — Fehler und Fehlerausschlüsse — Informationsverarbeitung — Verknüpfungsglieder

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
fehlerhaftes Verknüpfungsglied (z. B. UND-Glied, ODER-Glied, Speicherglied) durch z. B. Veränderung der Schaltzeiten, Nichtschalten oder unvollständiges Schalten	Für entsprechende Fehlerannahmen und Fehlerausschlüsse siehe Tabellen B.3, B.4 und B.5 und die entsprechenden Bauteile.	—

Tabelle B.17 — Fehler und Fehlerausschlüsse — Informationsverarbeitung — Verzögerungsglieder

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
fehlerhaftes Verzögerungsglied (z. B. pneumatische und pneumatisch/mechanische Zeit- und Zählglieder)	Ja, bei Verzögerungsgliedern ohne bewegte Bauteile, z. B. Festwiderstände, wenn übliche Betriebsbedingungen vorliegen (siehe Bemerkung) und die Druckluft ausreichend aufbereitet und filtriert ist.	Übliche Betriebsbedingungen liegen vor, wenn die vom Hersteller festgelegten Bedingungen befolgt werden.
Veränderung der Erfassungs- oder Ausgabeeigenschaften		
Bersten des Gehäuses oder Bruch der Deckel- oder Befestigungselemente	Ja, wenn Konstruktion, Dimensionierung und Einbau bewährten technischen Erfahrungen entsprechen.	—

Tabelle B.18 — Fehler und Fehlerausschlüsse — Informationsverarbeitung — Umformer

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
fehlerhafter Umformer [siehe Bemerkung 1)]	Ja, bei Umformern ohne bewegte Bauteile, z. B. Reflexdüse, wenn übliche Betriebsbedingungen vorliegen [siehe Bemerkung 2)] und die Druckluft ausreichend aufbereitet und filtriert ist	1) Hier werden z. B. Bauelemente für die Umformung eines pneumatischen Signals in ein elektrisches Signal, für die Erfassung von Positionen (Zylinderschalter, Reflexdüse) und für die Verstärkung pneumatischer Signale betrachtet. 2) Übliche Betriebsbedingungen liegen vor, wenn die vom Hersteller festgelegten Bedingungen befolgt werden.
Veränderung der Erfassungs- oder Ausgabeeigenschaften		
Bersten des Gehäuses oder Bruch der Deckel- oder Befestigungselemente	Ja, wenn Konstruktion, Dimensionierung und Einbau bewährten technischen Erfahrungen entsprechen	—

Anhang C
(informativ)

Validierungswerkzeuge für hydraulische Systeme

Bei Anwendung hydraulischer Systeme in Verbindung mit anderen Technologien sollten auch Anhang C berücksichtigt werden. Wenn hydraulische Bauteile elektrisch angeschlossen/gesteuert werden, sollten die entsprechenden Fehlerlisten im Anhang D berücksichtigt werden.

ANMERKUNG Zusätzliche Anforderungen können in nationalen Rechtsvorschriften enthalten sein.

Die Tabellen C.1 und C.2 enthalten grundlegende und bewährte Sicherheitsprinzipien. Luftblasen und Kavitation in der Hydraulikflüssigkeit sollten vermieden werden, weil sie zusätzliche Gefährdungen verursachen können, z. B. unbeabsichtigte Bewegungen.

Eine Aufzählung bewährter Bauteile ist in diesem Anhang C nicht enthalten. Der Status „bewährt“ ist in erster Linie anwendungsbezogen zu sehen. Bauteile können als „bewährt“ beschrieben werden, falls diese ISO 13849-1:2006, 6.2.2, und ISO 4414:2010, Abschnitte 5 bis 7, entsprechen. Ein für bestimmte Anwendungen bewährtes Bauteil kann für andere Anwendungen ungeeignet sein.

In den Tabellen C.3 bis C.12 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 C.1 — Grundlegende Sicherheitsprinzipien

Grundlegendes Sicherheitsprinzip	Bemerkungen
Anwendung geeigneter Werkstoffe und Herstellungsverfahren	Auswahl der Werkstoffe, der Herstellungs- und Behandlungsverfahren unter Berücksichtigung von z. B. Spannungen, Haltbarkeit, Elastizität, Reibung, Verschleiß, Korrosion, Temperatur, Hydraulikflüssigkeit.
richtige Dimensionierung und Formgebung	Berücksichtigen z. B. von Spannung, Dehnung, Ermüdung, Oberflächenrauheit, Grenzabmaßen, Herstellungsverfahren.
geeignete(r) Auswahl, Kombination, Anordnungen, Zusammenbau und Einbau der Bauteile/des Systems	Anwendung der Anwendungshinweise 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 Energiefreischalten an allen relevanten Einrichtungen 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 Ingangsetzung in ISO 12100:2010, 6.2.11.3. Berücksichtigen von unterschiedlichen Betriebsarten, z. B. Betriebsmodus, Instandhaltungsmodus. Dieses Prinzip darf bei einigen Anwendungen nicht angewendet werden, z. B. wenn durch einen Verlust von hydraulischem Druck eine zusätzliche Gefährdung entsteht.
geeignete Befestigung	Bei der Anwendung z. B. von Schraubensicherungen, Armaturen, Klebungen, Spannringen, Anwendungshinweise des Herstellers beachten. Überbeanspruchung kann durch Anwendung eines geeigneten Drehmomenten-Begrenzungs-Verfahrens vermieden werden.

Tabelle C.1 *(fortgesetzt)*

Grundlegendes Sicherheitsprinzip	Bemerkungen
Druckbegrenzung	Beispiele sind Druckbegrenzungsventile, Druckminder-/ Druckregelventile.
Begrenzung/Verringerung der Geschwindigkeit	Ein Beispiel ist die Geschwindigkeitsbegrenzung eines Kolbens durch ein Stromventil oder eine Drossel.
ausreichende Maßnahmen zur Vermeidung von Verunreinigung des Fluids	Berücksichtigen von Filtration/Abtrennung von Feststoffen/Wasser im Fluid. Eine Anzeige, die auf die Notwendigkeit des Filterwechsels aufmerksam macht, ist ebenfalls in Betracht zu ziehen.
geeigneter Schaltzeitbereich	Berücksichtigung von z. B. der Länge der Rohrleitungen, Druck, Entleerungskapazität, Verringerung der Federkraft, Reibung, Schmierung, Temperatur/Viskosität, Trägheit bei Beschleunigung und Verzögerung, Zusammenwirken von Grenzabmaßen.
Beständigkeit gegen Umgebungsbedingungen	Gestalten der Einrichtung, dass sie in allen für den Einsatz zu erwartenden Umgebungen und bei allen vorhersehbaren ungünstigen Bedingungen z. B. für Temperatur, Feuchte, Schwingungen, Verunreinigungen, arbeiten kann. Siehe Abschnitt 10 und Festlegungen/ Anwendungshinweise des Herstellers beachten.
Schutz gegen unerwarteten Anlauf	Berücksichtigen von unerwartetem Anlauf, verursacht durch gespeicherte Energie und nach Wiederherstellung der Energieversorgung, für unterschiedliche Betriebsarten, z. B. Betriebsmodus, Instandhaltungsmodus. Eine besondere Einrichtung zum Ablassen der gespeicherten Energie kann erforderlich sein. Besondere Anwendungen (z. B. Beibehaltung der Energie für Spanneinrichtungen oder Sicherung einer Stellung) sind gesondert zu betrachten.
Vereinfachung	Vermeiden von unnötigen Bauteilen im sicherheitsbezogenen System
geeigneter Temperaturbereich	Dieser ist überall im gesamten System zu berücksichtigen.
Trennung	Trennung der sicherheitsbezogenen Funktionen von anderen Funktionen.

Tabelle C.2 — Bewährte Sicherheitsprinzipien

Bewährtes Sicherheitsprinzip	Bemerkungen
Überdimensionierung/Sicherheitsfaktor	Der Sicherheitsfaktor ist in Normen angegeben oder geht auf Erfahrungen mit sicherheitsbezogenen Anwendungen zurück.
gesicherte Position	Das bewegliche Element des Bauteils wird mechanisch in einer der möglichen Positionen gehalten (Reibung allein ist nicht ausreichend). Um die Position zu verändern, ist das Aufbringen von Kraft notwendig.
erhöhte AUS-Kraft	Eine Lösung kann sein, dass das Flächenverhältnis für die Bewegung eines Ventilschiebers in die sichere Position (AUS-Stellung) gegenüber dem Flächenverhältnis für die Bewegung des Ventilschiebers in die EIN-Stellung wesentlich größer ist (ein Sicherheitsfaktor).

Tabelle C.2 *(fortgesetzt)*

Bewährtes Sicherheitsprinzip	Bemerkungen
durch den Lastdruck schließendes Ventil	Beispiele sind Ventile in Sitz- und Patronen-Bauart. Es ist zu berücksichtigen, wie der Lastdruck aufzubringen ist, um das Ventil auch dann geschlossen zu halten, wenn z. B. die Schließfeder des Ventils bricht.
mechanisch zwangläufige Wirkung	Die mechanisch zwangläufige Wirkung wird für die beweglichen Teile innerhalb der hydraulischen Bauteile angewendet. Siehe auch Tabelle A.2.
Vervielfachung von Teilen	Siehe Tabelle A.2.
Anwendung bewährter Federn	Siehe Tabelle A.2.
Begrenzung/Verringerung der Geschwindigkeit durch einen Widerstand gegen einen festgelegten Volumenstrom	Beispiele sind Festblende, Festdrossel.
Begrenzung/Verringerung der Kraft	Dies kann erreicht werden durch ein bewährtes Druck-begrenzungsventil, das z. B. mit einer bewährten Feder ausgestattet und korrekt bemessen und ausgewählt ist.
geeigneter Bereich für die Betriebsbedingungen	Die Eingrenzung der Betriebsbedingungen, z. B. der Bereiche für Druck, Volumenstrom und Temperatur, sollte berücksichtigt werden.
Überwachung des Zustands des Fluids	Berücksichtigen einer hoch wirksamen Filtration/Abrennung von Feststoffen/Wasser im Fluid. Zu berücksichtigen sind auch die chemischen/physikalischen Zustände des Fluids. Berücksichtigen einer Anzeige, die auf die Notwendigkeit des Filterwechsels aufmerksam macht.
ausreichend große positive Überdeckung in Kolbenschieberventilen	Die positive Überdeckung sichert die Anhaltefunktion und verhindert unzulässige Bewegungen.
Hysteresebegrenzung	Die Hysterese erhöht sich z. B. durch stärkere Reibung. Ein Zusammenwirken von Grenzabmaßen beeinflusst die Hysterese ebenfalls.

Tabelle C.3 — Fehler und Fehlerausschlüsse — Wegeventile

<table>
<tr><th>Betrachteter Fehler</th><th>Fehlerausschluss</th><th>Bemerkungen</th></tr>
<tr><td>Veränderung der Schaltzeiten</td><td>Ja, bei mechanisch zwangläufiger Betätigung (siehe Tabelle A.2) der bewegten Bauteile, sofern die Betätigungskraft ausreichend groß ist; oder, bezogen auf das Nichtöffnen eines Patronensitzventils besonderer Bauart, wenn es mit mindestens einem weiteren Ventil den Hauptvolumenstrom des Fluids steuert [siehe Bemerkung 1)].</td><td rowspan="2">1) Ein Patronensitzventil besonderer Bauart liegt vor, wenn:
— die aktive Fläche zum Auslösen der sicherheitsbezogenen Schaltbewegung mindestens 90 % der Gesamtfläche des bewegten Bauteils (Ventilsitz) beträgt,
— der wirksame Steuerdruck auf die aktive Fläche, hervorgerufen durch das Verhalten des betrachteten Sitzventils, bis zum maximalen Betriebsdruck (nach ISO 5598:2008, 3.2.429) ansteigen kann,
— der wirksame Steuerdruck auf die der aktiven Fläche gegenüberliegende Fläche des bewegten Bauteils auf einen im Vergleich zum maximalen Betriebsdruck sehr niedrigen Wert verringert wird, z. B. Rücklaufdruck bei abschaltbaren Druckventilen oder Speisedruck bei Saug-/Füllventilen,
— das bewegte Bauteil (Ventilsitz) mit Entlastungsnuten am Umfang versehen ist, und
— das (die) Vorsteuerventil(e) für dieses Sitzventil gemeinsam mit diesem Sitzventil in Blockbauweise (d. h. ohne Schlauchleitungen und Rohre zur Verbindung dieser Ventile) angeordnet ist (sind).</td></tr>
<tr><td>Nichtschalten (Hängenbleiben in einer End- oder Nulllage) oder nicht vollständiges Schalten (Hängenbleiben in einer beliebigen Zwischenstellung)</td><td>Ja, bei mechanisch zwangläufiger Betätigung (siehe Tabelle A.2) der bewegten Bauteile, sofern die Betätigungskraft ausreichend groß ist; oder, bezogen auf das Nichtöffnen eines Patronensitzventils besonderer Bauart, wenn es mit mindestens einem weiteren Ventil den Hauptvolumenstrom des Fluids steuert [siehe Bemerkung 1)].</td></tr>
<tr><td>Selbsttätige Veränderung der Ausgangs-Schaltstellung (ohne Eingangssignal)</td><td>Ja, bei mechanisch zwangläufiger Betätigung (siehe Tabelle A.2) der bewegten Bauteile, sofern die Haltekraft ausreichend groß ist; oder
ja, wenn bewährte Federn verwendet werden (siehe Tabelle A.2) und wenn übliche Einbau- und Betriebsbedingungen vorliegen [siehe Bemerkung 2)] oder, bezogen auf das Nichtöffnen eines Patronensitzventils besonderer Bauart, wenn es mit mindestens einem weiteren Ventil den Hauptvolumenstrom des Fluids steuert [siehe Bemerkung 1)] und wenn übliche Einbau- und Betriebsbedingungen vorliegen [siehe Bemerkung 2)].</td><td>2) Übliche Einbau- und Betriebsbedingungen liegen vor, wenn
— die vom Hersteller vorgegebenen Bedingungen befolgt werden,
— sich die Gewichtskraft des bewegten Bauteils sicherheitstechnisch nicht ungünstig auswirkt (z. B. waagerechter Einbau),
— keine besonderen Massenträgheitskräfte die bewegten Bauteile beeinträchtigen (z. B. Bewegungsrichtung berücksichtigt die Orientierung der beweglichen Maschinenteile, und
— keine extremen Schwingungs- und Schockbeanspruchungen auftreten</td></tr>
<tr><td>Leckage</td><td>Ja, bei Sitzventilen, wenn übliche Einbau- und Betriebsbedingungen vorliegen (siehe Bemerkung) und ein angemessenes Filtrationssystem vorhanden ist.</td><td>Übliche Einbau- und Betriebsbedingungen liegen vor, wenn die vom Hersteller vorgegebenen Bedingungen befolgt werden</td></tr>
<tr><td colspan="3">ANMERKUNG Werden die Steuerfunktionen durch individuelle Einzelfunktionen mehrerer Ventile realisiert, sollte eine Fehlerbetrachtung für jedes Ventil durchgeführt werden. Bei vorgesteuerten Ventilen sollte ebenso vorgegangen werden.</td></tr>
</table>

Tabelle C.3 *(fortgesetzt)*

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Veränderung des Leckagevolumenstroms nach einer langen Einsatzdauer	Nein	—
Bersten des Ventilgehäuses oder Bruch des/der bewegten Bauteils/Bauteile sowie Bruch der Befestigungs- oder Gehäuseschrauben	Ja, wenn Konstruktion, Dimensionierung und Einbau bewährten technischen Erfahrungen entsprechen.	
für Servo- und Proportionalventile: Hydraulische Fehler, die unkontrolliertes Verhalten bewirken	Ja, bei Servo- und Proportionalwegeventilen, wenn sie bedingt durch ihre konstruktive Ausführung sicherheitstechnisch wie konventionelle Wegeventile beurteilt werden können.	
ANMERKUNG Werden die Steuerfunktionen durch individuelle Einzelfunktionen mehrerer Ventile realisiert, sollte eine Fehlerbetrachtung für jedes Ventil durchgeführt werden. Bei vorgesteuerten Ventilen sollte ebenso vorgegangen werden.		

Tabelle C.4 — Fehler und Fehlerausschlüsse — Absperr-(Abschalt)-ventile, Rückschlagventile, Wechselventile usw.

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Veränderung der Schaltzeiten	Nein	—
Nichtöffnen, nicht vollständiges Öffnen, Nichtschließen oder nicht vollständiges Schließen (Hängenbleiben in einer Endlage oder in einer beliebigen Zwischenstellung)	Ja, wenn das Führungssystem für das/die bewegte(n) Bauteil(e) etwa denen eines nicht gesteuerten Kugelsitzventils ohne ein Dämpfungssystem entsprechen (siehe Bemerkung) und wenn bewährte Federn angewendet werden (siehe Tabelle A.2).	Für ein nicht gesteuertes Kugelsitzventil ohne Dämpfungssystem ist das Führungssystem im Allgemeinen so gestaltet, dass ein Hängenbleiben des bewegten Bauteils unwahrscheinlich ist.
selbsttätige Veränderung der Ausgangs-Schaltstellung (ohne Eingangssignal)	Ja, wenn übliche Einbau- und Betriebsbedingungen vorliegen (siehe Bemerkung) und eine ausreichende Schließkraft aufgrund der vorliegenden Drücke und Flächen vorhanden ist.	Übliche Einbau- und Betriebsbedingungen werden eingehalten, wenn: — die vom Hersteller festgelegten Bedingungen befolgt werden, und — keine besonderen Massenträgheitskräfte die bewegten Bauteile beeinträchtigen, z. B. Bewegungsrichtung berücksichtigt die Orientierung der beweglichen Maschinenteile, und — keine extremen Schwingungs- und Schockbeanspruchungen auftreten.
für Wechselventile: gleichzeitiger Verschluss beider Eingangsanschlüsse	Ja, wenn bedingt durch Konstruktion und Ausführung des bewegten Bauteils dieser gleichzeitige Verschluss unwahrscheinlich ist.	—
Leckage	Ja, wenn übliche Betriebsbedingungen vorliegen (siehe Bemerkung) und ein angemessenes Filtrationssystem vorhanden ist.	Übliche Betriebsbedingungen liegen vor, wenn die vom Hersteller vorgegebenen Bedingungen befolgt werden.

Tabelle C.4 *(fortgesetzt)*

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Veränderung des Leckagevolumenstroms über eine lange Einsatzdauer	Nein	—
Bersten des Ventilgehäuses oder Bruch des/der bewegten Bauteils/Bauteile sowie Bruch der Befestigungs- oder Gehäuseschrauben	Ja, wenn Konstruktion, Dimensionierung und Einbau bewährten technischen Erfahrungen entsprechen.	

