DEUTSCHE NORM **Entwurf** Juni 2010

DIN EN ISO 13849-2

DIN

ICS 13.110

Entwurf

Einsprüche bis 2010-08-07
Vorgesehen als Ersatz für
DIN EN ISO 13849-2:2008-09
und
DIN EN ISO 13849-2
Berichtigung 1:2009-01

Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung (ISO/DIS 13849-2:2010); Deutsche Fassung prEN ISO 13849-2:2010

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

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

Anwendungswarnvermerk

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

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

Stellungnahmen werden erbeten

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

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

Gesamtumfang 91 Seiten

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

Preisgruppe 29
www.din.de
www.beuth.de

1632341

Beginn der Gültigkeit

Diese Norm gilt ab ...[1)]

Nationales Vorwort

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

Dieses Dokument enthält die Deutsche Fassung des vom Technischen Komitees ISO/TC 199 „Safety of machinery“ des Internationalen Komitees für Normung (ISO) in Zusammenarbeit mit dem Technischen Komitee CEN/TC 114 „Sicherheit von Maschinen und Geräten“ des Europäischen Komitees für Normung (CEN) entsprechend der Vereinbarung zwischen dem CEN und ISO über die technische Zusammenarbeit (Wiener Vereinbarung) ausgearbeiteten Norm-Entwurfs prEN ISO 13849-2:2010. Die Sekretariate beider Technischer Komitees werden vom DIN (Deutschland) gehalten.

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

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

In Abschnitt 2 angegebene Normen

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

Im Verzeichnis „Literaturhinweise“ angegebene Normen

ISO/DIS 4413	siehe	E DIN EN ISO 4413
ISO/DIS 4414	siehe	E DIN EN ISO 4414
ISO 4960	siehe	DIN EN 10140 (modifizierte Übernahme)
ISO 5598	keine nationale Entsprechung	
ISO 11161	siehe	DIN EN ISO 11161
ISO 12100-2	siehe	DIN EN ISO 12100-2
ISO 13850	siehe	DIN EN ISO 13850
ISO 13851	siehe	DIN EN 574
ISO 13856-Reihe	siehe	DIN EN 1760-Reihe
ISO 14118	siehe	DIN EN 1037
ISO 14119	siehe	DIN EN 1088
IEC 60204-1	siehe	DIN EN 60204-1 (modifizierte Übernahme)
IEC 60269-1	siehe	DIN EN 60269-1
IEC 60529	siehe	DIN EN 60529
IEC 60664-Reihe	siehe	DIN EN 60664-Reihe
IEC 60812	siehe	DIN EN 60812
IEC 60947-Reihe	siehe	DIN EN 60947-Reihe
IEC 61025	siehe	DIN EN 61025

1) Wird bei Herausgabe als Norm festgelegt.

IEC 61078	siehe	DIN EN 61078
IEC 61165	siehe	DIN EN 61165
IEC 61249-2	siehe	DIN EN 61249-2
IEC 61558-Reihe	siehe	DIN EN 61558-Reihe
IEC 61810-Reihe	siehe	DIN EN 61810-Reihe

Änderungen

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

a) Anpassung der Anforderungen und Terminologie an die aktuelle Ausgabe ISO 13849-1:2006;

b) Aktualisierung der Verweise;

c) Analyse und Prüfung des Performance Levels (PL) nach ISO 13849-1:2006 ergänzt;

d) teilweise neue Benummerung der Abschnitte durch Aufnahme eines Abschnittes 3 „Begriffe“ und 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.

Nationaler Anhang NA (informativ)

Literaturhinweise

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

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

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

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

DIN EN 10140, *Kaltband — Grenzabmaße und Formtoleranzen*

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

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

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

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

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

DIN EN 60947 (alle Teile), *Niederspannungsschaltgeräte*

DIN EN 61025, *Fehlzustandsbaumanalyse*

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

DIN EN 61165, *Anwendung des Markoff-Verfahrens*

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

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

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

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

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

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

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

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

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

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

— Entwurf —

CEN/TC 114

Datum: 2010-03

prEN ISO 13849-2:2010

CEN/TC 114

Sekretariat: DIN

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

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

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

ICS:

Deskriptoren

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

— Entwurf —

Inhalt

Seite

Vorwort

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

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

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

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

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

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

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

— *Teil 1: Allgemeine Gestaltungsleitsätze*

— *Teil 2: Validierung*

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

Tabelle 1 — Gliederung der Abschnitte der Anhänge A bis D

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

Dieses Dokument enthält Literaturhinweise.

Anerkennungsnotiz

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

Einleitung

Dieses Dokument ist eine Typ-B-Norm ,wie in ISO 12100-1 angegeben.

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

Für Maschinen, die in den Anwendungsbereich einer Typ-C-Norm fallen und die nach den Anforderungen dieser Typ-C-Norm konstruiert und hergestellt worden sind, haben die Anforderungen der Typ-C-Norm Vorrang. Diese Internationale Norm legt das Validierungsverfahren, einschließlich sowohl Analyse als auch Prüfung, für die Sicherheitsfunktionen, Kategorien und Performance Levels von sicherheitsbezogenen Teilen von Steuerungen fest. Die meisten der Verfahren und Bedingungen in dieser Internationalen Norm beruhen auf der Annahme, dass das in ISO 13849-1:2006, 4.5.4 beschriebene vereinfachte Verfahren zur Abschätzung des Performance Level (PL) angewendet wird. Wird ein anderes Verfahren angewendet (z.B. das Markov-Modell), können einige Teile dieser Norm möglicherweise nicht angewendet werden und es können zusätzliche Anforderungen notwendig sein. Diese Norm gibt keine Anleitung für den besonderen Fall, wenn andere Verfahren zur Abschätzung des PL angewendet werden.

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

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

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

1 Anwendungsbereich

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

— die vorgesehenen Sicherheitsfunktionen, und

— die ausgeführten Kategorien, und

— den erreichten Performance Level

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

ANMERKUNG Anforderungen für programmierbare elektronische Systeme einschließlich der damit verbundenen Software sind in ISO 13849-1:2006, 4.6 und in den Normen der Reihe IEC 61508 enthalten.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO 12100-1, *Safety of machinery — Basic concepts, general principles for design — Part 1: Basic terminology, methodology*

ISO 13849-1:2006, *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*

3 Begriffe

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

4 Validierungsverfahren

4.1 Validierungsleitsätze

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

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

— den festgelegten Sicherheitseigenschaften der Sicherheitsfunktionen für diesen Teil, wie in der sinnvollen Gestaltung realisiert;

— den Anforderungen für den festgelegte Performance Level (siehe ISO 13849-1:2006, 4.5);

— den Anforderungen für die festgelegte Kategorie (siehe ISO 13849-1:2006, 6.2);

— Maßnahmen zur Steuerung und zur Vermeidung systematischer Ausfälle (siehe ISO 13849-1:2006, Anhang G), und

— falls vorhanden, die Anforderungen an die Software (siehe ISO 13849-1:2006, 4.6);

— die Fähigkeit, eine Sicherheitsfunktion unter den erwarteten Umgebungsbedingungen zu leisten.