Tabelle C.5 — Fehler und Fehlerausschlüsse — Stromventile

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Veränderung des Volumenstroms ohne Veränderung der Verstelleinrichtung	Ja, bei Stromventilen ohne bewegte Bauteile [siehe Bemerkung 1)], z. B. Drosselventile, wenn übliche Betriebsbedingungen vorliegen [siehe Bemerkung 2)] und ein ausreichendes Filtrationssystem vorhanden ist [siehe Bemerkung 3)].	1) Die Verstelleinrichtung wird nicht als bewegtes Bauteil betrachtet. Veränderungen des Volumenstroms durch Änderung der Druckdifferenz und der Viskosität sind bei diesem Ventiltyp physikalisch begrenzt und nicht Gegenstand dieser Fehlerannahme. 2) Übliche Betriebsbedingungen liegen vor, wenn die vom Hersteller festgelegten Bedingungen befolgt werden. 3) Wenn ein Rückschlagventil in das Stromventil eingebaut ist, sind dafür zusätzlich die Fehlerannahmen für Rückschlagventile zu beachten.
Veränderung des Volumenstroms bei nicht einstellbaren kreisförmigen Blenden und Düsen	Ja, bei einem Durchmesser > 0,8 mm, wenn übliche Betriebsbedingungen vorliegen [siehe Bemerkung 2)] und wenn ein ausreichendes Filtrationssystem vorhanden ist.	
bei Proportionalstromventilen: Veränderung des Volumenstroms durch unbeabsichtigte Veränderung des Einstellwertes	Nein	—
selbsttätige Veränderung der Verstelleinrichtung	Ja, bei einer wirksamen und dem jeweiligen Einsatzfall angepassten Sicherung der Verstelleinrichtung unter Beachtung sicherheitstechnischer Festlegungen	
unbeabsichtigtes Lösen (Herausdrehen) des Stellteils/der Stellteile der Verstelleinrichtung	Ja, wenn eine wirksame formschlüssige Sicherung gegen das Lösen (Herausdrehen) vorhanden ist	
Bersten des Ventilgehäuses oder Bruch des/der bewegten Bauteils/Bauteile sowie Bruch der Befestigungs- oder Gehäuseschrauben	Ja, wenn Konstruktion, Dimensionierung und Einbau bewährten technischen Erfahrungen entsprechen	

Tabelle C.6 — Fehler und Fehlerausschlüsse — Druckventile

<table>
<tr><th>Betrachteter Fehler</th><th>Fehlerausschluss</th><th>Bemerkungen</th></tr>
<tr><td>Nichtöffnen oder nicht ausreichendes Öffnen (weg- und zeitmäßig) bei Überschreiten des Einstelldruckes (Hängenbleiben oder Schwergängigkeit des bewegten Bauteils) [siehe Bemerkung 1)]</td><td rowspan="2">Ja, bezogen auf das Nichtöffnen eines Patronensitzventils besonderer Bauart, wenn es mit mindestens einem weiteren Ventil den Hauptvolumenstrom des Fluids steuert [siehe Bemerkung 1)] in Tabelle C.3); oder wenn das Führungssystem für das/die bewegte(n) Bauteil(e) etwa denen eines nicht gesteuerten Kugelsitzventils ohne Dämpfungssystem entsprechen [siehe Bemerkung 2)] und wenn bewährte Federn eingebaut sind (siehe Tabelle A.2).</td><td rowspan="2">1) Diese Fehlerannahme gilt nur, wenn das/die Druckventil(e) insbesondere angewendet wird (werden) für Kraftwirkungen, z. B. zum Spannen, und für das Steuern von gefahrbringenden Bewegungen, z. B. zum Hochhalten von Lasten. Diese Fehlerannahme gilt nicht für die übliche Funktion eines Druckventils in Hydrauliksystemen, z. B. Druckbegrenzung, Druckminderung.
2) Für ein nicht gesteuertes Kugelsitzventil ohne Dämpfungssystem ist das Führungssystem im Allgemeinen so gestaltet, dass ein Hängenbleiben des bewegten Bauteils unwahrscheinlich ist.</td></tr>
<tr><td>Nichtschließen oder nicht vollständiges Schließen (weg- und zeitmäßig) bei Unterschreiten des Einstelldruckes (Hängenbleiben oder Schwergängigkeit des bewegten Bauteils) [siehe Bemerkung 1)]</td></tr>
<tr><td>Veränderung des Druck-Regelverhaltens ohne Veränderung der Verstelleinrichtung [siehe Bemerkung 1)]</td><td>Ja, bei direkt betätigten Druckentlastungsventilen, wenn (eine) bewährte Feder(n) eingebaut ist (sind) (siehe Tabelle A.2).</td><td rowspan="2"></td></tr>
<tr><td>für Proportional-Druckventile: Veränderung des Druck-Regelverhaltens durch unbeabsichtigte Veränderung des Einstellwertes [siehe Bemerkung 1)]</td><td>Nein</td></tr>
<tr><td>selbsttätige Veränderung der Verstelleinrichtung</td><td>Ja, bei einer wirksamen und dem Einsatzfall angepassten Sicherung der Verstelleinrichtung unter Beachtung sicherheitstechnischer Festlegungen (z. B. Plombierung).</td><td rowspan="2">—</td></tr>
<tr><td>unbeabsichtigtes Herausdrehen des Stellteils der Verstelleinrichtung</td><td>Ja, wenn eine wirksame formschlüssige Sicherung gegen das Herausdrehen vorhanden ist.</td></tr>
<tr><td>Leckage</td><td>Ja, für Sitzventile, wenn übliche Betriebsbedingungen vorliegen (siehe Bemerkung) und wenn ein ausreichendes Filtrationssystem vorhanden ist.</td><td>Übliche Betriebsbedingungen liegen vor, wenn die vom Hersteller festgelegten Bedingungen befolgt werden</td></tr>
<tr><td>Veränderung des Leckage-Volumenstroms über eine lange Einsatzdauer</td><td>Nein</td><td rowspan="2">—</td></tr>
<tr><td>Bersten des Ventilgehäuses oder Bruch des/der bewegten Bauteils/Bauteile sowie Bruch der Befestigungs- oder Gehäuseschrauben</td><td>Ja, wenn Konstruktion, Dimensionierung und Einbau bewährten technischen Erfahrungen entsprechen.</td></tr>
</table>

Tabelle C.7 — Fehler und Fehlerausschlüsse — Rohrleitungen aus Metall

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Bersten und Leckage	Ja, wenn Dimensionierung, Auswahl der Werkstoffe und Befestigung bewährten technischen Erfahrungen entsprechen.	—
Fehler am Verbindungselement (z. B. Abreißen/Ausreißen, Leckage)	Ja, bei Verwendung von Anschweißverschraubungen, Anschweißflanschen oder Bördelverschraubungen, wenn Dimensionierung, Auswahl der Werkstoffe, Herstellung, Anordnung und Befestigung bewährten technischen Erfahrungen entsprechen.	—
Zusetzen (Verstopfen)	Ja, bei Rohrleitungen im Leistungskreis und bei Steuer- und Messrohrleitungen, wenn die Nennweite ≥ 3 mm ist.	

Tabelle C.8 — Fehler und Fehlerausschlüsse — Schlauchleitungen

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Bersten, Ausreißen aus/Abreißen an der Einbindung und Leckage	Nein	—
Zusetzen (Verstopfen)	Ja, bei Schlauchleitungen im Leistungskreis und bei Steuer- und Messschlauchleitungen, wenn die Nennweite ≥ 3 mm ist.	

Tabelle C.9 — Fehler und Fehlerausschlüsse — Verbindungselemente

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Bersten, Schraubenbruch oder Ausreißen von Gewinden	Ja, wenn Dimensionierung, Auswahl der Werkstoffe, Herstellung, Anordnung und Verbindung zur Leitung und/oder zum fluidtechnischen Bauteil bewährten technischen Erfahrungen entsprechen.	—
Leckage (Verlust der Dichtwirkung)	Nein (siehe Bemerkung)	Durch Verschleiß, Alterung, Nachlassen der Elastizität usw. ist kein Fehlerausschluss für eine lange Zeitdauer möglich. Ein plötzliches, weitgehendes Versagen der Dichtwirkung wird nicht angenommen.
Zusetzen (Verstopfen)	Ja, bei Anwendungen im Leistungskreis und bei Steuer- und Messverbindungselementen, wenn die Nennweite ≥ 3 mm ist.	—

Tabelle C.10 — Fehler und Fehlerausschlüsse — Filter

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Zusetzen/Verstopfen des Filterelements	Nein	—
Bruch des Filterelements	Ja, wenn das Filterelement eine ausreichende Druckfestigkeit hat und ein wirksames Bypassventil oder eine wirksame Verschmutzungs-Überwachung vorhanden ist.	
Ausfall des Bypassventils	Ja, wenn das Führungssystem des Bypassventils etwa dem eines nicht gesteuerten Kugelsitzventils ohne ein Dämpfungssystem entspricht (siehe Tabelle C.4) und wenn bewährte Federn angewendet werden (siehe Tabelle A.2).	
Ausfall der Verschmutzungs-Anzeigeeinrichtung oder -Überwachungseinrichtung	Nein	
Bersten des Filtergehäuses oder Bruch der Deckel- oder Verbindungselemente	Ja, wenn Dimensionierung, Auswahl der Werkstoffe, Anordnung im System und Befestigung bewährten technischen Erfahrungen entsprechen.	

Tabelle C.11 — Fehler und Fehlerausschlüsse — Energiespeicher

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Bruch/Bersten des Energiespeicher-Behälters oder der Verbindungselemente oder der Deckelschrauben sowie Ausreißen der Schraubengewinde	Ja, wenn Konstruktion, Auswahl der Ausrüstung, Auswahl der Werkstoffe und Anordnung im System bewährten technischen Erfahrungen entsprechen.	—
Leckage am Trennglied zwischen Gas und Druckflüssigkeit	Nein	
Ausfall/Bruch des Trennglieds zwischen Gas und Druckflüssigkeit	Ja, bei Zylinder-/Kolbenspeichern (siehe Bemerkung).	Eine plötzlich auftretende größere Leckage wird nicht angenommen.
Ausfalls des Füllventils auf der Gasseite	Ja, wenn das Füllventil nach bewährten technischen Erfahrungen eingebaut ist und wenn ein ausreichender Schutz gegen äußere Einflüsse vorhanden ist.	—

Tabelle C.12 — Fehler und Fehlerausschlüsse — Sensoren

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
fehlerhafter Sensor (siehe Bemerkung)	Nein	Sensoren in dieser Tabelle schließen die Signalerfassung, -verarbeitung und -ausgabe ein, insbesondere für Druck, Volumenstrom, Temperatur usw.
Veränderung der Erfassungs- oder Ausgabeeigenschaften	Nein	—

Anhang D
(informativ)

Validierungswerkzeuge für elektrische Systeme

D.1 Allgemeines

Bei Anwendung elektrischer Systeme in Verbindung mit anderen Technologien sollte auch Anhang D berücksichtigt werden.

Die Umgebungsbedingungen der IEC 60204-1 sind auf den Validierungsprozess anwendbar. Wenn andere Umgebungsbedingungen festgelegt sind, sollten auch sie berücksichtigt werden.

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

Die in Tabelle D.3 aufgeführten Bauteile gelten als bewährt, wenn sie der in ISO 13849-1:2006, 6.2.4, angegebenen Beschreibung entsprechen. Die in Tabelle D.3 aufgeführten Normen können über Eignung und Zuverlässigkeit der Bauteile für eine bestimmte Anwendung Auskunft geben. Ein für bestimmte Anwendungen bewährtes Bauteil kann für andere Anwendungen ungeeignet sein.

ANMERKUNG Komplexe elektronische Bauteile (z. B. PLCs, Mikroprozessoren, anwendungsspezifisch integrierter Schaltkreis) können nicht als bewährt angesehen werden.

In Abschnitt D.2 sowie in den Tabellen D.4 bis D.18 werden Fehlerausschlüsse und die zugehörigen Begründungen angegeben. Für weitere Ausschlüsse siehe 4.4.

Bei der Validierung sollten sowohl dauernd auftretende Fehler als auch kurzzeitige Störungen berücksichtigt werden.

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

Tabelle D.1 — Grundlegende Sicherheitsprinzipien

Grundlegendes Sicherheitsprinzip	Bemerkungen
Anwendung geeigneter Werkstoffe und Herstellungsverfahren	Auswahl des Werkstoffs, der Herstellungs- und Behandlungsverfahren unter Berücksichtigung von z. B. Spannung, Haltbarkeit, Elastizität, Reibung, Verschleiß, Korrosion, Temperatur, Leitfähigkeit, mechanischer Festigkeit der Isolierstoffe.
richtige Dimensionierung und Formgebung	Berücksichtigen z. B. von Spannung, Dehnung, Ermüdung, Oberflächenrauheit, Grenzabmaßen, Herstellungsverfahren.
Geeignete(r) 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.
richtige Schutzleiterverbindung	Eine Seite des Steuerstromkreises, eine Klemme jedes elektromagnetisch betätigten Geräts oder eine Klemme anderer elektrischer Geräte ist mit einem Schutzleiter verbunden (siehe IEC 60204-1:2005, 9.4.3.1).
Isolationsüberwachung	Eine Einrichtung zur Isolationsüberwachung ist anzuwenden, die einen Erdschluss entweder anzeigt oder den Stromkreis nach einem Erdschluss selbsttätig unterbricht (siehe IEC 60204-1:2005, 6.3.3.)

Tabelle D.1 *(fortgesetzt)*

Grundlegendes Sicherheitsprinzip	Bemerkungen
Anwendung des Prinzips der Energietrennung	Ein sicherer Zustand wird erreicht, indem alle wichtigen Einrichtungen von der Energiequelle abgetrennt werden, z. B. durch Anwendung eines üblicherweise geschlossenen Kontakts (NC) für Eingänge (Tast- und Positionsschalter) und eines üblicherweise geöffneten Kontakts (NO) für Relais (siehe auch ISO 12100:2010, 6.2.11.3). In einigen Fällen können Ausnahmen möglich sein, z. B. dann, wenn der Ausfall der Versorgung mit Elektroenergie eine zusätzliche Gefährdung darstellt. Zeitverzögernde Funktionen können erforderlich sein, um einen sicheren Zustand des Systems zu erreichen (siehe IEC 60204-1:2005, 9.2.2).
Unterdrückung von Spannungsspitzen	Eine Einrichtung zur Unterdrückung der Spannungsspitzen (RC-Glied, Diode, Varistor) ist parallel zur aufgebrachten Last, jedoch nicht parallel zu den Kontakten, anzuwenden. ANMERKUNG Durch eine Diode wird die Ausschaltzeit erhöht.
Verringerung der Ansprechzeit	Minimierung der Verzögerung beim Ausschalten der zum Schalten verwendeten Bauteile.
Verträglichkeit	Anwendung von Bauteilen, die für die angewendeten Spannungen und Ströme geeignet sind.
Beständigkeit gegen Umgebungsbeanspruchungen	Gestalten der Einrichtungen, dass sie in allen für den Einsatz erwarteten Umgebungen und unter ungünstigen Bedingungen, z. B. Temperatur, Feuchte, Vibration und elektromagnetische Störung (EMI), arbeiten können (siehe Abschnitt 10).
sichere Befestigung der Eingabegeräte	Die Eingabegeräte sind so zu sichern, z. B. durch Verriegelungsschalter, Positionsschalter, Grenzlagenschalter, Näherungsschalter, dass Stellung, Ausrichtung und Schalttoleranzen unter allen erwarteten Bedingungen, z. B. Vibration, üblicher Verschleiß, Eindringen von Fremdkörpern, Temperatur, eingehalten werden. Siehe ISO 14119:1998, Abschnitt 5.
Schutz gegen unerwarteten Anlauf	Vermeiden von unerwartetem Anlauf, z. B. nach Wiederherstellung der Energieversorgung (siehe ISO 12100:2010, 6.2.11.4, ISO 14118, IEC 60204-1).
Schutz des Steuerstromkreises	Der Steuerstromkreis sollte nach IEC 60204-1:2005, 7.2 und 9.1.1, geschützt werden.
aufeinander folgendes Schalten bei Stromkreisen mit Reihenanschlüssen redundanter Signale	Zum Vermeiden des Fehlers gemeinsamer Ursache beim Verschweißen beider Kontakte findet das gleichzeitige Ein- und Ausschalten nicht statt, so dass ein Kontakt immer ohne Strom schaltet.

Tabelle D.2 — Bewährte Sicherheitsprinzipien

Bewährtes Sicherheitsprinzip	Bemerkungen
mechanisch zwangläufig verbundene Kontakte	Anwendung mechanisch zwangläufig verbundener Kontakte, z. B. für Überwachungsfunktion in Systemen der Kategorie 2, 3 und 4 (siehe EN 50205, IEC 60947-4-1:2001, Anhang F, IEC 60947-5-1:2003 + A1:2009, Anhang L).
Fehlervermeidung in Kabeln	Um Kurzschlüsse zwischen zwei benachbarten Leitungen zu vermeiden, entweder — an jeder einzelnen Leitung Kabel verwenden, deren Abschirmung mit dem Schutzleitersystem verbunden ist, oder — in Flachkabeln, Anwendung eines Schutzleiters zwischen allen Signalleitungen.
Abstände zwischen elektrischen Leitern	Anwenden eines ausreichenden Abstands zwischen Anschlussklemmen, Bauteilen und Leitungen, so dass unbeabsichtigte Verbindungen vermieden werden.
Energiebegrenzung	Zur Zuführung einer begrenzten Energiemenge ist ein Kondensator anzuwenden, z. B. bei Anwendung einer Zeittaktsteuerung.
Begrenzung elektrischer Parameter	Begrenzung von Spannung, Strom, Energie oder Frequenz, um die Bewegung einzuschränken, z. B. durch Drehmomentbegrenzung, versetztes/zeitlich begrenztes Laufenlassen und verringerte Geschwindigkeit, zum Vermeiden eines unsicheren Zustands
Vermeidung undefinierter Zustände	Undefinierte Zustände im Steuersystem sind zu vermeiden. Das Steuersystem ist konstruktiv so zu gestalten, dass während des üblichen Betriebs und unter allen erwarteten Betriebsbedingungen der Zustand des Steuersystems, z. B. Ausgang/Ausgänge, vorherbestimmt werden kann.
Zwangläufiger Betätigungsmodus	Eine direkte Betätigung wird durch Formschluss (nicht durch Kraftschluss) ohne elastische Elemente übertragen, d. h. keine Anwendung von Federn zwischen Stellglied und Kontakten (siehe ISO 14119:1998, 5.1, ISO 12100:2010, 6.2.5).
Zustandsausrichtung bei Ausfällen	Nach Möglichkeit sollten alle Einrichtungen/Schaltungen bei Ausfall in einen sicheren Zustand übergehen oder zu sicheren Bedingungen.
gerichteter Ausfall	Wenn durchführbar, sollten Bauteile oder Systeme angewendet werden, bei denen die Ausfallart im Voraus bekannt ist (siehe ISO 12100:2010, 6.2.12.3).
Überdimensionierung	Bauteile, die in Schutzschaltkreisen angewendet werden, müssen unterlastet werden, z. B. durch — den Strom, der durch die Schaltkontakte geleitet wird, und der weniger als die Hälfte des Strom-Nennwertes betragen sollte, — die Schaltfrequenz der Bauteile, die weniger als die Hälfte des Schaltfrequenz-Nennwertes betragen sollte, und — die Gesamtanzahl der erwarteten Schaltungen, die höchstens 10 % der Anzahl der Schaltungen, für die diese elektrische Einrichtung ausgelegt ist, betragen sollte. ANMERKUNG Unterbelastung kann von der sinnvollen Gestaltung abhängen.
Verringerung von Fehlermöglichkeiten	Trennung sicherheitsbezogener von anderen Funktionen

Tabelle D.2 *(fortgesetzt)*

Bewährte Sicherheitsprinzipien	Bemerkungen
Gleichgewicht zwischen Komplexität/ Vereinfachung	Ein Ausgleich sollte hergestellt werden zwischen: — der Komplexität der Einrichtungen, um eine bessere Steuerung zu erreichen und — der Vereinfachung der Einrichtungen, um ihre Zuverlässigkeit zu verbessern

Tabelle D.3 — Bewährte Bauteile

Bewährtes Bauteile	Zusätzliche Bedingungen für „bewährt“	Norm oder Festlegung
Schalter mit zwangläufiger Betätigung (direktöffnend), z. B.: — Tastschalter; — Positionsschalter; — nockenbetätigte Wahlschalter, z. B. zur Auswahl der Betriebsart	—	IEC 60947-5-1:2003, Anhang K
Not-Aus-Einrichtung	—	ISO 13850 IEC 60947-5-5
Sicherung	—	IEC 60269-1
Leistungsschalter	—	IEC 60947-2
Lastschalter, Trennschalter	—	IEC 60947-3
Fehlerstromschutzeinrichtung/RCD (Residual current device)	—	IEC 60947-2:2006, Anhang B
Hauptschütz	Nur bewährt, wenn a) andere Einflüsse berücksichtigt sind, z. B. Schwingung, und b) Ausfall durch geeignete Verfahren vermieden ist, z. B. Überdimensionierung (siehe Tabelle D.2), und c) der Strom zur Last durch eine thermische Schutzeinrichtung begrenzt ist, und d) die Schaltungen mit einer Sicherung gegen Überlastungen geschützt werden. ANMERKUNG Fehlerausschluss ist nicht möglich.	IEC 60947-4-1
Betätigungs- und Schutzschalteinrichtung oder -gerät (Control and protective switching device (CPS))	—	IEC 60947-6-2

Tabelle D.3 *(fortgesetzt)*

Bewährtes Bauteil	Zusätzliche Bedingungen für „bewährt“	Norm oder Festlegung
Hilfsschütz (z. B. Relais)	Nur bewährt, wenn a) andere Einflüsse berücksichtigt sind, z. B. Schwingung, und b) zwangsläufig unter Spannung stehende Funktion vorliegt, und c) Ausfall durch geeignete Verfahren vermieden ist, z. B. Überdimensionierung (siehe Tabelle D.2), und d) der Strom in den Kontakten durch Sicherungen oder Schutzschalter begrenzt ist, um ein Verschweißen der Kontakte zu vermeiden, und e) Kontakte mechanisch zwangsgeführt sind, wenn sie für Überwachungen angewendet werden. ANMERKUNG Fehlerausschluss ist nicht möglich.	EN 50205 IEC 60947-5-1 IEC 60947-4-1:2001, Anhang F
Relais	Nur bewährt, wenn: a) andere Einflüsse berücksichtigt sind, z. B. Schwingung, und b) zwangsläufig unter Spannung stehende Funktion vorliegt, und c) Ausfall durch geeignete Verfahren vermieden ist, z. B. Überdimensionierung (siehe Tabelle D.2), und d) der Strom in den Kontakten durch Sicherungen oder Schutzschalter begrenzt ist, um ein Verschweißen der Kontakte zu vermeiden. ANMERKUNG Fehlerausschluss ist nicht möglich.	IEC 61810-1 IEC 61810-2
Transformator	—	IEC 61558
Kabel	Die Verkabelung außerhalb umschlossener Einbauräume sollte gegen mechanische Beschädigung (einschließlich z. B. Schwingung oder Biegung) geschützt werden.	IEC 60204-1:2005, Abschnitt 12
Stecker und Steckdose	—	Nach einer elektrischen Norm, die für die vorgesehene Anwendung zutrifft. Zu Verriegelung siehe auch ISO 14119.
Temperaturschalter	—	elektrisch siehe EN 60730-1
Druckschalter	—	elektrisch siehe IEC 60947-5-1 Druck siehe Anhänge B und C
elektromagnetisches Ventil	—	—

D.2 Fehlerausschluss

D.2.1 Allgemeines

Ein Fehlerausschluss ist nur dann gültig, wenn die Bestandteile innerhalb ihrer festgelegten Nennwerte betätigt werden.