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

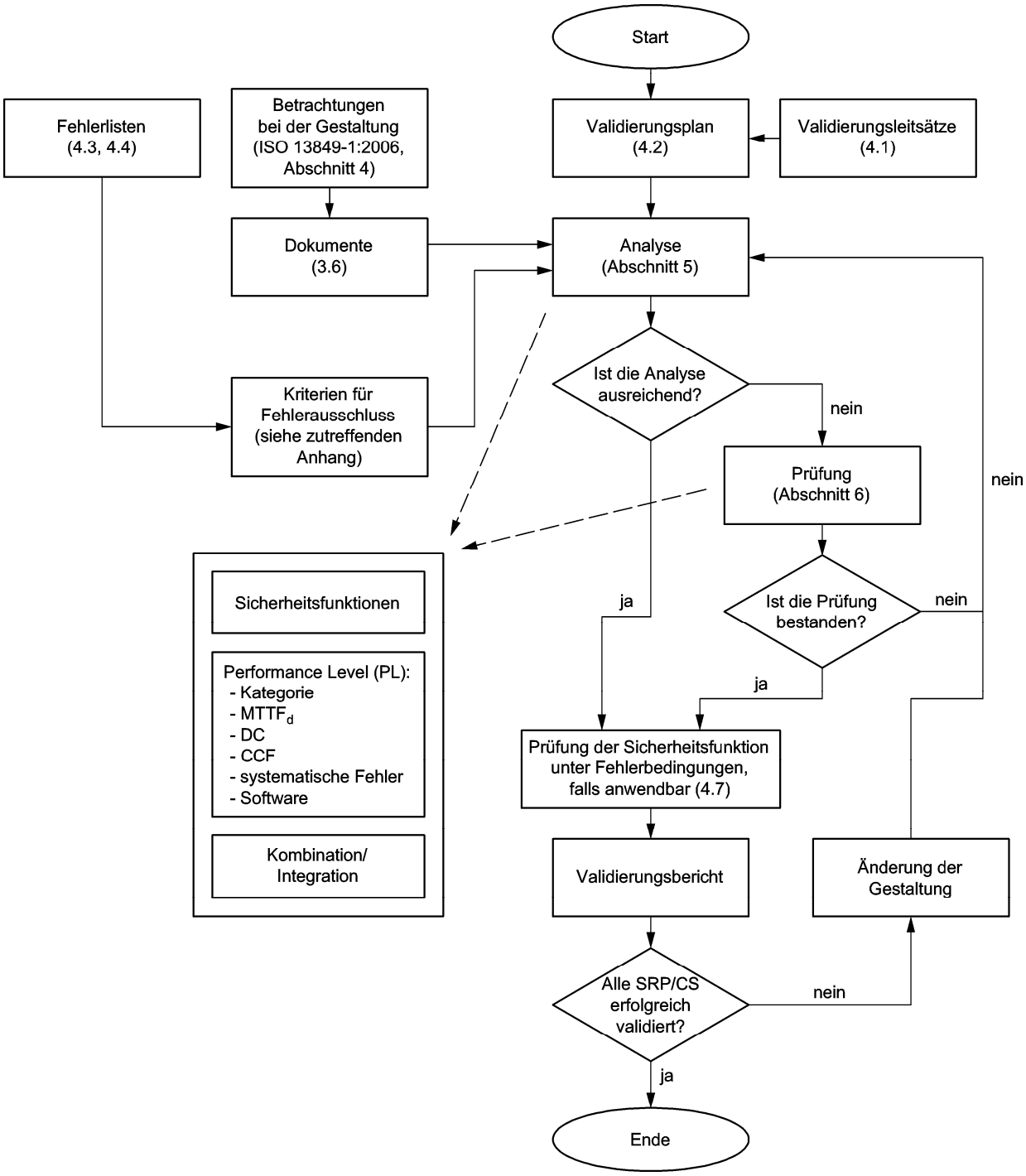
Die Validierung besteht aus der Durchführung der Analyse und aus der Durchführung von Funktionsprüfungen unter normalen Bedingungen in Übereinstimmung mit dem Validierungsplan. Bild 1 gibt einen Überblick über das Validierungsverfahren. Die Abwägung zwischen Analyse und Prüfung hängt von der Technologie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

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

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

— die Validierung der SRP/CS gesondert vor dem Einbau einschließlich der Simulation der angemessenen Eingangs- und Ausgangssignale;

— die Validierung der Auswirkungen bei Integration der sicherheitsbezogenen Teile in den Rest der Steuerung in Übereinstimmung mit ihrer Anwendung in der Maschine.



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

Bild 1 — Übersicht über das Validierungsverfahren

4.2 Validierungsplan

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

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

a) die Identität der Dokumente für die Festlegungen;

b) die Betriebs- und Umgebungsbedingungen während der Prüfung;

c) die anzuwendenden Analysen und Prüfungen;

d) den Verweis auf anzuwendende Prüfnormen;

e) die für jeden Teil der Validierung verantwortlichen Personen oder Parteien.

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

4.3 Allgemeine Fehlerlisten

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

— die einzubeziehenden Bauteile/Elemente, z. B. Leiter/ Kabel (siehe D.5.2);

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

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

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

In den Fehlerlisten sind nur permanente Fehler berücksichtigt.

4.4 Spezielle Fehlerlisten

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

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

— die aus der/n allgemeinen Liste(n) einbezogenen Fehler;

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

— die aus der/n allgemeinen Liste(n) entnommenen Fehler, die auf der Grundlage ausgeschlossen werden dürfen, dass die in den allgemeinen Listen enthaltenen (siehe ISO 13849-1:2006, 7.3) Kriterien befriedigt sind;

und, ausnahmsweise

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

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

4.5 Angaben zur Validierung

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

a) Spezifikation über die erforderliche Leistungsfähigkeit jeder Sicherheitsfunktion und ihre/n erforderliche Kategorie und Performance Level;

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

c) Blockdiagramm(e) mit Funktionsbeschreibung der Blöcke;

d) Steuerkreisdiagramm(e) einschließlich ihrer Verknüpfungen/Verbindungen;

e) Funktionsbeschreibung der Steuerkreisdiagramme;

f) Zeitfolgediagramm(e) für schaltende Bauteile, für Signale, die für die Sicherheit zuständig sind;

g) Beschreibung der entsprechenden Eigenschaften von früher validierten Bauteilen;

h) für andere sicherheitsbezogene Teile (ausgenommen der unter g) aufgelisteten) die Bauteillisten mit Stückbezeichnung, Nennwerten, Toleranzen, wesentlichen Betriebsbeanspruchungen, Typ-Bezeichnungen, Daten über Fehlerraten und Bauteilhersteller und alle anderen Daten, die für die Sicherheit maßgebend sind;

i) Analyse aller relevanten Fehler (siehe auch 4.2), die z. B. in A.5, B.5, C.5 und D.5 aufgelistet sind, einschließlich der Begründung aller ausgeschlossenen Fehler;

j) Analyse des Einflusses der im Verfahren verwendeten Werkstoffe;

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

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

1) eine Spezifikation, die klar und eindeutig ist, und die das Erreichen der geforderten sicherheitstechnischen Leistungsfähigkeit der Software bestätigt, und

2) den Beweis, dass die Software so gestaltet ist, dass sie den erforderlichen Performance Level erreicht, und

3) Einzelheiten über Prüfungen (insbesondere Prüfberichte), die durchgeführt wurden, um zu bestätigen, dass die geforderte sicherheitstechnische Leistungsfähigkeit erreicht wurde.

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

1) ein sicherheitsbezogenes Blockdiagramm (siehe ISO 13849-1:2006, Anhang B) oder vorgesehene Architektur (siehe ISO 13849-1:2006, 6.2);

2) die Bestimmung von $MTTF_d$ (mittlere Zeit bis zum gefahrbringenden Ausfall), DC_{avg} (durchschnittlicher Diagnosedeckungsgrad) und CCF (Ausfall infolge gemeinsamer Ursache);

3) die Bestimmung der Kategorie (siehe Tabelle 2).

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

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

Tabelle 2 — Anforderungen an die Dokumentation für Kategorien als Teil des Performance Levels

Anforderungen an die Dokumentation	Kategorie, für die eine Dokumentation erforderlich ist				
	B	1	2	3	4
grundlegende Sicherheitsprinzipien	X	X	X	X	X
zu erwartende Betriebsbeanspruchungen	X	X	X	X	X
Einfluss der zu verarbeitenden Werkstoffe	X	X	X	X	X
Leistungsfähigkeit während anderer wesentlicher äußerer Einflüsse	X	X	X	X	X
bewährte Bauteile	–	X	–	–	–
bewährte Sicherheitsprinzipien	–	X	X	X	X
mittlere Zeit bis zum gefahrbringenden Ausfall ($MTTF_d$) jeden Kanals	X	X	X	X	X
das Prüfverfahren für die Sicherheitsfunktion(en)	–	–	X	–	–
durchgeführte Diagnosemaßnahmen einschließlich Fehlerreaktion	–	–	X	X	X
Prüfintervalle, wenn festgelegt	–	–	X	X	X
Diagnosedeckungsgrad (DC_{avg})	–	–	X	X	X
bei der Gestaltung berücksichtigte vorhersehbare Einzelfehler und das angewendete Erkennungsverfahren	–	–	X	X	X
die erkannten Fehler gemeinsamer Ursache und wie sie verhindert werden	–	–	X	X	X
die vorhersehbaren ausgeschlossenen Einzelfehler	–	–	–	X	X
Fehler, die zu erkennen sind	–	–	X	X	X
verschiedene Fehleranhäufungen, die bei der Gestaltung zu berücksichtigen sind	–	–	–	–	X
wie die Sicherheitsfunktion in jedem Fehlerfall aufrechterhalten bleibt	–	–	–	X	X
wie die Sicherheitsfunktion bei allen Fehlerkombinationen aufrechterhalten bleibt	–	–	–	–	X
Maßnahmen gegen systematische Fehler	X	X	X	X	X
Maßnahmen gegen Softwarefehler	X	–	X	X	X

X Dokumentation ist erforderlich
– Dokumentation ist nicht erforderlich

ANMERKUNG Die in Tabelle 2 erwähnten Kategorien entsprechen denen, die in ISO 13849-1:2006 angegeben sind.