D.2.2 „Zinn-Whiskers“

Wenn bleifreie Verfahren und Produkte angewendet und verwendet werden, können elektrische Kurzschlüsse durch die Bildung von *Zinn-Whiskern* vorkommen. Diese Möglichkeit sollte beurteilt und berücksichtigt werden, wenn der Fehlerausschluss „Kurzschluss ...“ eines beliebigen Bauteils angewendet wird. Wird zum Beispiel das Risiko der Zinn-Whisker-Bildung als hoch eingeschätzt, ist der Fehlerausschluss „Kurzschluss eines Widerstands“ nutzlos, da ein Kurzschluss zwischen den Kontakten dieses Bauteils betrachtet werden muss.

ANMERKUNG 1 Die Bildung von Zinn-Whiskern ist eine Erscheinung, die hauptsächlich bei Oberflächen mit reiner, glänzender Zinnbeschichtung auftritt. Die nadelähnlichen Überstände können eine Länge bis zu 100 µm erreichen und elektrische Kurzschlüsse verursachen. Die vorherrschende Theorie lautet, dass Whiskers durch Druckbelastung verursacht werden, die sich beim Verzinnen aufbaut.

ANMERKUNG 2 Die Literaturhinweise [34] und [35] können zur Beurteilung des Phänomens hilfreich sein.

ANMERKUNG 3 Whiskers an Leiterplatten wurden noch nicht festgestellt. Die Leiterbahnen bestehen üblicherweise aus Kupfer ohne Zinnbeschichtung. Kontaktstellen können mit Zinnlegierung beschichtet sein, doch scheint das Produktionsverfahren die Anfälligkeit für die Whisker-Bildung nicht zu fördern.

D.2.3 Kurzschlüsse an PCB-montierten Teilen

Kurzschlüsse an Teilen, die auf einer Leiterplatte (en: **P**rinted **C**ircuit **B**oard) montiert sind, können nur dann ausgeschlossen werden, wenn der Fehlerausschluss „Kurzschluss zwischen zwei benachbarten Leiterbahnen/Kontaktstellen“ wie in Tabelle D.5 durchgeführt wurde.

D.2.4 Fehlerausschlüsse und integrierte Schaltkreise

Da es nicht möglich ist, Fehler auszuschließen, die eine Fehlfunktion eines integrierten Schaltkreises verursachen können (siehe Tabellen D.20 und D.21), kann ein einziger Fehler zum Verlust einer Sicherheitsfunktion (einschließlich ihrer Überprüfung/Prüfung), die in einem einzelnen integrierten Schaltkreis umgesetzt wird, führen. Folglich ist es sehr unwahrscheinlich, dass die für die Anforderungen an die Fehlertoleranz und/oder Fehlererkennung der Kategorie 2, 3 oder 4 erforderliche Mehrkanalfunktionalität bei Anwendung eines einzelnen integrierten Schaltkreises erreicht werden kann, es sei denn die besonderen Architekturanforderungen an integrierte Schaltkreise nach IEC 61508-2:2010, Anhang E, werden erfüllt.

Tabelle D.4 — Fehler und Fehlerausschlüsse — Leitungen/Kabel

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Kurzschluss zwischen zwei beliebigen Leitern	Kurzschlüsse zwischen Leitern, — die dauerhaft (fest) verlegt und gegen äußere Beschädigung geschützt sind, z. B. durch Kabelkanal, Panzerrohr, oder — in unterschiedlichen Mantelleitungen, oder — innerhalb eines elektrischen Einbauraumes (siehe Bemerkung), oder — die einzeln durch eine Erdverbindung geschützt sind.	Voraussetzung ist, dass sowohl die Leitungen als auch der Einbauraum den jeweiligen Anforderungen entsprechen (siehe IEC 60204-1).
Kurzschluss zwischen einem beliebigen Leiter und einem ungeschützten leitenden Teil oder der Erde oder einer Schutzleiterverbindung	Kurzschlüsse zwischen Leiter und jedem ungeschützten leitenden Teil innerhalb eines Einbauraumes (siehe Bemerkung).	
Unterbrechung eines Leiters	Nein	—

Tabelle D.5 — Fehler und Fehlerausschlüsse — Leiterplatten/bestückte Leiterplatten

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Kurzschluss zwischen benachbarten Leiterbahnen/Kontaktstellen	Kurzschlüsse zwischen benachbarten Leitern, wenn die Bemerkungen zutreffen.	Als Basismaterial wird mindestens EP GC nach IEC 60893-1 verwendet. Die Luft- und Kriechstrecken werden mindestens nach IEC 60664-5 (für Strecken von mehr als 2 mm IEC 60664-1) bemessen mit Verschmutzungsgrad 2/ Überspannungskategorie III; wenn beide Leiterbahnen über ein SELV/PELV-Netzgerät versorgt werden, gilt Verschmutzungsgrad 2/Überspannungskategorie II mit einer Mindeststrecke von 0,1 mm. Die montierte Platte ist in eine Einfassung eingebaut, die vor leitfähiger Verschmutzung schützt, z. B. eine Einfassung mit einem Schutzgrad von mindestens IP 54, und die gedruckte(n) Seite(n) der bestückten Platte wird/werden mit einer alterungsbeständigen Lack- oder Schutzschicht so versehen, dass alle Leiterbahnen abgedeckt sind. ANMERKUNG 1 Erfahrungen haben gezeigt, dass Lötmasken als Schutzschicht ausreichen. ANMERKUNG 2 Eine weitere Schutzschicht, die nach IEC 60664-3 abdeckt, kann die Kriech- und Luftstrecken verringern.
Unterbrechung in allen Leiterbahnen	Nein	—

Tabelle D.6 — Fehler und Fehlerausschlüsse — Klemmstellen

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Kurzschluss zwischen benachbarten Klemmen	Kurzschluss zwischen benachbarten Klemmen, wenn die Bemerkungen 1) und 2) zutreffen.	1) Es werden Klemmen und Verbindungen nach IEC 60947-7-1 oder IEC 60947-7-2 verwendet, und die Anforderungen von IEC 60204-1:2006, 13.1.1 sind erfüllt. 2) Die Ausführung selbst stellt sicher, dass Kurzschluss verhindert wird, z. B. durch Kunststoff-Schrumpfschlauch über der Verbindungsstelle.
Unterbrechung einzelner Klemmen	Nein	—

Tabelle D.7 — Fehler und Fehlerausschlüsse — Mehrpolige Steckverbindungen

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Kurzschluss zwischen zwei beliebigen benachbarten Steckerstiften	Kurzschluss zwischen benachbarten Steckerstiften, wenn die Bemerkung zutrifft. Wenn der Leiter auf eine PCB montiert ist, gelten die Erwägungen zum Fehlerausschluss aus Tabelle D.5.	Für mehradrige Drähte durch Anwendung von Aderendhülsen oder anderer geeigneter Mittel. Kriech- und Luftstrecken und alle Abstände sollten mindestens nach IEC 60664-1, Überspannungskategorie III, bemessen sein.
vertauschter oder unrichtig eingesteckter Stift, wenn keine mechanische Möglichkeit zur Verhinderung vorgesehen ist	Nein	—
Kurzschluss zwischen einem beliebigen Leiter (siehe Bemerkung) und der Erde oder einem leitenden Teil oder dem Schutzleiter	Nein	Die Drahtader des Kabels wird als Teil der mehrpoligen Steckverbindung angesehen.
Unterbrechung einzelner Steckerstifte	Nein	—

Tabelle D.8 — Fehler und Fehlerausschlüsse — Schalter — Elektromechanische Positionsschalter, Handschalter (z. B. Tastschalter, Rücksetzschalter, DIP-Schalter, magnetisch betätigte Kontakte, Reedschalter, Druckschalter, Temperaturschalter)

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Nichtschließen von Kontakten	Druckempfindliche Einrichtungen nach ISO 13856.	—
Nichtöffnen von Kontakten	Kontakte nach IEC 60947-5-1:2003, Anhang K öffnen sich.	—
Kurzschluss von benachbarten Kontakten, die voneinander isoliert sind	Kurzschluss für Schalter nach IEC 60947-5-1 kann ausgeschlossen werden (siehe Bemerkung).	Leitfähige Teile, die sich lösen, sollten die Isolation zwischen Kontakten nicht überbrücken können.
gleichzeitiger Kurzschluss zwischen den drei Klemmen von Wechselkontakten	Gleichzeitiger Kurzschluss für Schalter nach IEC 60947-5-1 kann ausgeschlossen werden (siehe Bemerkung).	
Für PL e ist kein Fehlerausschluss für mechanische (z. B. die mechanische Verbindung zwischen Schalter und Kontaktelementen) und elektrische Aspekte zulässig. In diesem Fall ist Redundanz erforderlich. Für Not-Halt-Einrichtungen nach IEC 60947-5-5 ist ein Fehlerausschluss für mechanische Aspekte zulässig, wenn eine Höchstanzahl von Betätigungen berücksichtigt wird.		
ANMERKUNG Fehlerlisten für die mechanischen Gesichtspunkte sind im Anhang A enthalten.		

Tabelle D.9 — Fehler und Fehlerausschlüsse — Schalter — Elektromechanische Einrichtungen
(z. B. Relais, Schütze)

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
alle Kontakte bleiben unter Spannung, wenn die Spule abgeschaltet ist (z. B. durch einen mechanischen Fehler)	Nein	—
alle Kontakte bleiben abgeschaltet, wenn Energie ansteht (z. B. durch einen mechanischen Fehler, Unterbrechung der Spule)	Nein	
Nichtöffnen von Kontakten	Nein	
Nichtschließen von Kontakten	Nein	
gleichzeitiger Kurzschluss zwischen den drei Klemmen eines Wechselkontaktes	Gleichzeitiger Kurzschluss kann ausgeschlossen werden, wenn die Bemerkungen zutreffen.	Kriech- und Luftstrecken werden mindestens nach IEC 60664-1 mit mindestens Verschmutzungsgrad 2/ Überspannungskategorie III, bemessen. Leitfähige Teile, die sich lösen, können die Isolation zwischen den Kontakten und der Spule nicht überbrücken.
Kurzschluss zwischen zwei Kontakten untereinander und/oder zwischen Kontakten und Wicklung	Kurzschluss kann ausgeschlossen werden, wenn die Bemerkungen zutreffen.	
gleichzeitiges Geschlossensein üblicherweise offener und üblicherweise geschlossener Kontakte	Gleichzeitiges Geschlossensein der Kontakte kann ausgeschlossen werden, wenn die Bemerkung zutrifft.	Es werden zwangläufig betätigte (oder mechanisch verbundene) Kontakte angewendet. (Siehe IEC 60947-5-1:2003, Anhang L).

Tabelle D.10 — Fehler und Fehlerausschlüsse — Schalter — Näherungsschalter

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Ausgang dauernd niederohmig	Nein (siehe Bemerkung).	Siehe IEC 60947-5-3.
Ausgang dauernd hochohmig	Nein (siehe Bemerkung).	Es sollten Maßnahmen zur Fehlerverhinderung beschrieben werden.
Spannungsversorgung unterbrochen	Nein	—
Nichtbetätigen des Schalters infolge eines mechanischen Ausfalls	Nichtbetätigung infolge eines mechanischen Ausfalls, wenn die Bemerkung zutrifft.	Alle Teile des Schalters sollten mechanisch ausreichend gut befestigt sein. Für mechanische Aspekte siehe Anhang A.
Kurzschluss zwischen den drei Anschlüssen eines Wechselkontaktes	Nein	—

Tabelle D.11 — Fehler und Fehlerausschlüsse — Elektromagnetische Ventile

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Nichtschalten in die geschaltete Stellung	Nein	—
Nichtschalten in Ruhestellung	Nein	
ANMERKUNG Die Fehlerlisten für die mechanischen Aspekte von pneumatischen und hydraulischen Ventilen werden in Anhang B und Anhang C behandelt.		

Tabelle D.12 — Fehler und Fehlerausschlüsse — Einzelne elektrische Bauteile — Transformatoren

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Unterbrechung einer Wicklung	Nein	–
Kurzschluss zwischen verschiedenen Wicklungen	Kurzschluss zwischen verschiedenen Wicklungen kann ausgeschlossen werden, wenn Bemerkung 1) und 2) zutreffen.	1) Es sollten die Anforderungen von IEC 61558 erfüllt werden. 2) Zwischen unterschiedlichen Wicklungen sind doppelte oder verstärkte Isolierungen oder eine Schutzabdeckung anzuwenden. Es ist nach IEC 61558-1:2005, Abschnitt 18, zu prüfen. Geeignete Prüfspannungen sind in IEC 61558-1:2005, Tabelle 8a, angegeben. Windungs- und Wicklungsschlüsse sind durch geeignete Maßnahmen zu verhindern, z. B. durch — Imprägnierung der Windungen und Wicklungen, so dass alle Hohlräume zwischen Wickelkörper und Wicklung ausgefüllt sind, und — Anwendung von Wickeldrähten mit erhöhten Anforderungen an Isolation und Wärmebeständigkeit. 3) Bei sekundärem Kurzschluss sollte keine Erwärmung über die festgelegte Betriebstemperatur hinaus auftreten.
Kurzschluss in einer Wicklung	Kurzschluss in einer Wicklung kann ausgeschlossen werden, wenn Bemerkung 1) zutrifft.	
Veränderung des wirksamen Windungsverhältnisses	Veränderung des wirksamen Verhältnisses der Windungen kann ausgeschlossen werden, wenn Bemerkung 1) zutrifft. Siehe auch die Anleitung in Bemerkung 3).	

Tabelle D.13 — Fehler und Fehlerausschlüsse — Einzelne elektrische Bauteile — Induktivitäten

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Unterbrechung	Nein	–
Kurzschluss	Kurzschluss kann ausgeschlossen werden, wenn die Bemerkung zutrifft	Die Spule ist einlagig gewickelt, glasiert oder vergossen, hat axiale Drahtanschlüsse und ist axial eingebaut.
zufällige Veränderung des Wertes $0{,}5\ L_N < L < L_N$ + Abweichung, wobei L_N der Nennwert der Induktivität ist	Nein	Abhängig von der Art der Bauweise können andere Bereiche in Betracht gezogen werden.

Tabelle D.14 — Fehler und Fehlerausschlüsse — Einzelne elektrische Bauteile — Widerstände

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Unterbrechung	Nein	–
Kurzschluss	Kurzschluss kann ausgeschlossen werden, wenn Bemerkung 1) oder 2) zutrifft.	1) Für Schichtwiderstände oder für Drahtwiderstände mit einer Sicherung gegen das Abwickeln des Drahtes im Falle eines Bruches, mit axialen Drahtanschlüssen, axial eingebaut und mit einer Lackschicht. 2) Widerstände in SMD-Technologie (SMD: Surface-mounted device) Typ Metallschicht, Baugröße MELF, mini MELF oder µMELF. 3) Beispiel: Wenn das Risiko der Zinn-Whisker-Bildung als hoch angesehen wird, ist der Fehlerausschluss „Kurzschluss eines Widerstands“ nutzlos, da es als Kurzschluss zwischen den Kontakten dieses Bauteils betrachtet werden muss.
Zufällige Veränderung des Wertes $0{,}5\ R_N < R < 2\ R_N$, wobei R_N der Nennwert des Widerstandes ist [siehe Bemerkung 3)]	Nein	Abhängig von der Art der Bauweise können andere Bereiche in Betracht gezogen werden.

Tabelle D.15 — Fehler und Fehlerausschlüsse — Einzelne elektrische Bauteile — Widerstandsnetzwerke

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Unterbrechung	Nein	—
Kurzschluss zwischen zwei beliebigen Anschlüssen	Nein	
Kurzschluss zwischen beliebigen Anschlüssen	Nein	
Zufällige Veränderung des Wertes $0{,}5\ R_N < R < 2\ R_N$, wobei R_N der Nennwert des Widerstandes ist	Nein	Abhängig von der Art der Bauweise können andere Bereiche in Betracht gezogen werden.

Tabelle D.16 — Fehler und Fehlerausschlüsse — Einzelne elektrische Bauteile — Potentiometer

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Unterbrechung eines einzelnen Anschlusses	Nein	—
Kurzschluss zwischen allen Anschlüssen	Nein	
Kurzschluss zwischen zwei beliebigen Anschlüssen	Nein	
Zufällige Veränderung des Wertes $0{,}5\ R_P < R < 2\ R_P$, wobei R_P der Nennwert des Widerstandes ist	Nein	Abhängig von der Art der Bauweise können andere Bereiche in Betracht gezogen werden.

Tabelle D.17 — Fehler und Fehlerausschlüsse — Einzelne elektrische Bauteile — Kondensatoren

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Unterbrechung	Nein	—
Kurzschluss	Nein	
Zufällige Veränderung des Wertes $0{,}5\ C_N < C < C_N +$ Abweichung, wobei C_N der Nennwert der Kapazität des Kondensators ist	Nein	Abhängig von der Art der Bauweise können andere Bereiche in Betracht gezogen werden.
Veränderung des Wertes tan δ	Nein	—

Tabelle D.18 — Fehler und Fehlerausschlüsse — Elektronische Bauteile — Diskrete Halbleiter

(z. B. Dioden, Zener-Dioden, Transistoren, Triacs, Thyristoren, Spannungsregler, Quarzkristall, Fototransistoren, lichtemittierende Dioden [LEDs])

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Unterbrechung eines Anschlusses	Nein	—
Kurzschluss zwischen zwei beliebigen Anschlüssen	Nein	
Kurzschluss gleichzeitig zwischen allen Anschlüssen	Nein	
Veränderung von Kenndaten	Nein	

Tabelle D.19 — Fehler und Fehlerausschlüsse — Elektronische Bauteile — Optokoppler

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Unterbrechung eines einzelnen Anschlusses	Nein	—
Kurzschluss zwischen zwei beliebigen eingangsseitigen Anschlüssen	Nein	
Kurzschluss zwischen zwei beliebigen ausgangsseitigen Anschlüssen	Nein	
Kurzschluss zwischen zwei beliebigen Anschlüssen des Ein- und Ausgangs	Kurzschluss zwischen Ein- und Ausgang kann ausgeschlossen werden, wenn die Bemerkungen zutreffen.	Der Optokoppler ist entsprechend Überspannungskategorie III nach IEC 60664-1 gebaut. Wird ein SELV/PELV-Netzanschluss verwendet, gelten Verschmutzungsgrad 2/ Überspannungskategorie II. ANMERKUNG Siehe Tabelle D.5. Es werden Maßnahmen getroffen, um sicherzustellen, dass ein interner Fehler des Optokopplers nicht zu übermäßigem Temperaturanstieg seiner Isolierwerkstoffe führen kann.

Tabelle D.20 — Fehler und Fehlerausschlüsse — Elektronische Bauteile — Nicht programmierbare integrierte Schaltkreise

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Unterbrechung eines einzelnen Anschlusses	Nein	—
Kurzschluss zwischen zwei beliebigen Anschlüssen	Nein	
Stuck-At-Fehler (d. h. Kurzschluss zu 1 und 0 bei isoliertem Eingang oder unterbrochenem Ausgang). Statisches „0”- und „1”-Signal an allen Ein- und Ausgängen, einzeln oder gleichzeitig	Nein	
Störschwingung der Ausgänge	Nein	
Veränderung von Kennwerten, (z. B. Eingangs-/Ausgangsspannung analoger Geräte)	Nein	
ANMERKUNG In diesem Teil der ISO 13849 werden integrierte Schaltkreise (ICs) mit weniger als 1 000 Gates und/oder weniger als 24 Steckerstiften, Funktionsverstärker, Schieberegister und Hybridmodule als nicht komplex betrachtet. Diese Festlegung ist willkürlich.		

Tabelle D.21 — Fehler und Fehlerausschlüsse — Elektronische Bauteile — Programmierbare und/oder komplexe integrierte Schaltkreise

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Fehler in allen Teilen der Funktion oder in einem Teil der Funktion einschließlich Software-Fehler	Nein	—
Unterbrechung eines einzelnen Anschlusses	Nein	
Kurzschluss zwischen zwei beliebigen Anschlüssen	Nein	
Stuck-At-Fehler (d. h. Kurzschluss zu 1 und 0 bei isoliertem Eingang oder unterbrochenem Ausgang). Statisches „0”- und „1”-Signal an allen Ein- und Ausgängen, einzeln oder gleichzeitig	Nein	
Störschwingung der Ausgänge	Nein	
Veränderung von Kennwerten, z. B. Eingangs-/Ausgangsspannung analoger Geräte	Nein	
unerkannte Fehler in der Hardware, die wegen der Komplexität des IC nicht entdeckt werden	Nein	
Die Analyse sollte zusätzlich Fehler aufdecken, die berücksichtigt werden sollten, wenn sie die Ausführung der sicherheitsbezogenen Funktion beeinflussen.		
ANMERKUNG In dieser Norm wird ein IC als komplex betrachtet, wenn er aus mehr als 1 000 Gates und/oder mehr als 24 Steckerstiften besteht. Diese Festlegung ist willkürlich.		

Anhang E
(informativ)

Beispiel für die Validierung von Fehlverhalten und Mitteln zur Diagnose

E.1 Allgemeines

Dieses Beispiel berücksichtigt die Validierung des PL einer Sicherheitsfunktion (SF 1), mit Ausnahme der Anforderungen der folgenden Aspekte des PL:

— $MTTF_d$-Werte;

— Ausfälle infolge gemeinsamer Ursache (CCFs);

— Softwareanalyse;

— systematische Ausfälle.

Das Beispiel umfasst nicht die Validierung von:

— der Festlegung der Sicherheitsanforderungen (siehe Abschnitt 7);

— Eigenschaften der Sicherheitsfunktionen (siehe Abschnitt 8);

— Umgebungsanforderungen (siehe Abschnitt 10);

— Instandhaltungsanforderungen (siehe Abschnitt 11);

— Dokumentationsanforderungen (siehe Abschnitt 12).

Im vorliegenden Beispiel werden drei Sicherheitsfunktionen SF 1, SF 2 und SF 3 betrachtet.

SF 1 ist eine sicherheitsbezogene Stopp-Funktion von vier einzelnen Maschinen-Antriebselementen, die durch das Öffnen einer verriegelten trennenden Schutzeinrichtung ausgelöst wird, wobei diese Funktion jeweils als separate Sicherheitsfunktion für jedes einzelne Antriebselement behandelt wird (SF 1.0, SF 1.1, SF 1.2 und SF 1.3). Um den Umfang des Beispiels zu verringern, wurde die Validierung auf SF 1.0 und SF 1.3 beschränkt.

Anhang A stellt eine Anleitung zur Verfügung, wie das Fehlverhalten und der Diagnosedeckungsgrad eines gegebenen Steuerkreises zu untersuchen sind. Die Verfahren, die zur Bestimmung des Diagnose-deckungsgrades angewendet werden, beruhen auf der Fehlermode und Einflussanalyse (FMEA), wobei ISO 13849-1:2006, Anhang E, berücksichtigt wird.

ANMERKUNG Dieses Beispiel umfasst nicht das gesamte Validierungsverfahren sicherheitsbezogener Teile von Steuerungen (SRP/CS). Insbesondere wurde die notwendige Validierung der PLC-Software nicht berücksichtigt. Validierung sicherheitsbezogener Software, siehe 9.5.

E.2 Beschreibung der Maschine

Das Beispiel beruht auf einer automatischen Montagemaschine, mit manueller Bestückung und Entnahme von Werkstücken. Es ist vorgesehen, dass die Maschine zwei aufeinander folgende Operationen an jedem Werkstück durchführt: Einsetzen einer Kugel und Montage von Schrauben.

Die Maschine umfasst vier Stationen: eine zum Bestücken, eine zur Entnahme und zwei Arbeitsstationen (siehe Bild E.1). Die erste Arbeitsstation ist der pneumatisch angetriebene Kugeleinsetzvorgang und die zweite ist die pneumatisch angetriebene Schraubenmontage.

Ein elektrisch betriebener Drehtisch bewegt die Werkstücke zu jeder der vier Stationen. Die Werkstücke werden von Hand auf die auf dem Drehtisch angebrachten Werkstückhalter gesetzt und von diesen entnommen. Ein umrichtergesteuerter Elektromotor treibt ein Umlaufgetriebe und das Riemenantriebssystem, das den Drehtisch bewegt, an.

An der ersten Arbeitsstation wird eine Kugel mit einem waagerecht montierten pneumatischen Zylinder in das Werkstück eingesetzt, der von einem monostabilen 5/2-Wegeventil (1V1, siehe Bild E.3) gesteuert wird. Die Grundstellung (Ventil ohne Spannung) dieses Zylinders ist die eingefahrene Stellung. Die Tiefe der eingesetzten Kugel wird überprüft, indem ein Grenzlagenschalter an der vollständig ausgefahrenen Stellung des Zylinders überwacht wird. Der aufgebrachte Pressdruck wird durch einen Drucksensor in der Zuleitung zum Ausfahren (des Zylinders) überwacht.

Die Schraubstation besteht aus einem senkrecht montierten, kolbenstangenlosen pneumatischen Zylinder, der eine pneumatisch angetriebene, sich drehende Schraubeinheit trägt. Die Schraubeinheit wird durch den pneumatischen Zylinder angehoben und abgesenkt, was durch ein monostabiles 5/2-Wegeventil (2V1) gesteuert wird. Die Grundstellung (Ventil ohne Spannung) dieses Zylinders ist die obere Stellung, wobei die Schraubeinheit angehoben ist. Zusätzlich befindet sich ein entsperrbares Rückschlagventil (2V2) an der unteren Verbindung mit dem pneumatischen Zylinder.

Die Drehbewegung der Schraubeinheit wird durch einen pneumatischen Motor erzeugt, der durch ein monostabiles 5/2-Wegeventil (3V1) gesteuert wird. Die Grundstellung (Ventil ohne Spannung) dieses pneumatischen Motors ist der AUS-Zustand. Das mit der Schraubeinheit erzeugte Drehmoment wird durch einen Drucksensor in der Luftversorgungsleitung der Schraubeinheit überwacht.

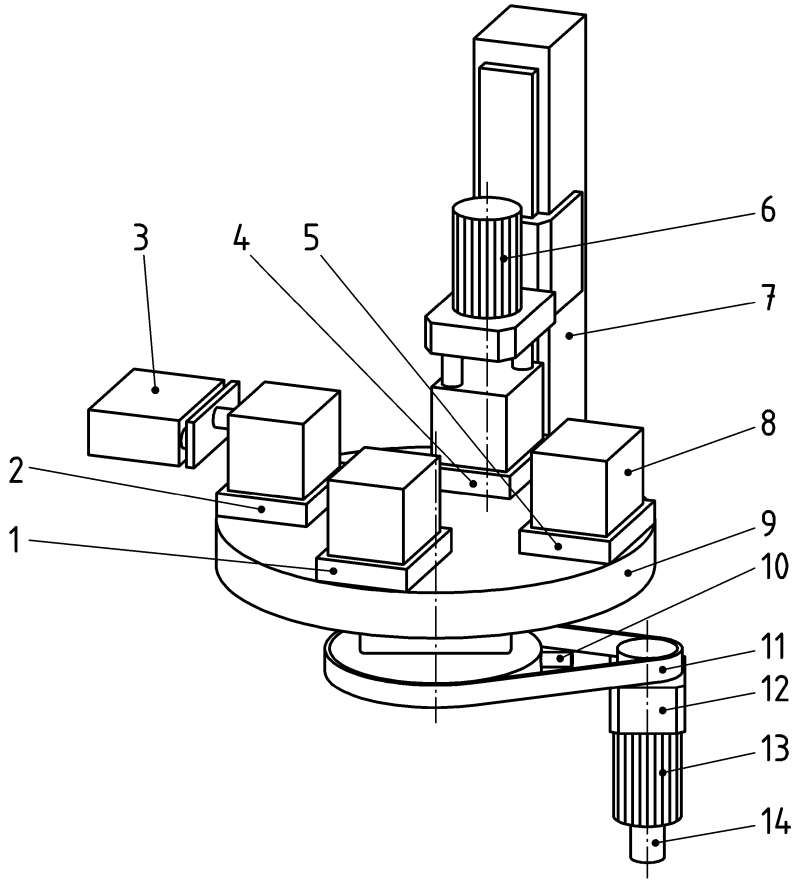
Ein einzelner Zyklus der Maschine im automatischen Betriebsmodus wird durch das Betätigen des Anlauf-Tastschalters ausgelöst. Zu Beginn eines Zyklus befinden sich drei Werkstücke auf dem Drehtisch: (i) ein neu aufgeladenes Werkstück, (ii) ein teilweise fertig gestelltes Werkstück (Kugel eingesetzt) und (iii) ein fertig gestelltes Werkstück (Kugel eingesetzt und Schraube angezogen). Jeder Zyklus der Maschine besteht aus einer Drehung des Drehtisches um 90°, gefolgt von gleichzeitigem Einsetzen der Kugel und Schraubvorgängen an den neu aufgeladenen und teilweise fertig gestellten Werkstücken. Die Maschine kommt dann zu einem betriebsbedingten Halt, wonach der Bediener die verriegelte trennende Schutzeinrichtung öffnet, um das fertig gestellte Werkstück zu entnehmen und ein neues Werkstück aufzubringen. Die Fertigstellung eines Werkstücks erfordert drei Maschinenzyklen, um das Werkstück um 270° von der Stelle zum Bestücken bis zur Entnahmestelle zu drehen.

Die folgenden Betriebsarten sind vorgesehen:

— automatischer Betrieb mit Bestücken und Entnahme von Hand (vollständige Bewegung der Maschine mit der verriegelten trennenden Schutzeinrichtung in der geschlossenen Stellung);

— Einrichtbetrieb für den Drehtisch (Bewegung des Drehtisches mit einer Steuereinrichtung mit selbsttätiger Rückstellung und bei geöffneter verriegelter trennender Schutzeinrichtung).

Die Maschine weist mechanische Gefährdungen auf, die aus Bewegungen der pneumatischen Antriebe (an den Arbeitsstationen zum Einsetzen der Kugel und zum Schrauben) und des elektrisch betriebenen Drehtisches entstehen können. Aus diesem Grund wurden mechanisch trennende Schutzeinrichtungen angebracht, von denen alle feststehend sind mit Ausnahme einer verriegelten trennenden Schutzeinrichtung, die den Zugang zur Bestückungs- und Entnahmestation (der Gefahrenzone) ermöglicht.



Legende

1	Einlegestation	8	Werkstück
2	Kugeleinsetzstation	9	Drehtisch
3	Kugeleinsetzzylinder (A1)	10	Impulsgeber (G2)
4	Schraubstation	11	Antriebsriemen
5	Entnahmestation	12	Getriebe
6	Schraubeinheit (A3)	13	Elektromotor (M1)
7	Vertikalantrieb für Schraubeinheit (A2)	14	Drehsensor (G1)

Bild E.1 — Beispielmaschine — Automatische Montagemaschine

E.3 Festlegung der Anforderungen an Sicherheitsfunktionen

Im automatischen Betrieb erfolgt der Schutz gegen gefährliche Bewegungen durch folgende Sicherheitsfunktion:

— SF 1 sicherheitsbezogenes Anhalten, das durch das Öffnen der verriegelten trennenden Schutzeinrichtung ausgelöst wird und Vermeidung eines unerwarteten Anlaufs, wenn die verriegelte trennende Schutzeinrichtung geöffnet ist.

In diesem speziellen Beispiel, kann das für jedes einzelne der vier Maschinen-Antriebselemente als gesonderte Sicherheitsfunktion betrachtet werden:

— SF 1.0 Elektromotor des Drehtisches (M1);

— SF 1.1 Kugeleinsetzzylinder (A1);

— SF 1.2 Vertikalzylinder für Schraubeinheit (A2);

— SF 1.3 Pneumatikmotor der Schraubeinheit (A3).

ANMERKUNG 1 In diesem Beispiel werden der sicherheitsbezogene Halt und der Schutz gegen unerwarteten Anlauf als eine einzige Sicherheitsfunktion betrachtet, weil beide in dieselbe Kombination aus SRP/CS einbezogen sind.

Während des Einrichtbetriebs für den Drehtisch, bei dem die verriegelte trennende Schutzeinrichtung geöffnet ist (mit den durch SF 1.1, SF 1.2 und SF 1.3 ausgeschalteten pneumatischen Antrieben), wird der sichere Zustand der Drehtischbewegung durch eine Kombination folgender Sicherheitsfunktionen erreicht:

— SF 2 sicher begrenzte Geschwindigkeit;

— SF 3 selbsttätiger Rückstellungsbetrieb.

Tabelle E.1 — Aktive Sicherheitsfunktionen entsprechend der jeweiligen Betriebsart

Betriebsart	Sicherheitsfunktion					
	SF 1.0	SF 1.1	SF 1.2	SF 1.3	SF 2	SF 3
Automatischer Betrieb (verriegelte trennende Schutzeinrichtung geschlossen)	X	X	X	X		
Einrichtbetrieb (verriegelte trennende Schutzeinrichtung geöffnet)		X	X	X	X	X
X: Sicherheitsfunktion aktiv						

Nach Vornahme einer Risikobeurteilung wurden den Sicherheitsfunktionen folgende PL_r-Werte zugewiesen:

— PL_r d für SF 1 (sicherheitsbezogenes Anhalten und Vermeidung von unerwartetem Anlauf);

— PL_r d für SF 2 (sicher begrenzte Geschwindigkeit);

— PL_r c für SF 3 (selbsttätige Rückstellung).

ANMERKUNG 2 Die Auswahl von PL_r c für SF 3 berücksichtigt ihre Anwendung in Kombination mit SF 2, für die PL d erreicht wird.

Wenn SF 1 verlangt wird, werden folgende Vorgänge ausgelöst:

— der Drehtisch führt ein gesteuertes Abschalten entsprechend der Stoppkategorie 2 nach IEC 60204-1 aus;

— der waagerecht montierte pneumatische Zylinder (A1) der Arbeitsstation zum Einsetzen der Kugel und der senkrecht montierte pneumatische Zylinder (A2) der Arbeitsstation zum Schrauben kehren in ihre Grundstellungen zurück und/oder verbleiben darin (d. h. eingefahren bzw. oben);

— die Schraubeinheit (A3) hält sofort an.

ANMERKUNG 3 Für das Beispiel hat die Risikobeurteilung ermittelt, dass der Ausfall der gesteuerten Verzögerung des Drehtisches als Ergebnis einer Fehlfunktion des Inverters annehmbar war, und dass die Bewegung der pneumatischen Zylinder A1 und A2 in ihre Grundstellungen keine Gefährdung dargestellt hat.

Der Mindestabstand zwischen der verriegelten trennenden Schutzeinrichtung und diesen sich bewegenden Teilen der Maschine wurde nach ISO 13855 basierend auf der Abschaltzeit der Maschine ermittelt.

Die Maschine verfügt über weitere Sicherheitsfunktionen wie einem Not-Halt, einer Wiederanlaufsperre, Reset sowie einer Betriebsartenwahl, die in diesem Beispiel aber nicht berücksichtigt werden und demzufolge werden auch die dafür maßgeblichen Bauteile nicht in den Schaltplänen der Bilder E.2 und E.3 dargestellt.