4.6 Validierungsaufzeichnung

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

Für jedes sicherheitsbezogene Teil, das einen Teil des Validierungsverfahrens nicht bestanden hat, muss die Aufzeichnung den Teil (die Teile) beschreiben, die die Validierungsprüfungen und/oder -analysen nicht bestanden haben. Es muss sichergestellt sein, dass sämtliche Teile nach der Veränderung erfolgreich neu validiert werden.

5 Validierung durch Analyse

5.1 Allgemeines

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

— die erkannten Sicherheitsfunktion(en) und den/die erforderlichen Performance Level, die sich bei der Risikoanalyse an der Maschine ergeben (siehe ISO 13849-1:2006, Bild 1 und 3);

— die Zuverlässigkeit ($MTTF_d$, DC_{av} und CCF) (siehe ISO 13849-1:2006, 4.2 bis 4.5);

— die Systemstruktur (z. B. vorgesehene Architektur) (siehe ISO 13849-1:2006, 4.2 bis 4.5, Abschnitt 6);

— die nicht quantifizierbaren qualitativen Aspekte, die Auswirkung auf das Systemverhalten haben (siehe ISO 13849-1:2006, 4.2 bis 4.5);

— deterministische Argumente.

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

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

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

5.2 Analysentechniken

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

a) „Top-down“ (deduktive) Techniken sind zur Bestimmung der Ursachen geeignet, die zu den festgestellten Ausgangsereignissen führen können und zur Abschätzung der Wahrscheinlichkeit von Ausgangsereignissen abhängig von der Wahrscheinlichkeit der Ursachen. Sie können auch angewendet werden bei der Untersuchung der Folgen von erkannten Mehrfachfehlern. Beispiele für „top-down“-Techniken sind die Fehlerbaumanalyse (FTA – siehe IEC 61025) und die Ereignisbaumanalyse (ETA).

b) „Bottom-up“ (induktive) Techniken sind für die Untersuchung der Folgen von festgestellten Einzelfehlern geeignet. Beispiele für „bottom-up“-Techniken sind die Ausfallarten- und Effektanalyse (FMEA - siehe IEC 60812) und die Fehlerarten, Auswirkungs- und kritischen Zustandsanalyse (FMECA).

6 Validierung durch Prüfen

6.1 Allgemeines

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

Die Validierung durch Prüfungen muss geplant und in logischer Weise ausgeführt werden. Insbesondere:

a) Vor Beginn der Prüfungen muss ein Prüfplan ausgearbeitet werden, der Folgendes beinhalten muss:

   1) die Prüfspezifikationen;

   2) die zu erwartenden Ergebnisse der Prüfungen;

   3) die Reihenfolge der Prüfungen.

b) Prüfaufzeichnungen müssen erstellt werden, die Folgendes beinhalten:

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

   2) die Umgebungsbedingungen (siehe Abschnitt 10);

   3) die Vorgehensweisen bei der Prüfung und die verwendete Ausrüstung;

   4) das Prüfdatum;

   5) die Ergebnisse der Prüfung.

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

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

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

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

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

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

a) normale Umgebungsbedingungen bei bestimmungsgemäßer Verwendung; oder

b) Bedingungen bei besonderen Nennwerten; oder

c) bestimmte Bandbreiten für Bedingungen, wenn Driften zu erwarten ist.

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

6.2 Messunsicherheit

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

a) Zeitmessungen,

b) Druckmessungen,

c) Kraftmessungen,

d) elektrischen Messungen,

e) Messungen der relativen Feuchte,

f) Abstandsmessungen.

Abweichungen von diesen Messunsicherheiten müssen begründet werden.

6.3 Höherwertige Festlegungen

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

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

6.4 Anzahl der Prüflinge

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

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

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

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

7 Validierung der Spezifikation der Sicherheitsanforderungen

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

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

Es muss sichergestellt sein, dass die Anforderungen an alle Sicherheitsfunktionen der Maschinensteuerung dokumentiert werden.