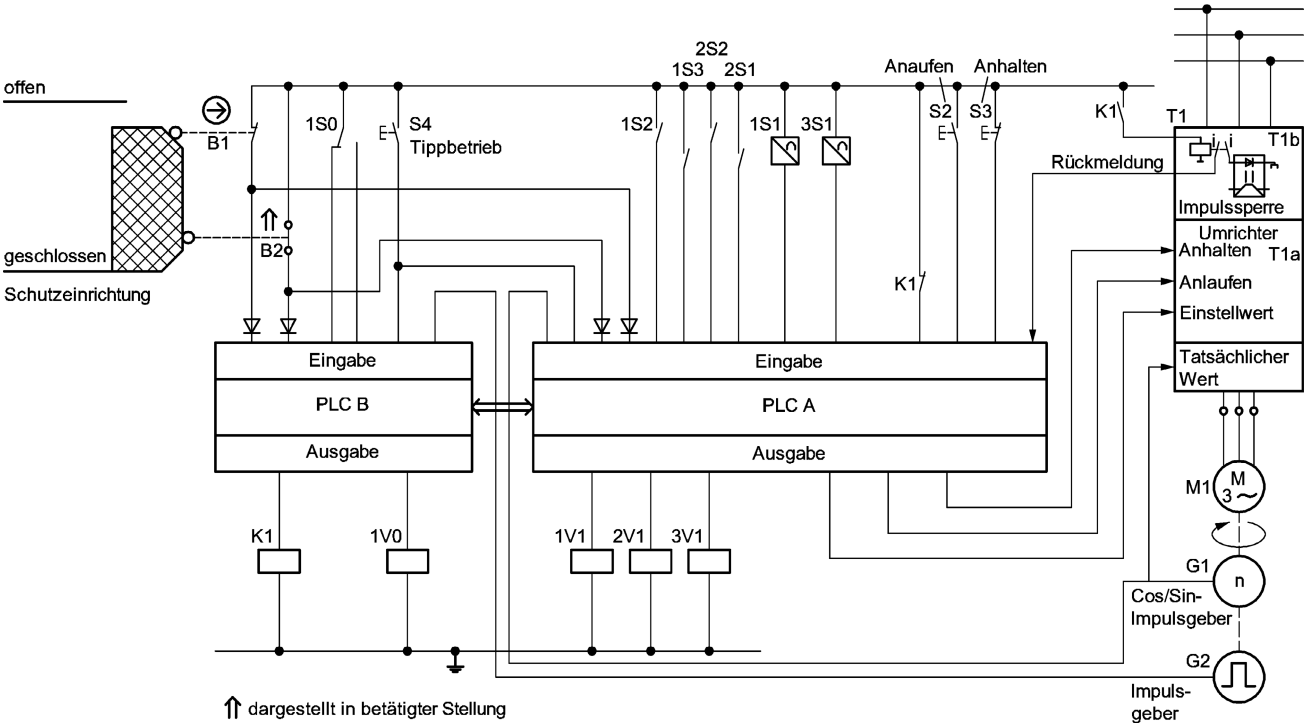


Bild E.2 — Automatische Montagemaschine — Elektrischer Schaltplan

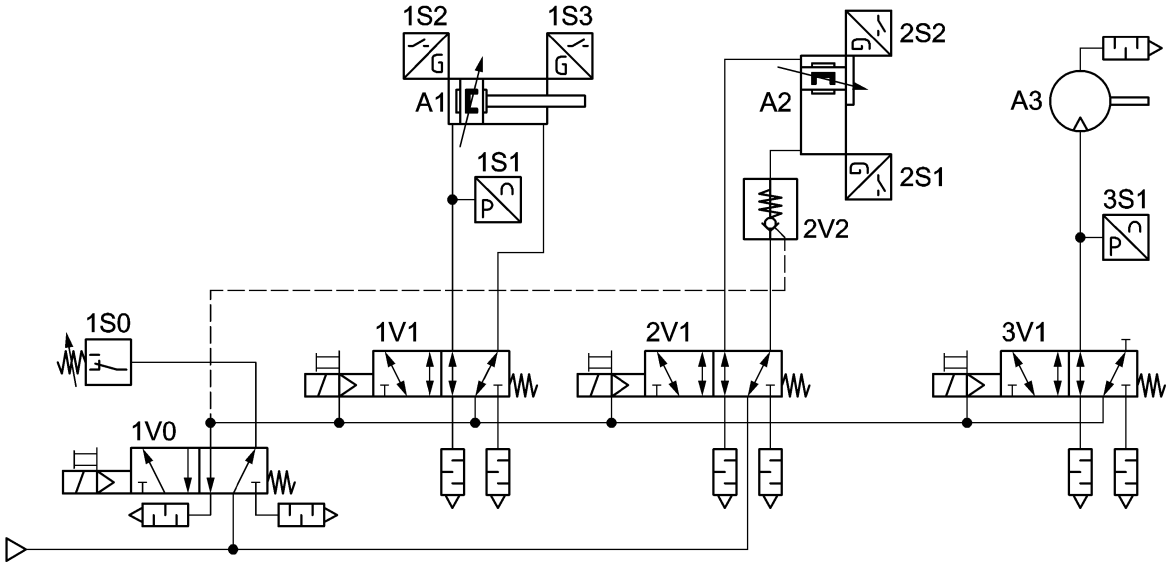


Bild E.3 — Automatische Montagemaschine — Pneumatischer Schaltplan

E.4 Gestaltung der SRP/CS

E.4.1 Allgemeines

Die Steuerung wurde in diesem Beispiel unter Anwendung einer Kombination von elektromechanischen, elektronischen und pneumatischen Techniken ausgeführt.

Um den PL_r für SF 1 und SF 2 zu erreichen, wurde Kategorie 3 ausgewählt. Deshalb wurde ein diversitärer redundanter und überwachter Aufbau für alle elektrischen und pneumatischen Teile, die mit diesen Sicherheitsfunktionen verbunden sind, realisiert (siehe Bilder E.2 und E.3).

Um PL_r für SF 3 zu erreichen, wurde eine Kombination von Kategorie 2 und Kategorie 3 ausgewählt.

Die Signale von den Sensoren und Schaltern (Positionsschalter für die verriegelte trennende Schutzeinrichtung, Tastschalter für selbsttätige Rückstellung) wurden verdoppelt und mit zwei verschiedenen PLCs (unterschiedliche Arten von Hardware für PLC A und PLC B) verbunden. Diese verarbeiten die Signale unter Verwendung von besonderen Softwarefunktionsblöcken (SRASW). Jede PLC steuert auch die Funktion des Drehtischumrichters und der pneumatisch angetriebenen Maschinen-Antriebselemente über Steuersignale, die jeweils von den Steuersignalen der jeweils anderen PLC unabhängig sind.

Zu Diagnose- (Kreuzvergleich) und Synchronisierungszwecken kommunizieren die beiden PLCs miteinander über ein Standardbussystem.

Der spezifische Umrichter in diesem Beispiel hat eine zusätzliche Vorrichtung (internes Relais), um die Ansteuerung der Leistungshalbleiter auszuschalten (Impulssperre), was als zweiter Abschalteweg betrachtet werden kann (sicher abgeschaltetes Moment (STO) nach IEC 61800-5-2).

Diese Impulssperre führt nicht zu einem abrupten Halt des sich drehenden Motors, weil das Ausschalten der Umrichtersteuerung des Motors ein ungesteuertes Abbremsen verursacht. In diesem Beispiel würde die Impulssperre jedoch das Anhalten des Drehtisches immer noch bewirken, bevor eine Bedienperson die Gefahrenzone erreichen kann. Somit ist das gesteuerte Abbremsen bis zum Stillstand, die üblicherweise der Impulssperre vorausgeht, keine geforderte Eigenschaft von SF 1.0.

Im pneumatischen Kreis wird die Luftzufuhr zu jedem Maschinen-Antriebselement (A1, A2 und A3) durch ein vorgesteuertes monostabiles 5/2-Wegeventil (1V1, 2V1 und 3V1) gesteuert. Die Steuerluft für alle drei Ventile wird durch ein zusätzliches Ventil (1V0) derselben Bauart geschaltet, wodurch ein redundanter Kanal realisiert wird. Der Zustand dieses Freigabeventils wird mittels eines Druckschalters (1S0) überwacht. Die Luftzufuhr für A2 wird von der Hauptluftzufuhr entnommen, während die Luftzufuhr für A1 und A3 der Steuerluftzufuhr entnommen wird (1V0).

Das Energiefreischalten der Antriebskammer des sich bewegenden Zylinders A1 während des Eindringens in den Arbeitsraum erfolgt ebenfalls über zwei Kanäle:

— Entlüftung über 1V1 durch Schalten in die Ruhestellung, und

— Energiefreischalten über 1V0 durch Schalten in die Ruhestellung.

Der Zustand von 1V1 wird mit einem Grenzlagenschalter (1S2) überwacht.

Ein entsperrbares Rückschlagventil (2V2), das ebenfalls seine Steuerluft von 1V0 bezieht, befindet sich am unteren Anschluß von A2 (senkrecht montierter kolbenstangenfreier pneumatischer Zylinder). Das ermöglicht einen redundanten Kanal zum Anhalten der Abwärtsbewegung und zum Hochhalten des Maschinen-Antriebselements in seiner Ausgangsstellung (oben).

Der Zustand von 2V1 wird mit einem Grenzlagenschalter (2S2) überwacht.

Die Luftversorgung für den pneumatischen Motor A3 (Schraubeinheit) erfolgt vielmehr über die Steuerluftzufuhr (1V0) als über die Hauptluftzufuhr. Diese Verwendung von 1V0 zur Abschaltung der Luftzufuhr zu A3 zusätzlich zu 3V1 sorgt für einen redundanten Steuerungskanal, wodurch sichergestellt wird, dass A3 sich nicht weiter dreht, falls 3V1 in geschalteter Stellung ausfällt. Der Zustand von 3V1 wird mit einem Drucksensor (3S1) überwacht, der ein analoges Ausgangssignal liefert.

In Übereinstimmung mit Kategorie 3 werden grundlegende und bewährte Sicherheitsprinzipien eingehalten, und die Anforderungen an Kategorie B werden ebenfalls erfüllt. Insbesondere wurden die Anforderungen der Normen IEC 60204-1 und ISO 4414 angewendet.

Die Eigenschaften der Bauteile, die in SRP/CS enthalten sind, werden ausführlich in Tabelle E.2 erklärt.

Tabelle E.2 — Eigenschaften von Bauteilen, die SRP/CS implementieren
(Teileliste aus Bild E.2 und Bild E.3)

Kennzeichnung des Bauteils	Funktion	Element	Eigenschaft	Bewährtes Sicherheitsprinzip[a]	Möglicher Fehlerausschluss
B1	Überwachung der Stellung der verriegelten trennenden Schutzeinrichtung	Verriegelungsschalter	IEC 60947-5-1:2003, einschließlich Zwangsöffnung nach IEC 60947-5-1:2003, Anhang K	Zwangläufiger Betätigungsmodus	Ein Ausfall der Schaltkontakte zur Öffnung bei Betätigung kann ausgeschlossen werden. Elektrische Fehler, weil B1 über einen zwangläufigen Betätigungsmodus verfügt
B2	Überwachung der Stellung der verriegelten trennenden Schutzeinrichtung	Verriegelungsschalter	IEC 60947-5-1	nein	nein
S4	Erzeugt die selbsttätige Rückstellungsbewegung im Einrichtbetrieb	Schließerdrucktaster	—	nein	nein
PLC A PLC B	Verarbeitung sicherheitsbezogener und nicht sicherheitsbezogener Signale	Speicherprogrammierbare Steuerung (PLC)	IEC 61131-1 und IEC 61131-2	nein	nein
K1	Erzeugt ein redundantes STOPP-Signal für den Umrichter bei einem Versagen im PLC A-Pfad	Hilfsschütz	IEC 60947-5-1, einschließlich zwangsgeführte Kontaktelemente nach IEC 60947-5-1:2003, Anhang L und EN 50205	zwangsgeführte Kontakte	nein
T1	Treibt den Elektromotor für den Drehtisch an	Umrichter	Der Umrichter verfügt über einen zusätzlichen Abschalteweg durch Impulssperre	Sperrrelais mit zwangsgeführten Kontakten	nein
G1	Misst die Geschwindigkeit des Elektromotors für den Drehtisch	Drehzahlsensor (Cos/Sin-Impulsgeber)	—	nein	nein
G2	Überwacht die Bewegung des Drehtisches	Impulssensor	—	nein	nein
1V0	Schalten der Vorsteuerluft für die Wegeventile 1V1, 2V1, 3V1 und Ansteuern des Rückschlagventils 2V2	Magnet-Wegeventil	Ventil mit Federvorspannung, 5/2-Funktion, vorgesteuert, interne Vorsteuerluft-Versorgung, Schieberventil mit Überdeckung	Tabelle B.2 Überdimensionierung/Sicherheitsfaktor, gesicherte Position (Anwendung bewährter Federn), ausreichende positive Überdeckung bei Kolbenschieberventilen	Druckaufbau bei Anschluss 4 mit geleertem Anschluss 5 in Normalstellung, Versagen der Dichtung durch Fließpressung, Bewegen des Ventilschiebers ohne Antriebskraft

Tabelle E.2 *(fortgesetzt)*

Kennzeichnung des Bauteils	Funktion	Element	Eigenschaft	Bewährtes Sicherheitsprinzip[a]	Möglicher Fehlerausschluss
1V1	Steuern des Zylinders A1 zum Einsetzen der Kugel	siehe 1V0	siehe 1V0	siehe 1V0	siehe 1V0
2V1	Steuern des Zylinders A2 zum Schrauben				
3V1	Steuern der Schraubeinheit A3 (pneumatischer Motor)				
2V2	Absturzsicherung für den senkrecht montierten Zylinder A2 der Schraubeinheit	Rückschlagventil	entsperrbares Rückschlagventil, federbelastetes Sitzventil	Tabelle B.2: durch den Lastdruck geschlossenes Ventil	Öffnen ohne Ansteuersignal
1S0	Überwacht den Zustand von Ventil 1V0	Druckschalter	Fester Schaltpunkt	Grundlegende Sicherheitsprinzipien sind zur Überwachung nicht erforderlich (keine Sicherheitsfunktion)	Nein
1S1	Überwacht den während des Kugeleinsetzvorgangs aufgebrachten Druck	Drucksensor	Analoges Ausgabesignal	Grundlegende Sicherheitsprinzipien sind zur Überwachung nicht erforderlich (keine Sicherheitsfunktion)	Nein
3S1	Überwacht das während des Schraubvorgangs aufgebrachte Drehmoment (Druck)				
1S2, 1S3	Grenzlagenschalter für Zylinder A1 zum Einsetzen der Kugel	Näherungssensor	Magnetisches Messprinzip	Grundlegende Sicherheitsprinzipien sind zur Überwachung nicht erforderlich (keine Sicherheitsfunktion)	Nein
2S1, 2S2	Grenzlagenschalter für Zylinder A2 zum Schrauben				
A1	Kugeleinsetzzylinder	Pneumatischer Zylinder	nach ISO 13849-1:2006, 3.1.1, nicht im Anwendungsbereich dieser Norm		
A2	Schraubzylinder	Kolbenstangenloser pneumatischer Zylinder mit äußerer Führung	nach ISO 13849-1:2006, 3.1.1, nicht im Anwendungsbereich dieser Norm		
A3	Schraubeinheit	Pneumatischer Motor	nach ISO 13849-1:2006, 3.1.1, nicht im Anwendungsbereich dieser Norm		

[a] Bei der Gestaltung der Bauteile wurden auch grundlegende Sicherheitsprinzipien berücksichtigt (siehe Tabelle D.1 für elektrische Bauteile und Tabelle B.1 für pneumatische Bauteile).

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

Entsprechend der Spezifikation der Maschine muss das Öffnen der verriegelten trennenden Schutzeinrichtung das Anhalten der vier Maschinen-Antriebselemente veranlassen: (i) Drehtisch, (angetrieben durch einen umrichtergesteuerten Motor), (ii) Zylinder zum Einsetzen der Kugel, (iii) Zylinder zum vertikalen Bewegen der Schraubeinheit und (iv) Schraubeinheit. Diese Funktion kann deshalb wie in Bild E.4 gezeigt dargestellt werden.

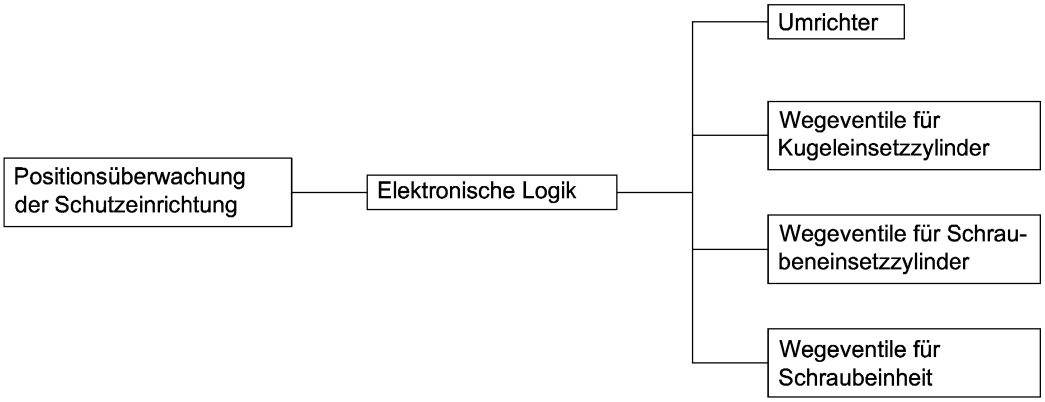


Bild E.4 — Funktionsblöcke SF 1.0, SF 1.1, SF 1.2 und SF 1.3

Sobald die verriegelte trennende Schutzeinrichtung geöffnet wird, veranlasst PLC A ein Abschalten des Drehtisches, indem ein Abschaltsignal an den Umrichter (T1a) abgegeben wird. PLC B überwacht das sich daraus ergebende Abbremsen des Drehtisches über G2. Wenn PLC B erkennt, dass der Drehtisch den Stillstand erreicht hat, wird K1 abgeschaltet, um die Impulssperre am Umrichter (T1b) auszulösen. Wenn der Drehtisch aufgrund eines Fehlers in T1a oder PLC A nicht anhält, erkennt PLC B diesen Fehler und steuert über sein eigenes Abschaltsignal den Umrichter (T1b) ab. Das ist der zweite unabhängige Kanal für die Abschaltfunktion. Der Teil der Sicherheitsfunktion hinsichtlich der Vermeidung eines unerwarteten Anlaufens wird auf dieselbe Weise ausgeführt.

Bei Öffnen der verriegelten trennenden Schutzeinrichtung veranlasst PLC A außerdem, ein erstes Abschalten des Kugeleinsetzzylinders, des Schraubeneinsetzzylinders und der Schraubeinheit durch das Abschalten von 1V1, 2V1 und 3V1. PLC B veranlasst einen weiteren Stopp dieser Aktuatoren durch Abschalten von 1V0.

Wenn der Drehtisch bereits abgeschaltet ist, aber die Arbeitsstationen zum Einsetzen der Kugel und zur Schraubbefestigung beim Öffnen der verriegelten trennenden Schutzeinrichtung noch in Betrieb sind, dann schaltet PLC A sofort 1V1, 2V1 und 3V1 ab und PLC B schaltet sofort K1 ab. PLC B schaltet auch 1V0 nach einer Verzögerung ab, was ermöglicht, dass der Kugeleinsetzzylinder (A1) seinen Weg in die Grundstellung abschließt.

Solange sich die verriegelte trennende Schutzeinrichtung in offener Stellung befindet, ist es erforderlich sicher zu stellen, dass ein Versagen des Freigabepfads von PLC A nicht zu einem ungesteuerten Anlaufen führt. Das wird erreicht, indem PLC B K1 abschaltet, sobald der Drehtischmotor zum Stillstand gekommen ist und 1V0 ebenfalls abgeschaltet wird, um ein Anlaufen des Kugeleinsetzzylinders oder des Schraubzylinders zu verhindern.

Die Bewertung des PL für die SRP/CS, die SF 1 ausführen, wurde wie folgt durchgeführt:

a) **Identifikation der sicherheitsbezogenen Teile**

Die sicherheitsbezogenen Teile der Abschaltfunktion SF 1.0 und deren Aufteilung in Kanäle kann durch das in Bild E.5 gezeigte sicherheitsbezogene Blockdiagramm dargestellt werden.

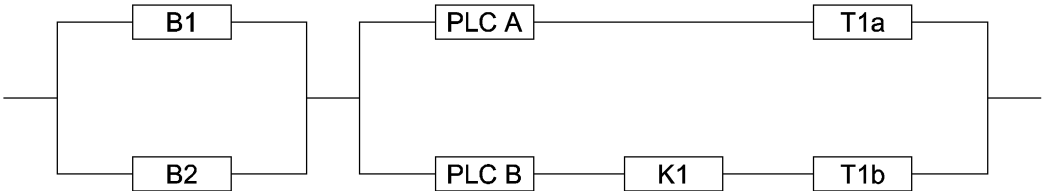
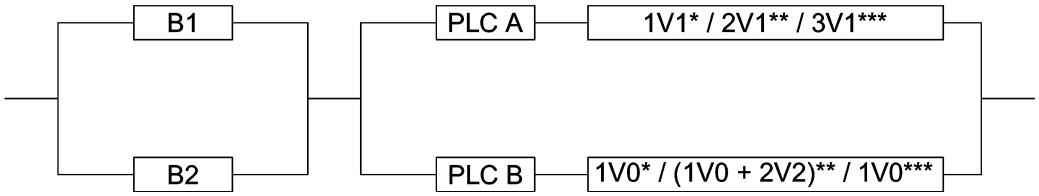


Bild E.5 — Sicherheitsbezogenes Blockdiagram von SF 1.0

Auf ähnliche Weise können die sicherheitsbezogenen Teile der Abschaltfunktionen SF 1.1, SF 1.2 und SF 1.3 und ihre Aufteilung in Kanäle durch das in Bild E.6 gezeigte sicherheitsbezogene Blockdiagramm dargestellt werden.



*SF 1.1 **SF 1.2 ***SF 1.3

Bild E.6 — Sicherheitsbezogenes Blockdiagramm von SF 1.1, SF 1.2 und SF 1.3

Die beiden Teile der Diagramme in den Bildern E.5 und E.6 können jeweils der vorgesehenen Architektur für Kategorie 3 zugeordnet werden, so dass die Diagramme, wie in Bild E.7 dargestellt, auf die beiden SRP/CS (Eingang, Logik/Ausgang) vereinfacht werden können.

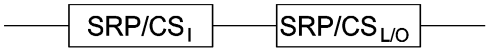


Bild E.7 — Kombination von SRP/CS die die Sicherheitsfunktionen ausführen

Für jede SRP/CS wurde ein PL bestimmt, indem das vereinfachte Verfahren aus ISO 13849-1:2006, 4.5.4, angewendet wurde.

b) **Bestimmung der $MTTF_d$ jedes Kanals**

Für die Bestimmung der $MTTF_d$-Werte der Bauteile werden vom Hersteller zur Verfügung gestellte Zuverlässigkeitsdaten verwendet.

Für die Bestimmung der $MTTF_d$ eines Kanals wurde das „Parts-Count"-Verfahren (siehe ISO 13849-1:2006, Anhang D) angewendet. Der unterschiedliche redundante Aufbau führt zu unterschiedlichen $MTTF_d$-Werten für jeden Kanal, deshalb ergibt die Anwendung der Symmetrisierungsgleichung ein Durchschnittsergebnis für die $MTTF_d$ von 25 Jahren (mittel) für jeden Kanal von sowohl SRP/CS_I als auch $SRP/CS_{L/O}$ von SF 1.0, SF 1.1, SF 1.2 und SF 1.3 (siehe ISO 13849-1:2006, D.2).

c) Bestimmung von DC_{avg}

Der DC_{avg} wurde für beide SRP/CS aus dem DC der internen Tests und den Überwachungsmaßnahmen für die verschiedenen Bauteile bestimmt.

Eine Überprüfung der Plausibilität der Schutzeinrichtungs-Verriegelungsschalter B1 und B2 durch PLC A und PLC B nach ISO 13849-1:2006, Anhang E, ergibt einen hohen DC_{avg} (99 %) für die SRP/CS_I von SF 1.0, SF 1.1, SF 1.2 und SF 1.3.

Es werden folgende Diagnosemaßnahmen in den SRP/$CS_{L/O}$ von SF 1.0, SF 1.1, SF 1.2 und SF 1.3 realisiert:

— Überwachung des Hilfsschützes K1 durch PLC A über die Stellung der K1-Kontakte;

— Kreuzvergleich zwischen PLC A und PLC B;

— indirekte Überwachung von T1a und PLC A durch PLC B über G2;

— indirekte Überwachung der PLC A-Ausgangskarte durch PLC A selbst mittels 1S2, 2S2, 3S1 und G1;

— Überwachung des Programmablaufs durch einen internen Watchdog in PLC A und in PLC B;

— Indirekte Überwachung von T1a durch PLC A über G1;

— Überwachung von T1b durch PLC A über die Stellung des Impulssperrrelais;

— indirekte Überwachung von PLC B durch PLC A über die Stellung der K1-Kontakte;

— indirekte Überwachung der PLC B-Ausgangskarte durch PLC B selbst mittels 1S0;

— indirekte Überwachung von 1V1 durch PLC A über 1S2;

— indirekte Überwachung von 2V1 durch PLC A über 2S2;

— indirekte Überwachung von 3V1 durch PLC A über 3S1;

— indirekte Überwachung von 1V0 durch PLC B über 1S0;

— Fehlererkennung von PLC A, T1a und 1V1, 2V1 und 3V1 durch Prozessbeobachtung.

Nach ISO 13849-1:2006, Anhang E, bieten diese Diagnosemaßnahmen ein Ergebnis von DC_{avg} mittel (90 %) für die SRP/$CS_{L/O}$ von SF 1.0, SF 1.1, SF 1.2 und SF 1.3.

d) **Bestimmung der Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF)**

Es wird angenommen, dass geeignete Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (Trennung, Ungleichheit, Schutz gegen Überdruck, Umgebungsbedingungen) für beide SRP/CS von SF 1.0, SF 1.1, SF 1.2 und SF 1.3 getroffen wurden, die nach ISO 13849-1:2006, Anhang F, einen Wert von 75 Punkten für jede SRP/CS ergeben.

e) **Bestimmung des PL für jedes SRP/CS**

Der PL für jedes SRP/CS wird wie folgt bestimmt:

SRP/CS_l von SF 1,0, SF 1.1, SF 1.2 und SF 1.3:

— Kategorie 3;

— mittlere $MTTF_d$ jedes Kanals;

— hoher DC_{avg};

— 75 Punkte für Maßnahmen gegen CCF.

Werden diese Werte nach ISO 13849-1:2006, Bild 5, ausgewertet, jedoch mit DC_{avg} begrenzt auf mittel (Kategorie 3), ergibt sich PL d.

$SRP/CS_{L/O}$ von SF 1,0, SF 1.1, SF 1.2 und SF 1.3:

— Kategorie 3;

— mittlere $MTTF_d$ jedes Kanals;

— mittlerer DC_{avg},

— 75 Punkte für Maßnahmen gegen CCF.

Werden diese Werte nach ISO 13849-1:2006, Bild 5, ausgewertet, ergibt sich PL d.

f) **Ermittlung des PL für die Kombination von SRP/CS, die SF 1.0, SF 1.1, SF 1.2 und SF 1.3 ausführen**

Entsprechend ISO 13849-1:2006, 6.3, und unter Berücksichtigung der Tatsache, dass die einzelnen SRP/CS für SF 1.0, SF 1.1, SF 1.2 und SF 1.3 die gleichen Werte von PL aufweisen, wird der PL für die gesamte Kombination von SRP/CS für SF 1.0, SF 1.1, SF 1.2 und SF 1.3 wie folgt ermittelt:

— $PL_{niedrig} = d$;

— $N_{niedrig} = 2$;

Der PL für die Kombination von SRP/CS für jede der Funktionen SF 1.0, SF 1.1, SF 1.2 und SF 1.3 ist daher PL d.

ANMERKUNG Die Berechnung des resultierenden PL durch Addition der PFH-Werte aller Untersysteme führt zu einem genaueren Ergebnis.

g) **systematische Ausfälle**

Es wird angenommen, dass geeignete Maßnahmen nach ISO 13849-1:2006, Anhang G, gegen systematische Ausfälle der SRP/CS für SF 1.0, SF 1.1, SF 1.2 und SF 1.3 angewendet wurden.

E.4.3 Sicherheitsfunktion SF 2 — Sicher begrenzte Geschwindigkeit (SLS – en: safely-limited speed)

Wenn sich die Maschine im Einrichtbetrieb und die verriegelte trennende Schutzeinrichtung in offener Stellung befindet, kann sich der Drehtisch nur mit einer sicher begrenzten Geschwindigkeit (SLS) bewegen, die sowohl von G1 als auch von G2 gemessen wird. PLC A überwacht das Signal von G1 und PLC B überwacht das Signal von G2 und beide PLCs führen den Vergleich beabsichtigte/tatsächliche Geschwindigkeit unabhängig voneinander aus. Wird die Geschwindigkeit durch den Umrichter T1a nicht erfolgreich auf den begrenzten Wert verringert, kann PLC A reagieren, indem sie ein Abschaltsignal an den Umrichter (T1a) abgibt. PLC B kann durch Aktivieren einer verzögerten Impulssperre am Umrichter (T1b) über K1 reagieren.

a) **Identifikation der sicherheitsbezogenen Teile**

Die sicherheitsbezogenen Teile der Sicherheitsfunktion SF 2 und ihre Unterteilung in Kanäle kann durch das in Bild E.8 gezeigte sicherheitsbezogene Blockdiagramm dargestellt werden.

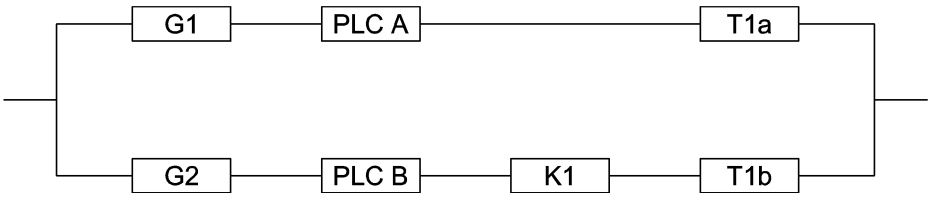


Bild E.8 — Sicherheitsbezogenes Blockdiagramm — SF 2

Für die SRP/CS wurde durch Anwendung des vereinfachten Verfahrens aus ISO 13849-1:2006, 4.5.4, ein PL bestimmt.

Das Diagramm kann der vorgesehenen Architektur für Kategorie 3 zugeordnet werden, so dass die Sicherheitsfunktion, wie in Bild E.9 dargestellt, durch ein SRP/CS ausgeführt wird.

Bild E.9 — SRP/CS, das die Sicherheitsfunktion SF 2 ausführt

Für die SRP/CS wurde durch Anwendung des vereinfachten Verfahrens aus ISO 13849-1:2006, 4.5.4, ein PL bestimmt.

b) **Bestimmung der $MTTF_d$ jedes Kanals**

Für die Bestimmung der $MTTF_d$-Werte der Bauteile wurden die Zuverlässigkeitsdaten des Herstellers verwendet.

Für die Bestimmung der $MTTF_d$ eines Kanals wurde das „Parts-Count"-Verfahren angewendet (siehe ISO 13849-1:2006, Anhang D). Der diversitäre redundante Aufbau führt zu unterschiedlichen $MTTF_d$-Werten für jeden Kanal, deshalb bietet die Anwendung der Symmetrisierungsgleichung ein Durchschnittsergebnis einer mittleren $MTTF_d$ (mehr als 25 Jahre) für jeden Kanal der SRP/CS.

c) **Bestimmung des DC_{avg}**

Der DC_{avg} für die SRP/CS wurde aus dem DC der internen Tests und den Überwachungsmaßnahmen für die verschiedenen Bauteilen bestimmt.

Es werden folgende Diagnosemaßnahmen realisiert:

— Überwachung des Hilfsschützes K1 durch PLC A über die Stellung der K1-Kontakte;

— Kreuzvergleich zwischen PLC A und PLC B;

— indirekte Überwachung von G1, T1a und PLC A durch PLC B über G2;

— Überwachung von T1b durch PLC A über die Stellung des Impulssperrrelais;

— Überwachung des Programmablaufs durch einen internen Watchdog in PLC A und in PLC B;

— indirekte Überwachung von G2 und PLC B durch PLC A über die Stellung der K1-Kontakte;

— Überwachung von G1 durch PLC A;

— Überwachung von G1 und T1a (Plausibilität der Sin/Cos-Werte);

— Überwachung von G2 durch PLC B (nach Betätigen von S4, führt PLC B eine Prüfung hinsichtlich Impulsen von G2 durch; sind keine Impulse vorhanden, schaltet PLC B T1b ab).

Nach ISO 13849-1:2006, Anhang E, bieten diese Diagnosemaßnahmen ein Ergebnis von DC_{avg} mittel (90 %) für die SRP/CS.

d) **Bestimmung der Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF)**

Es wird angenommen, dass geeignete Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (Trennung, Ungleichheit, Schutz gegen Überdruck, Umgebungsbedingungen) für die SRP/CS getroffen wurden, die nach ISO 13849-1:2006, Anhang F, einen Wert von 75 Punkten für die SRP/CS erreichen.

e) **Bestimmung des PL für die SRP/CS**

Der PL für die SRP/CS wird wie folgt bestimmt:

— Kategorie 3;

— mittlere $MTTF_d$ jedes Kanals;

— mittlerer DC_{avg};

— 75 Punkte für Maßnahmen gegen CCF.

Werden diese Werte nach ISO 13849-1:2006, Bild 5, ausgewertet, jedoch mit DC_{avg} begrenzt auf mittel (Kategorie 3), ergibt sich PL d.

f) **systematische Ausfälle**

Es wird angenommen, dass geeignete Maßnahmen nach ISO 13849-1:2006, Anhang G, gegen systematische Ausfälle bei den SRP/CS angewendet wurden.

E.4.4 Sicherheitsfunktion SF 3 — Selbsttätiger Rückstellungsbetrieb

Die Bewegung des Drehtisches (bei sicher reduzierter Geschwindigkeit) bei geöffneter verriegelter Schutzeinrichtung wird in Gang gesetzt und fortgeführt, solange der Taster S4 betätigt wird. Die Bewegung stoppt, wenn der Taster nicht mehr betätigt wird. Befindet sich der Taster in der unbetätigten Stellung, muss ein unerwartetes Wiederanlaufen verhindert werden. Das Signal des Tasters S4 wird in beiden PLCs verarbeitet.

a) **Identifikation der sicherheitsbezogenen Teile**

Die sicherheitsbezogenen Teile der Sicherheitsfunktion SF 3 und ihre Trennung in Kanäle kann durch das in Bild E.10 gezeigte sicherheitsbezogene Blockdiagramm dargestellt werden.

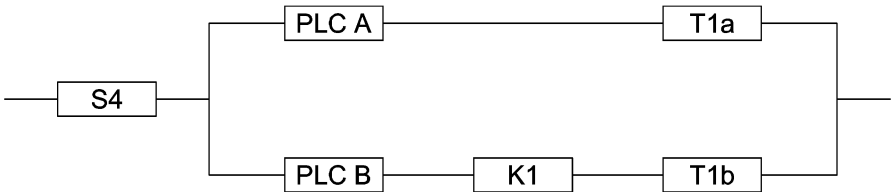


Bild E.10 — Sicherheitsbezogene Blockdiagramm von SF 3

Die beiden Teile des Diagramms können jeweils der vorgesehenen Architektur für Kategorie 1 und Kategorie 3 zugeordnet werden, so dass das Diagramm auf die beiden SRP/CS (Eingang, Logik/Ausgang), wie in Bild E.11 dargestellt, vereinfacht werden kann.

Bild E.11 — Kombination von SRP/CS, die die Sicherheitsfunktion SF 3 ausführen

Für jede SRP/CS wurde durch Anwendung des vereinfachten Verfahrens aus ISO 13849-1:2006, 4.5.4, ein PL bestimmt.

b) **Bestimmung der $MTTF_d$ jedes Kanals**

Die $MTTF_d$ für die SRP/CS_I (Taster für selbsttätigen Rückstellungsbetrieb) wird an Hand des B_{10d}-Wertes des Herstellers berechnet, um eine hohes Ergebnis für die $MTTF_d$ zu erhalten.

Die Bestimmung der $MTTF_d$ von $SRP/CS_{L/O}$ ergibt, wie bei $SRP/CS_{L/O}$ von SF 1.0, ein durchschnittliches Ergebnis von 25 Jahren (mittel) für die $MTTF_d$ (mehr als 25 Jahre) für jeden Kanal.

c) **Bestimmung des DC_{avg}**

Der DC_{avg} für beide SRP/CS wurde aus dem DC der internen Tests und den Überwachungsmaßnahmen für die verschiedenen Bauteilen berechnet.

Die zeitliche Überwachung des Tasters S4 für den selbsttätigen Rückstellungsbetrieb (Stellungswechsel ein/aus in einem Zeitfenster) durch PLC A und PLC B nach ISO 13849-1:2006, Anhang E, führt zu einem niedrigen DC_{avg} (75 %) für die SRP/CS_I.

Bei $SRP/CS_{L/O}$ von SF 3 werden die gleichen Überwachungsmaßnahmen wie für $SRP/CS_{L/O}$ von SF 1.0 angewendet, was zu einem mittleren DC_{avg} (90 %) für die $SRP/CS_{L/O}$ führt.

d) **Bestimmung der Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF)**

Es wird angenommen, dass geeignete Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (Trennung, Ungleichheit, Schutz gegen Überdruck, Umgebungsbedingungen) für jedes SRP/CS getroffen wurden, so dass nach ISO 13849-1:2006, Anhang F, einen Wert von 75 Punkten für beide SRP/CS erreicht wird.

e) **Bestimmung des PL für jedes SRP/CS**

Der PL für jedes SRP/CS wird wie folgt bestimmt:

SRP/CS_I:

— Kategorie 1;

— hohe $MTTF_d$ jedes Kanals.

Werden diese Werte nach ISO 13849-1:2006, Bild 5, ausgewertet, ergibt sich PL c.

$SRP/CS_{L/O}$:

— Kategorie 3;

— mittlere $MTTF_d$ jedes Kanals;

— mittlerer DC_{avg},

— 75 Punkte für Maßnahmen gegen CCF.

Werden diese Werte nach ISO 13849-1:2006, Bild 5, ausgewertet, ergibt sich PL d.

f) **Ermittlung des PL für die Kombination von SRP/CS, die SF 3 ausführen**

Entsprechend ISO 13849-1:2006, 6.3, und unter Berücksichtigung beider SRP/CS von SF 3, wird der PL für die gesamte Kombination von SRP/CS wie folgt ermittelt:

— $PL_{niedrig}$ = c;

— $N_{niedrig}$ = 1;

Der PL für die Kombination von SRP/CS für SF 3 ist daher PL c.

g) **systematische Ausfälle**

Es wird angenommen, dass geeignete Maßnahmen nach ISO 13849-1:2006, Anhang G, gegen systematische Ausfälle beider SRP/CS für SF 3 angewendet wurden.

E.5 Validierung

E.5.1 Allgemeines

Wie in E.1 angeführt, wurde das Beispiel auf die Validierung von Fehlverhalten und Mitteln zur Diagnose der Sicherheitsfunktionen SF 1.0 und SF 1.3 beschränkt.

Nach 9.2 und 9.3 wird die Validierung des Fehlverhaltens und der Mittel zur Diagnose durch eine Überprüfung der Entwicklungsdokumente, eine Ausfallanalyse und ergänzende Fehlereingabeprüfungen durchgeführt.

Folgende Schritte werden ausgeführt:

a) die Diagnosemaßnahmen und die damit geprüften/überwachten Bauteile (Komponenten, Blöcke) sind zu identifizieren;

b) der auf jede Diagnosemaßnahme (DC) übertragene DC-Wert für ein einzelnes Bauteil ist zu verifizieren;

c) das Fehlverhalten des Systems ist zu analysieren und die Prüffälle sind festzulegen;

d) die richtige Berechnung des DC_{avg} für jede SRP/CS ist zu überprüfen;

e) die erforderlichen Prüfungen sind durchzuführen, um die DC-Werte zu bestätigen.

E.5.2 Validierung von Fehlverhalten und DC_{avg}

Eine Überprüfung der Dokumentation (sicherheitsbezogenes Blockdiagramm und Liste der Diagnosemaßnahmen für die SRP/CS) bestätigt, dass

— die in den sicherheitsbezogenen Blockdiagrammen angegebenen Blöcke (Bauteile), die sich auf jedes SRP/CS und die Kombination von SRP/CS beziehen; sowie

— die Diagnosemaßnahmen und überwachten Bauteile,

die in der sinnvollen Gestaltung des Systems vorausgesetzt werden, für alle Sicherheitsfunktionen korrekt sind.