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

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

— vorgesehenen Anwendungsanforderungen und Sicherheitserfordernissen;

— Betriebs- und Umgebungsbedingungen sowie möglichem menschlichen Versagen (z. B. Missbrauch) berücksichtigt wurden.

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

8 Validierung der Sicherheitsfunktionen

Die Validierung der Sicherheitsfunktionen muss nachweisen, dass die Betätigung der gestalteten SRP/CS oder Kombination der SRP/CS, die die Sicherheitsfunktion enthalten, den festgelegten Eigenschaften entspricht.

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

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

— funktionale Analyse der Schaltbilder, Überprüfungen des Programms (siehe 9.5);

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

— Simulation;

— Überprüfung der in die Maschine eingebauten Hardwarebestandteile und der Software, um ihre Übereinstimmung mit der Dokumentation (z. B. Herstellung, Art, Bauart) zu bestätigen;

— Funktionsprüfung der Sicherheitsfunktionen (nach ISO 13849-1:2006, Abschnitt 5) in allen Betriebsarten der Maschine. Die Funktionsprüfung muss sicherstellen, dass alle sicherheitsbezogenen Ausgangssignale über ihren gesamten Bereich umgesetzt sind. Das schließt Überlastungsprüfungen ein. Die Prüffälle werden normalerweise von den Spezifikationen abgeleitet, können jedoch auch einige Fälle enthalten, die aus der Analyse der Schaltbilder oder des Programms abgeleitet sind;

— erweiterte Funktionsprüfung, um vorhersehbare abnormale Signale und Kombinationen von Signalen von irgendeiner Eingangsquelle zu überprüfen, einschließlich Energieunterbrechung, -wiederkehr und fehlerhafte Betätigungen;

— Überprüfung der Betriebsverknüpfung der SRP/CS auf Erfüllung ergonomischer Richtlinien (siehe ISO 13849-1:2006, 4.8).

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

9 Validierung der Performance Levels und Kategorien

9.1 Analyse und Prüfung der Performance Level und Kategorien

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

— eine Fehleranalyse der Steuerkreisdiagramme (siehe Abschnitt 5);

und wo die Fehleranalyse nicht überzeugend ist:

— bei redundanten Systemen Fehlereingabeprüfungen bei den tatsächlich vorhandenen Steuerkreisen und Fehlersimulation an demselben Typ/Modell der tatsächlich vorhandenen Bauteile, besonders in zweifelhaften Bereichen hinsichtlich der bei der Analyse festgestellten Leistungsfähigkeit (siehe Abschnitt 6);

— eine Simulation des Verhaltens der Steuerung bei Fehlerfällen, z. B. mit Mitteln von Hardware- und/oder Softwaremodellen.

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

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

— Fehlereingabeprüfungen an einem Produktionsmuster;

— Fehlereingabeprüfungen an einem Hardwaremodell;

— Softwaresimulation von Fehlern;

— Subsystemfehler, z. B. Energieversorgung.

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

9.2 Validierung der Festlegungen für Kategorien

9.2.1 Kategorie B

Die SRP/CS der Kategorie B müssen in Übereinstimmung mit den grundlegenden Sicherheitsprinzipien validiert werden (siehe A.2, B.2, C.2 und D.2), indem aufgezeigt wird, dass die Spezifikation, die Gestaltung, Konstruktion und Wahl der Bauteile mit ISO 13849-1:2006, 6.2.3 übereinstimmen. Es muss nachgewiesen sein, dass die $MTTF_d$ des Kanals mindestens drei Jahre beträgt. Das muss durch Prüfung so erreicht werden, dass die SRP/CS, so wie in den Dokumenten für die Validierung vorgesehen, in Übereinstimmung mit ihren Spezifikationen sind (siehe 4.5). Für die Validierung der Umgebungsbedingungen siehe 6.1.