Mit einer Fehlermode- und Ausfallanalyse (FMEA) werden die DC-Werte, die jeder überwachten Einheit jedes SRP/CS zugewiesen wurden sowie das Fehlverhalten des Systems überprüft.

Da die Sicherheitsfunktion SF 1 sowohl das sicherheitsbezogene Abschalten als auch die nachfolgende Verhinderung eines unerwarteten Wiederanlaufs ausführen muss, wird die Ausfallanalyse für jedes zugehörige Bauteil in einer gesonderten Zeile für jede dieser Anforderungen betrachtet.

Für die Analyse wurden die entsprechenden Fehlerlisten in den Anhängen A, B, C und D verwendet.

Im Folgenden wird die FMEA für die Sicherheitsfunktionen SF 1.0 und SF 1.3 einschließlich der Prüffälle betrachtet.

E.5.3 FMEA und DC_{avg} für SF 1.0 und SF 1.3

E.5.3.1 SF 1.0

Um die Analyse von SF 1.0 zu erleichtern, ist das zugehörige sicherheitsbezogene Blockdiagramm in Bild E.12 noch einmal abgebildet:

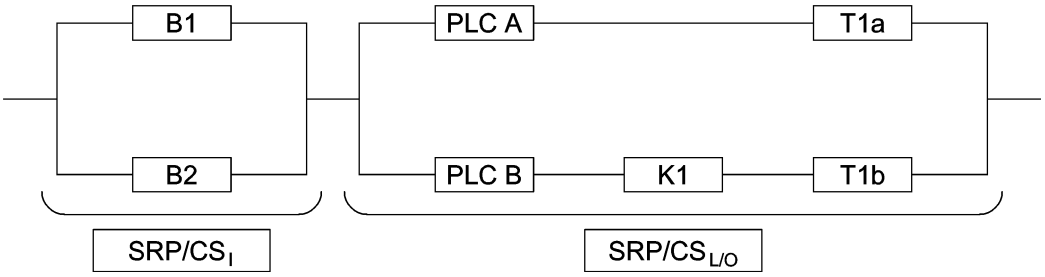


Bild E.12 — Sicherheitsbezogenes Blockdiagramm — SF 1.0

Siehe Tabelle E.3 und E.4

Tabelle E.3 — FMEA und Abschätzung des DC-Wertes für Bauteile von SRP/CS_I für SF 1.0

	Bauteil/ Einheit	Möglicher Ausfall	Fehlererkennung	Wirkung/ Reaktion	Prüfungen zur Bestätigung
F1	Verriegelungsschalter B1	Der Kontakt öffnet sich nicht, wenn die Schutzeinrichtung geöffnet wird (mechanische Fehler).[a]	Ein Fehler wird unabhängig von PLC A und PLC B erkannt durch eine Signaländerung in B2, wenn die Sicherheitsfunktion angefordert wird (Öffnen der Schutzeinrichtung, Plausibilitätsprüfung).	Der Elektromotor M1 wird über T1a durch die PLC A und über K1 und T1b durch die PLC B abgeschaltet und ein Wiederanlauf wird verhindert.	Am entsprechenden Eingang beider PLCs muss vor Öffnen der Schutzeinrichtung ein statischer High-Pegel angelegt werden.
F2		Kein gefährlicher Fehler während die Schutzeinrichtung offen ist (Fehlerausschluss).	—	—	—
Eine Plausibilitätsprüfung von B1 und B2 durch PLC A und PLC B ergibt einen DC-Wert von 99 % für B1 (siehe ISO 13849-1:2006, Tabelle E.1).					
F3	Verriegelungsschalter B2	Der Kontakt öffnet sich nicht, wenn die Schutzeinrichtung geöffnet wird (elektrische oder mechanische Fehler).	Ein Fehler wird unabhängig von PLC A und PLC B erkannt durch eine Signaländerung in B1, wenn die Sicherheitsfunktion angefordert wird (Öffnen der Schutzeinrichtung, Plausibilitätsprüfung).	Der Elektromotor M1 wird über T1a durch die PLC A und über K1 und T1b durch die PLC B abgeschaltet und ein Wiederanlauf wird verhindert.	Am entsprechenden Eingang beider PLCs muss vor Öffnen der Schutzeinrichtung ein statischer High-Pegel angelegt werden.
F4		Spontanes Schließen des Kontaktes, während die Schutzeinrichtung offen ist (mechanische Fehler).	Ein Fehler wird unabhängig und sofort von PLC A und PLC B erkannt, da es keine entsprechende Signaländerung in B 1 gibt.	Der Elektromotor M1 wird über T1a durch die PLC A und über K1 und T1b durch die PLC B abgeschaltet und ein Wiederanlauf wird verhindert.	Am entsprechenden Eingang beider PLCs muss ein statischer High-Pegel angeschlossen werden, während die Schutzeinrichtung geöffnet ist.
Eine Plausibilitätsprüfung von B1 und B2 durch PLC A und PLC B ergibt einen DC-Wert von 99 % für B2 (siehe ISO 13849-1:2006, Tabelle E.1).					
ANMERKUNG Leiter werden nicht in die Fehleranalyse einbezogen, da davon ausgegangen wird, dass sie nur aufgrund systematischer Ursachen ausfallen.					
[a] Elektrische Fehler können ausgeschlossen werden, da B1 über einen direkten Ansteuerungsmodus verfügt (siehe IEC 60947-5-1:2003, Anhang K).					

Anhand der Analyse kann geschlossen werden, dass alle Einzelfehler in den SRP/CS_l entweder sofort oder bei der nächsten Anforderung der Sicherheitsfunktion erkannt werden. Wenn ein Einzelfehler auftritt, wird die Sicherheitsfunktion immer ausgeführt und ein Wiederanlauf verhindert.

Infolge der Analyse wird vorausgesetzt, dass die angenommenen Werte für DC (hoch) bei der Gestaltung von B1 und B2 angemessen sind. Da der DC-Wert beider Bauteile gleich ist (99 %), ist der DC_{avg}-Wert von SRP/CS_l hoch (99 %), wie bereits während des Gestaltungsprozesses bestimmt wurde.

Diese Eigenschaften sind typisch für Kategorie 3, die bei der Gestaltung ausgewählt wurde (siehe E.4.1), um die in E.3 (PL_r-Werte) angegebene Festlegung der Anforderungen an die Sicherheitsfunktionen zu erfüllen.

Um die ordnungsgemäße Durchführung der Diagnosemaßnahmen zu überprüfen, könnten die in der letzten Spalte von Tabelle E.3 beschriebenen Prüfungen durchgeführt werden.

Tabelle E.4 — FMEA und Abschätzung des DC-Wertes für Bauteile von SRP/$CS_{L/O}$ für SF 1.0

	Bauteil/ Einheit	Mögliche Ausfälle	Fehlererkennung	Wirkung/ Reaktion	Prüfungen zur Bestätigung
F1	PLC A	Stuck-At-Fehler an der Eingabe-/-Ausgabekarte, oder Stuck-At-Fehler oder falsche Kodierung oder keine Ausführung im Prozessor, wodurch verhindert wird, dass die PLC A vor dem oder während des Öffnens der Schutzeinrichtung einen Abschaltbefehl an T1a sendet.	Ein Fehler wird von PLC B durch Lesen von G2 erkannt. Hierzu wird ein zeitbezogener Vergleich des eigenen Signals mit der erwarteten Änderung der Drehzahl durchgeführt. Einige Fehler (z. B. an Ausgabekarten) werden von der PLC A durch Lesen von G1 bei Betriebs-Aus des Elektromotors M1 oder wenn die Sicherheitsfunktion angefordert wird, erkannt. Weitere Fehler können frühzeitig von der internen Watchdog-Funktion (WD[a]) der PLC A erkannt werden.	Der Elektromotor M1 wird von PLC B über K1 und T1b nach einer Zeitverzögerung nach Öffnen der Schutzeinrichtung abgeschaltet und ein Wiederanlauf wird verhindert. Fehler, die von PLC A durch Lesen von G1 beim Betriebs-Aus erkannt werden, meldet PLC A an PLC B. Infolge der Meldung an PLC B wird der Elektromotor M1 abgeschaltet und ein Wiederanlauf wird durch PLC B verhindert. Bei Fehlern, die von der WD-Funktion erkannt werden, versucht PLC A, den Elektromotor M1 abzuschalten und den Wideranlauf über T1a zu verhindern, bevor die Sicherheitsfunktion angefordert wird oder bevor der Elektromotor M1 zum Betriebs-Aus kommt. Anschließend versucht PLC A die PLC B zu informieren.	Am Stopp-Ausgang von PLC A muss vor Öffnen der Schutzeinrichtung ein statischer High-Pegel angelegt werden
F2		Stuck-At-Fehler an der Eingabe-/-Ausgabekarte, oder Stuck-At-Fehler oder falsche Kodierung oder keine Ausführung im Prozessor, wodurch der Abschaltbefehl der PLC A von T1a zurückgesetzt wird, während die Schutzeinrichtung offen ist.	Fehler können nicht von PLC B durch Lesen von G2 erkannt werden, weil der Motor M1 durch PLC B über K1 und T1b abgeschaltet bleibt, während die Schutzeinrichtung offen ist. Einige Fehler (z. B. Ausgabekarten) werden von der PLC A durch Lesen von G1 beim Schließen der Schutzeinrichtung erkannt. Die oben genannten sowie zusätzliche Fehler werden von der Bedienperson durch Prozessbeobachtung beim Schließen der Schutzeinrichtung erkannt oder von PLC B, wenn die Sicherheitsfunktion als das nächste Mal angefordert wird (Öffnen der Schutzeinrichtung). Weitere Fehler können frühzeitig von der WD[a]-Funktion der PLC A erkannt werden.	Der Elektromotor M1 bleibt durch PLC B über K1 und T1b abgeschaltet, während die Schutzeinrichtung offen ist. Fehler, die von PLC A durch Lesen von G1 beim Schließen der Schutzeinrichtung erkannt werden, meldet PLC B an PLC A. Infolge der Meldung an PLC B wird das unbeabsichtigte Anlaufen des Elektromotors M1 durch PLC B verhindert. Bei Fehlern, die von der WD-Funktion erkannt werden, versucht PLC A, den Elektromotor M1 abgeschaltet zu halten und den Wiederanlauf über T1a zu verhindern, sowie PLC B zu informieren.	Übermitteln des Startsignals an den Umrichter, während die Schutzeinrichtung geöffnet ist.
Infolge der indirekten Überwachung von PLC A durch PLC B über G2, der indirekten Eigen-Überwachung der Ausgabekarte von PLC A durch G1, der Überwachung des Programmablaufs durch die interne Watchdog-Funktion und der Fehlererkennung durch die Prozessbeobachtung wird angenommen, dass PLC A einen DC von 90 % aufweist (siehe ISO 13849-1:2006, Tabelle E.1). Bei den oben genannten Werten kann davon ausgegangen werden, dass ISO 13849-1:2006, Tabelle E.1, Anmerkung 2, berücksichtigt wurde.					
ANMERKUNG Es wird berücksichtigt, dass die meisten PLC-Fehler an den Eingabe-/Ausgabekarten auftreten und dass es sich dabei um Stuck-At-Fehler handelt (90 % aller Fehler in einer PLC), aber die WD-Funktion kann nur einige Fehler erkennen, die den Programmablauf beeinträchtigen					

Tabelle E.4 *(fortgesetzt)*

	Bauteil/ Einheit	Mögliche Ausfälle	Fehlererkennung	Wirkung/ Reaktion	Prüfungen zur Bestätigung
F3	Umrichter T1a	Stuck-At-Fehler und weitere vielschichtige interne Fehler in der Steuer- und Leistungselektronik des Umrichters, die verhindern, dass T1a den Motor abschaltet, bevor oder wenn die Schutzeinrichtung geöffnet wird.	Ein Fehler wird von PLC B durch Lesen von G2 erkannt, wenn die Sicherheitsfunktion angefordert wird. Ein Fehler wird auch von PLC A durch Lesen von G1 bei einem Betriebs-Aus des Elektromotors M1 erkannt, oder wenn die Sicherheitsfunktion angefordert wird.	Der Elektromotor M1 wird von PLC B über K1 und T1b nach einer Zeitverzögerung nach Öffnen der Schutzeinrichtung abgeschaltet und ein Wiederanlauf wird verhindert. Wenn ein Fehler während des Betriebs-Aus erkannt wird, wird dies von PLC A an PLC B gemeldet. Infolge der Meldung an PLC B wird der Elektromotor M1 abgeschaltet und ein Wiederanlauf wird durch PLC B verhindert.	Der Stopp-Eingang des Umrichters wird auf high gesetzt, bevor oder während die Schutzeinrichtung geöffnet wird.
F4		Stuck-At-Fehler und weitere vielschichtige interne Fehler in der Steuer- und Leistungselektronik des Umrichters, wodurch Ansteuerungssignale für Leistungshalbleiter von T1a erzeugt werden, während die Schutzeinrichtung geöffnet ist.	Fehler können nicht von PLC B durch Lesen von G2 erkannt werden, weil der Motor M1 durch PLC B über K1 und T1b abgeschaltet bleibt, während die Schutzeinrichtung offen ist. Ein Fehler wird von der Bedienperson durch Prozessbeobachtung beim Schliessen der Schutzeinrichtung erkannt. Ein Fehler wird auch von PLC A durch Lesen von G1 beim Schließen der Schutzeinrichtung erkannt.	Der Elektromotor M1 bleibt durch PLC B über K1 und T1b abgeschaltet, während die Schutzeinrichtung offen ist. Beim Schließen der Schutzeinrichtung tritt ein unbeabsichtigter Wiederanlauf des Motors auf (ungefährlich). Wenn ein Fehler erkannt wurde, meldet PLC A dies an PLC B. Infolge der Meldung an PLC B wird ein unbeabsichtigtes Einschalten des Elektromotors M1 und ein Wiederanlauf durch PLC B verhindert.	Senden eines des Startsignals an den Umrichter, während die Schutzeinrichtung geöffnet ist.
Infolge der indirekten Überwachung von T1a durch PLC B über G2, der indirekten Überwachung von T1a durch PLC A über G1 und der Fehlererkennung durch Prozessbeobachtung wird angenommen, dass T1a einen DC-Wert von 99 % aufweist.					
F5	PLC B	Stuck-At-Fehler an der Eingabe-/-Ausgabekarte, oder Stuck-At-Fehler oder falsche Kodierung oder keine Ausführung im Prozessor, wodurch verhindert wird, dass die PLC B vor dem oder während des Öffnens der Schutzeinrichtung K1 abschaltet	Ein Fehler wird durch PLC A-Überwachung des zwangsgeführten K1-Rückmeldekontakts erkannt, wenn die Sicherheitsfunktion angefordert wird. Einige Fehler können frühzeitig von der WD[a]-Funktion der PLC B erkannt werden.	Der Elektromotor M1 wird von PLC A sofort über T1a abgeschaltet, wenn die Schutzeinrichtung geöffnet wird und der Wiederanlauf wird verhindert. Bei Fehlern, die von der WD-Funktion erkannt werden, versucht PLC B dies an PLC A zu melden und anschließend den Elektromotor M1 abzuschalten und den Wiederanlauf über T1b zu verhindern, bevor die Sicherheitsfunktion angefordert wird.	K1 wird in der spannungsführenden Stellung gehalten, während die Schutzeinrichtung geöffnet wird.
F6		Stuck-At-Fehler an der Eingabe-/-Ausgabekarte, oder Stuck-At-Fehler oder falsche Kodierung oder keine Ausführung im Prozessor, wodurch der Abschaltbefehl der PLC B von K1 zurückgesetzt wird, während die Schutzeinrichtung offen ist.	Ein Fehler wird sofort durch PLC A-Überwachung des zwangsgeführten K1-Rückmeldekontakts erkannt. Einige Fehler können frühzeitig von der WD[a]-Funktion der PLC B erkannt werden.	Der Elektromotor M1 bleibt durch PLC A über T1a abgeschaltet, während die Schutzeinrichtung offen ist, und ein Wiederanlauf wird verhindert. Bei Fehlern, die von der WD-Funktion erkannt werden, versucht PLC B, den Elektromotor M1 abgeschaltet zu halten und den Wiederanlauf über T1b zu verhindern, sowie PLC A zu informieren.	K1 wird in die spannungsführende Stellung geschaltet, während die Schutzeinrichtung offen ist.
Infolge der indirekten Überwachung von PLC B durch PLC A über die Stellung des K1-Rückmeldekontakts sowie infolge der Überwachung des Programmablaufs durch die interne Watchdog-Funktion, wird angenommen, dass PLC B einen DC von 90 % aufweist.					
ANMERKUNG Es wird berücksichtigt, dass die meisten PLC-Fehler an den Eingabe-/Ausgabekarten auftreten und dass es sich dabei um Stuck-At-Fehler handelt (90 % aller Fehler in einer PLC), aber die WD-Funktion einer PLC kann nur einige Fehler erkennen, die den Programmablauf beeinträchtigen.					

Tabelle E.4 *(fortgesetzt)*

	Bauteil/ Einheit	Mögliche Ausfälle	Fehlererkennung	Wirkung/ Reaktion	Prüfungen zur Bestätigung
F7	Hilfsschütz K1	Der Kontakt öffnet sich nicht, wenn die Schutzeinrichtung geöffnet wird (elektrischer Fehler, z. B. verschweißte Kontakte).	Ein Fehler wird durch PLC A-Überwachung des zwangsgeführten K1-Rückmeldekontakts erkannt, wenn die Sicherheitsfunktion angefordert wird.	Der Elektromotor M1 wird von PLC A sofort über T1a abgeschaltet, wenn die Schutzeinrichtung geöffnet wird und der Wiederanlauf wird verhindert.	Der K1-Kontakt wird in der EIN-Stellung gehalten, wenn die Schutzeinrichtung geöffnet wird.
F8		Kein gefährlicher Fehler während die Schutzeinrichtung offen ist (Fehlerausschluss)	—	—	—
Die Überwachung des Hilfsschützes K1 durch PLC A über die Stellung des zwangsgeführten K1-Rückmeldekontakts ergibt einen DC von 99 % für K1.					
F9	Umrichter T1b	Nichtöffnen des internen Relaiskontakts beim Öffnen der Schutzeinrichtung	Ein Fehler wird durch PLC A-Überwachung des zwangsgeführten Rückmeldekontakts für das interne Relais von T1b erkannt, wenn die Sicherheitsfunktion angefordert wird.	Der Elektromotor M1 wird von PLC A sofort über T1a abgeschaltet, wenn die Schutzeinrichtung geöffnet wird und der Wiederanlauf wird verhindert.	Der Eingang der Spule des Sperrrelais in T1b wird auf high gesetzt, wenn die Schutzeinrichtung geöffnet wird.
F10		Kein gefährlicher Fehler während die Schutzeinrichtung offen ist (Fehlerausschluss)	—	—	—
Die Überwachung des internen (Impulssperr-)-relais von T1b durch PLC A ergibt einen DC von 99 % für T1b.					

[a] Einige interne Fehler von PLCs, die nicht *von vornherein* zu einem Versagen der Sicherheitsfunktion führen (z. B. Unfähigkeit von PLCs, einen Abschaltbefehl an den Antrieb oder an ein Ventil zu senden, oder Unfähigkeit, einen Abschaltbefehl am Antrieb oder an einem Ventil aufrechtzuerhalten), können von der WD-Funktion erkannt werden.

Anhand der Analyse kann geschlossen werden, dass alle Einzelfehler in den SRP/CS entweder sofort oder bei einem Betriebs-Aus des Elektromotors M1 erkannt werden, oder bei der nächsten Anforderung der Sicherheitsfunktion. Wenn ein Einzelfehler auftritt, wird die Sicherheitsfunktion immer ausgeführt. Ein Wiederanlauf nur eines Kanals ist bei nicht erkannten Fehlern in PLC A und PLC B möglich.

Die Analyse ergibt, dass die DC-Werte, die während der Gestaltung der SRP/$CS_{L/O}$ angenommen wurden, angemessen sind. Bei Berücksichtigung der geschätzten $MTTF_d$-Werte und der DC-Werte für die verschiedenen in SRP/$CS_{L/O}$ verwendeten Bauteile wird ein DC_{avg}-Ergebnis von mittel (90 %) erreicht, wie bereits während der Gestaltung angenommen wurde.

Diese Eigenschaften sind typisch für Kategorie 3, die bei der Gestaltung ausgewählt wurde (siehe E.4.1), um die in E.3 (PL_r-Werte) angegebene Festlegung der Anforderungen an die Sicherheitsfunktionen zu erfüllen.

Um die ordnungsgemäße Durchführung der Diagnosemaßnahmen zu überprüfen, könnten die in der letzten Spalte von Tabelle E.4 beschriebenen Prüfungen durchgeführt werden.

E.5.3.2 SF 1.3

Um die Analyse von SF 1.3 zu erleichtern, ist das zugehörige sicherheitsbezogene Blockdiagramm in Bild E.13 noch einmal abgebildet.

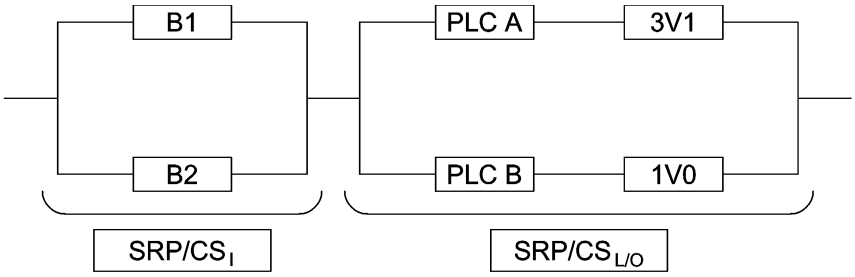


Bild E.13 — Sicherheitsbezogenes Blockdiagramm für SF 1.3

Für SRP/CS_I von SF 1.3 sind die Diagnosemaßnahmen und die geprüften/überwachten Bauteile identisch mit denen für SF 1.0 und daher ist der DC_{avg}-Wert von SRP/CS_I ebenfalls hoch (99 %).

Siehe Tabelle E.5.

Tabelle E.5 — FMEA von SRP/$CS_{L/O}$ für SF 1.3

	Bauteil/ Einheit	Mögliche Fehler/Ausfälle	Fehlererkennung	Wirkung/ Reaktion	Prüfungen zur Bestätigung
F1	PLC A	Stuck-At-Fehler an der Eingabe-/-Ausgabekarte, oder Stuck-At-Fehler oder falsche Kodierung oder keine Ausführung im Prozessor, wodurch verhindert wird, dass die PLC A vor dem oder während des Öffnens der Schutzeinrichtung 3V1 abschaltet	Einige Fehler (z. B. Ausgabekarten) werden von der PLC A durch Lesen von Drucksensor 3S1 bei Betriebs-Aus des Pneumatikmotors A3 oder wenn die Sicherheitsfunktion angefordert wird, erkannt. Weitere Fehler können frühzeitig von der internen Watchdog-Funktion (WD[a]) der PLC A erkannt werden.	Der Pneumatikmotor A3 wird von PLC B über 1V0 nach einer Zeitverzögerung nach Öffnen der Schutzeinrichtung abgeschaltet. Fehler, die von PLC A durch Lesen von 3S1 beim Betriebs-Aus erkannt werden, werden von PLC A an PLC B gemeldet. Infolge der Meldung an PLC B wird der Pneumatikmotor A3 über 3V1 abgeschaltet und ein Wiederanlauf wird durch PLC B verhindert. Bei Fehlern, die von der WD-Funktion erkannt werden, versucht PLC A, den Pneumatikmotor A3 abzuschalten und den Wideranlauf über 3V1 zu verhindern, bevor die Sicherheitsfunktion angefordert wird oder bevor der Pneumatikmotor A3 zum Betriebs-Aus kommt. Anschließend versucht PLC A dies an PLC B zu melden.	Am 3V1-Ausgang von PLC A muss vor Öffnen der Schutzeinrichtung ein statischer High-Pegel angelegt werden
F2		Stuck-At-Fehler an der Eingabe-/-Ausgabekarte, oder Stuck-At-Fehler oder falsche Kodierung oder keine Ausführung im Prozessor, wodurch die PLC A 3V1 einschaltet, während die Schutzeinrichtung offen ist.	Einige Fehler (z. B. Ausgabekarten) werden von der PLC A durch Lesen des Drucksensors 3S1 beim Schließen der Schutzeinrichtung erkannt. Weitere Fehler können frühzeitig von der WD[a]-Funktion der PLC A erkannt werden.	Der Pneumatikmotor A3 bleibt durch PLC B über 1V0 abgeschaltet, während die Schutzeinrichtung offen ist. Beim Schließen der Schutzeinrichtung schaltet PLC B 1V0 ein und der Pneumatikmotor A3 läuft wieder an (nicht gefährlich). Fehler, die von PLC A durch Lesen von 3S1 beim Schließen der Schutzeinrichtung erkannt werden, werden von PLC A an PLC B gemeldet. Infolge der Meldung an PLC B wird das unbeabsichtigte Anlaufen des Pneumatikmotors A3 sowie der Wiederanlauf durch PLC B verhindert. Bei Fehlern, die von der WD-Funktion erkannt werden, versucht PLC A, den Pneumatikmotor A3 abgeschaltet zu halten und den Wiederanlauf über 3V1zu verhindern, sowie dies an PLC B zu melden.	Der 3V1-Ausgang der PLC A ist auf einen High-Pegel zu legen, während die Schutzeinrichtung offen ist.
Infolge der indirekten Eigen-Überwachung der Ausgabekarte von PLC A durch 3S1 und der Überwachung des Programmablaufs durch die interne Watchdog-Funktion wird angenommen, dass PLC A einen DC von 90 % aufweist.					
ANMERKUNG Es wird berücksichtigt, dass die meisten PLC-Fehler an den Eingabe-/Ausgabekarten auftreten und dass es sich dabei um Stuck-At-Fehler handelt (90 % aller Fehler in einer PLC), aber die WD-Funktion einer PLC kann nur einige Fehler erkennen, die den Programmablauf beeinträchtigen.					

Tabelle E.5 *(fortgesetzt)*

	Bauteil/ Einheit	Mögliche Fehler/Ausfälle	Fehlererkennung	Wirkung/ Reaktion	Prüfungen zur Bestätigung
F3	elektromagnetisches Wegeventil 3V1	Nicht-Schalten (Hängenbleiben in der geschalteten Stellung) oder nicht vollständiges Zurückschalten (Hängenbleiben in einer beliebigen Zwischenstellung) oder Veränderung der Schaltzeiten, bevor oder während sich die Schutzeinrichtung öffnet.	Ein Fehler wird von PLC A durch Lesen des Drucksensors 3S1 bei einem Betriebs-Aus des Pneumatikmotors A3 erkannt, oder wenn die Sicherheitsfunktion abgefordert wird. Die Bedienperson kann Fehler auch durch Prozessbeobachtung feststellen.	Der Pneumatikmotor A3 wird von PLC B über 1V0 nach einer Zeitverzögerung nach Öffnen der Schutzeinrichtung abgeschaltet. PLC A meldet an PLC B, wenn ein Fehler erkannt wurde. Infolge dieser Meldung schaltet PLC B den Pneumatikmotor A3 über 1V0 ab und ein Wiederanlauf wird verhindert.	Beim Öffnen der Schutzeinrichtung sind die elektrischen und pneumatischen Steuersignale für 3V1 auf High-Level zu legen.
F4		selbsttätige Veränderung der Ausgangs-Schaltstellung (ohne Eingangssignal), während die Schutzeinrichtung offen ist. ANMERKUNG Dieser Fehler kann ausgeschlossen werden, da in 3V1 bewährte Federn verwendet und übliche Einbau- und Betriebsbedingungen angewendet werden.	—	—	—
Infolge der indirekten Überwachung von 3V1 durch PLC A über 3S1 und der Fehlererkennung durch Prozessbeobachtung wird angenommen, dass 3V1a einen DC-Wert von 99 % aufweist.					
F5	PLC B	Stuck-At-Fehler an der Eingabe-/-Ausgabekarte, oder Stuck-At-Fehler oder falsche Kodierung oder keine Ausführung im Prozessor, wodurch verhindert wird, dass die PLC B vor dem oder während des Öffnens der Schutzeinrichtung 1V0 abschaltet.	Einige Fehler (z. B. Ausgabekarten) werden von der PLC B durch Lesen von Druckschalter 1S0 erkannt, wenn die Sicherheitsfunktion angefordert wird. Weitere Fehler können frühzeitig von der Wd[a]-Funktion der PLC B erkannt werden.	Der Pneumatikmotor A3 wird von PLC A sofort über 3V1 abgeschaltet, wenn die Schutzeinrichtung geöffnet wird. Fehler, die von PLC B durch Lesen des Druckschalters 1S0 erkannt werden, werden von PLC B an PLC A gemeldet und PLC B hält K1 deaktiviert. Infolge dieser Meldung verhindert PLC A einen Wiederanlauf. Fehler, die von der WD-Funktion erkannt werden, versucht PLC B an PLC A zu melden und anschließend den Pneumatikmotor A3 über 1V0 abzuschalten und den Wiederanlauf zu verhindern, bevor die Sicherheitsfunktion angefordert wird.	Am 1V0-Ausgang der PLC B ist ein statischer High-Pegel anzulegen, bevor die Schutzeinrichtung geöffnet wird.

Tabelle E.5 *(fortgesetzt)*

	Bauteil/ Einheit	Mögliche Fehler/Ausfälle	Fehlererkennung	Wirkung/ Reaktion	Prüfungen zur Bestätigung
F6	PLC B	Stuck-At-Fehler an der Eingabe-/-Ausgabekarte, oder Stuck-At-Fehler oder falsche Kodierung oder keine Ausführung im Prozessor, wodurch PLC B 1V0 einschaltet, während die Schutzeinrichtung offen ist.	Einige Fehler (z. B. Ausgabekarten) werden von der PLC B sofort durch Lesen von Druckschalter 1S0 erkannt. Weitere Fehler können frühzeitig von der WD[a]-Funktion der PLC B erkannt werden.	Der Pneumatikmotor A3 bleibt durch PLC A über 3V1 abgeschaltet, während die Schutzeinrichtung offen ist. Fehler, die von PLC B durch Lesen des Druckschalters 1S0 erkannt werden, meldet PLC B an PLC A und hält K1 deaktiviert. Infolge dieser Meldung verhindert PLC A einen Wiederanlauf. Fehler, die von der WD-Funktion erkannt werden, versucht PLC B an PLC A zu melden und anschließend den Pneumatikmotor A3 über 1V0 abgeschaltet zu halten und den Wiederanlauf zu verhindern.	Der 1V0-Ausgang der PLC B ist auf einen High-Pegel zu legen, während die Schutzeinrichtung offen ist.
Infolge der indirekten Eigen-Überwachung der Ausgabekarte von PLC B durch 1S0, der indirekten Überwachung von PLC B durch PLC A über die Stellung des K1-Rückmeldekontakts sowie infolge der Überwachung des Programmablaufs durch die interne Watchdog-Funktion, wird angenommen, dass PLC B einen DC von 90 % aufweist.					
ANMERKUNG Es wird berücksichtigt, dass die meisten PLC-Fehler an den Eingabe-/Ausgabekarten auftreten und dass es sich dabei um Stuck-At-Fehler handelt (90 % aller Fehler in einer PLC), aber die WD-Funktion einer PLC kann nur einige Fehler erkennen, die den Programmablauf beeinträchtigen.					
F7	Magnet ventil 1V0	Nicht-Schalten (Hängenbleiben in der geschalteten Stellung) oder nicht vollständiges Zurückschalten (Hängenbleiben in einer beliebigen Zwischenstellung) oder Veränderung der Schaltzeiten, bevor oder während sich die Schutzeinrichtung öffnet.	Ein Fehler wird von PLC B durch Lesen des Druckschalters 1S0 erkannt, wenn die Sicherheitsfunktion angefordert wird.	Der Pneumatikmotor A3 wird von PLC A sofort über 3V1 abgeschaltet, wenn die Schutzeinrichtung geöffnet wird. Fehler, die von PLC B durch Lesen des Druckschalters 1S0 erkannt werden, meldet PLC B an PLC A und hält K1 deaktiviert. Infolge dieser Meldung verhindert PLC A einen Wiederanlauf.	Am 1V0-Ausgang der PLC B ist ein statischer High-Pegel anzulegen, bevor die Schutzeinrichtung geöffnet wird.
F8	Magnet-ventil 1V0	selbsttätige Veränderung der Ausgangs-Schaltstellung (ohne Eingangssignal), während die Schutzeinrichtung offen ist. ANMERKUNG Dieser Fehler kann ausgeschlossen werden, da in 1V0 bewährte Federn verwendet und übliche Einbau- und Betriebsbedingungen angewendet werden.	—	—	—
Die indirekte Überwachung von 1V0 durch PLC B über 1S0 ergibt einen DC von 99 % für 1V0.					

[a] Einige interne Fehler von PLCs, die nicht *von vornherein* zu einem Versagen der Sicherheitsfunktion führen (z. B. Unfähigkeit von PLCs, einen Abschaltbefehl an den Antrieb oder an ein Ventil zu senden, oder Unfähigkeit, einen Abschaltbefehl am Antrieb oder an einem Ventil aufrechtzuerhalten), können von der WD-Funktion erkannt werden.

Anhand der Analyse kann geschlossen werden, dass die meisten Einzelfehler in den SRP/CS entweder sofort oder bei einem Betriebs-Aus des Pneumatikmotors A3 erkannt werden, oder bei der nächsten Anforderung der Sicherheitsfunktion. Wenn ein Einzelfehler auftritt, wird die Sicherheitsfunktion immer ausgeführt. Ein Wiederanlauf nur eines Kanals ist bei nicht erkannten Fehlern in PLC A und PLC B möglich.

Die Analyse ergibt, dass die DC-Werte, die während der Gestaltung der SRP/$CS_{L/O}$ angenommen wurden, angemessen sind. Bei Berücksichtigung der geschätzten $MTTF_d$-Werte und der DC-Werte für die verschiedenen in SRP/$CS_{L/O}$ verwendeten Bauteile wird ein DC_{avg}-Ergebnis von mittel (90 %) erreicht, wie bereits während der Gestaltung angenommen wurde.

Diese Eigenschaften sind typisch für Kategorie 3, die bei der Gestaltung ausgewählt wurde (siehe E.4.1), um die in E.3 (PL_r-Werte) angegebene Festlegung der Anforderungen an die Sicherheitsfunktionen zu erfüllen.

Um die ordnungsgemäße Durchführung der Diagnosemaßnahmen zu überprüfen, könnten die in der letzten Spalte der Tabelle E.5 beschriebenen Prüfungen durchgeführt werden.

Anhang ZA
(informativ)

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

Diese Europäische Norm wurde im Rahmen eines Mandates, das dem CEN von der Europäischen Kommission und der Europäischen Freihandelszone erteilt wurde, erarbeitet, um ein Mittel zur Erfüllung der grundlegenden Anforderungen der Richtlinie nach der neuen Konzeption 2006/42/EG Maschinenrichtlinie bereitzustellen.

Sobald diese Norm im Amtsblatt der Europäischen Union im Rahmen der betreffenden Richtlinie in Bezug genommen und in mindestens einem der Mitgliedstaaten als nationale Norm umgesetzt worden ist, berechtigt die Übereinstimmung mit den normativen Abschnitten dieser Norm innerhalb der Grenzen des Anwendungsbereichs dieser Norm zu der Annahme, dass eine Übereinstimmung mit den entsprechenden grundlegenden Anforderungen in 1.2.1 der Richtlinie und der zugehörigen EFTA-Vorschriften gegeben ist.

WARNHINWEIS — Für Produkte, die in den Anwendungsbereich dieser Norm fallen, können weitere Anforderungen und weitere EU-Richtlinien anwendbar sein.

Literaturhinweise

[1] ISO 4079-1, *Rubber hoses and hose assemblies — Textile-reinforced hydraulic types — Specification — Part 1: Oil-based fluid applications*

[2] ISO 4413:2010, *Hydraulic fluid power — General rules and safety requirements for systems and their components*

[3] ISO 4414:2010, *Pneumatic fluid power — General rules and safety requirements for systems and their components*

[4] ISO 4960, *Cold-reduced carbon steel strip with a mass fraction of carbon over 0,25 %*

[5] ISO 5598:2008, *Fluid power systems and components — Vocabulary*

[6] ISO 11161, *Safety of machinery — Integrated manufacturing systems — Basic requirements*

[7] ISO 13850, *Safety of machinery — Emergency stop — Principles for design*

[8] ISO 13851, *Safety of machinery — Two-hand control devices — Functional aspects and design Principles*

[9] ISO 13855, *Safety of machinery — Positioning of safeguards with respect to the approach speeds of parts of the human body*

[10] ISO 13856 (alle Teile), *Safety of machinery — Pressure-sensitive protective devices*

[11] ISO 14118:2000, *Safety of machinery — Prevention of unexpected start-up*

[12] ISO 14119:1998, *Safety of machinery — Interlocking devices associated with guards — Principles for design and selection*

[13] IEC 60204-1:2005, *Safety of machinery — Electrical equipment of machines — Part 1: General requirements*

[14] IEC 60269-1, *Low-voltage fuses — Part 1: General requirements*

[15] IEC 60529, *Degrees of protection provided by enclosures (IP code)*

[16] IEC 60664 (alle Teile), *Insulation coordination for equipment within low-voltage systems*

[17] IEC 60812, *Analysis techniques for system reliability — Procedure for failure mode and effects analysis (FMEA)*

[18] IEC 60893-1, *Insulating materials — Industrial rigid laminated sheets based on thermosetting resins for electrical purposes — Part 1: Definitions, designations and general requirements*

[19] IEC 60947 (alle Teile), *Low-voltage switchgear and controlgear*

[20] IEC 61025, *Fault tree analysis (FTA)*

[21] IEC 61078, *Analysis techniques for dependability — Reliability block diagram and boolean methods*

[22] IEC 61131-1, *Programmable controllers — Part 1: General information*

[23] IEC 61131-2, *Programmable controllers — Part 2: Equipment requirements and tests*

[24] IEC 61165, *Application of Markov techniques*

[25] IEC 61249 (alle Teile), *Materials for printed boards and other interconnecting structures*

[26] IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems*

[27] IEC 61558 (alle Teile), *Safety of power transformers, power supplies, reactors and similar products*

[28] IEC 61800-5-2, *Adjustable speed electrical power drive systems — Part 5-2: Safety requirements — Functional*

[29] IEC 61810 (alle Teile), *Electromechanical elementary relays*

[30] EN 952:1996, *Sicherheit von Maschinen — Sicherheitstechnische Anforderungen an fluidtechnische Anlagen und deren Bauteile — Hydraulik*

[31] EN 953:1996, *Sicherheit von Maschinen — Sicherheitstechnische Anforderungen an fluidtechnische Anlagen und deren Bauteile — Pneumatik*

[32] EN 50205, *Relais mit (mechanisch) zwangsgeführten Kontakten*

[33] EN 60730 (alle Teile), *Automatische und elektrische Regel- und Steuergeräte für den Hausgebrauch und ähnliche Anwendungen*

[34] JESD22A121.01, *Test Method for Measuring Whisker Growth on Tin and Alloy Surfaces Finishes*[1)]

[35] JESD201, *Environmental Acceptance Requirements for Tin Whisker Susceptibility of Tin and Alloy Surface Finishes*[1)]

1) JEDEC Solid State Technology Association, 2500 Wilson Boulevard, Arlington, VA 22201-3834, www.jedec.org/download/search/22a1121-01.pdf