9.2.2 Kategorie 1

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

a) sie die Anforderungen der Kategorie B erfüllen;

b) die Bauteile bewährt sind (siehe A.4 und D.4) unter mindestens einer der folgenden Bedingungen:

   1) sie sind in zahlreichen Fällen mit erfolgreichen Ergebnissen bei ähnlichen Anwendungen benutzt worden;

   2) sie sind nach Prinzipien hergestellt worden, die ihre Eignung und Zuverlässigkeit für sicherheitsbezogene Anwendungen aufzeigen;

c) bewährte Sicherheitsprinzipien (wo anwendbar, siehe A.3, B.3, C.3 und D.3) richtig einbezogen wurden. Wo neu entwickelte Prinzipien angewendet wurden, muss Folgendes validiert werden:

   1) wie die zu erwartenden Ausfallarten vermieden wurden;

   2) wie Fehler vermieden oder ihre Wahrscheinlichkeit reduziert wurde.

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

9.2.3 Kategorie 2

SRP/CS der Kategorie 2 müssen validiert werden, um aufzuzeigen, dass:

a) sie die Anforderungen der Kategorie B erfüllen;

b) die angewendeten bewährten Sicherheitsprinzipien (sofern anwendbar) die Anforderungen von 9.2.2 c) erfüllen;

c) die Prüfeinrichtung alle relevanten Fehler erkennt, die nacheinander während des Prüfablaufs berücksichtigt werden, und eine angemessene Reaktion der Steuerung bewirkt, die:

   1) einen sicheren Zustand einleitet, oder wenn das nicht möglich ist,

   2) eine Warnung vor der Gefährdung vorsieht;

d) die mit der Prüfeinrichtung durchgeführten Prüfungen nicht in einen unsicheren Zustand führen;

e) die Einleitung der Prüfung durchgeführt wird:

   1) beim Anlauf der Maschine und vor der Einleitung einer gefährlichen Situation, und

   2) periodisch während des Betriebs, wenn die Risikobeurteilung und die Art des Betriebs zeigen, dass dies notwendig ist.

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

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

h) die Anforderungsrate ≤ Testrate/100 ist;

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

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

ANMERKUNG In besonderen Fällen können höhere Werte der $MTTF_d$ erforderlich sein, zum Beispiel wegen eines hohen PL_r.

9.2.4 Kategorie 3

SRP/CS der Kategorie 3 müssen validiert werden, um aufzuzeigen, dass:

a) sie die Anforderungen der Kategorie B erfüllen;

b) die bewährten Sicherheitsprinzipien (wenn anwendbar) die Anforderungen von 9.2.2 c) erfüllen;

c) ein Einzelfehler nicht zum Verlust der Sicherheitsfunktion führt;

d) Einzelfehler (einschließlich Fehler gemeinsamer Ursache) in Übereinstimmung mit der sinnvollen Gestaltung und der angewendeten Technologie erkannt werden;

e) die $MTTF_d$ jeden Kanals mindestens drei Jahre beträgt;

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

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

ANMERKUNG In besonderen Fällen können höhere Werte der $MTTF_d$ erforderlich sein, zum Beispiel wegen eines hohen PL_r.

9.2.5 Kategorie 4

SRP/CS der Kategorie 4 müssen validiert werden, um aufzuzeigen, dass:

a) sie die Anforderungen der Kategorie B erfüllen;

b) die bewährten Sicherheitsprinzipien (wenn anwendbar) die Anforderungen von 9.2.2 c) erfüllen;

c) ein Einzelfehler (einschließlich Fehler gemeinsamer Ursache) nicht zum Verlust der Sicherheitsfunktion führt;

d) die Einzelfehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt werden;

e) wenn d) nicht möglich ist, eine Anhäufung von Fehlern nicht zum Verlust der Sicherheitsfunktion(en) führt. Der in Betracht gezogene Umfang der Anhäufung von Fehlern muss in Übereinstimmung mit der sinnvollen Gestaltung sein;

f) die $MTTF_d$ jeden Kanals mindestens 30 Jahre beträgt;

g) der DC_{avg} mindestens 99 % beträgt;

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

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

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

Die $MTTF_d$-Werte für Bauteile (einschließlich B_{10d}-, T_{10d}- und n_{op}-Werte) müssen auf ihre Plausibilität überprüft werden (z. B. gegen ISO 13849-1:2006, Anhang C). Beispielsweise muss die Dokumentation des Ursprungs dieser Werte überprüft werden.

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

Die DC-Werte von Bauteilen oder Blöcken müssen auf umfassende Dokumentation überprüft werden (z. B. nach ISO 13849-1:2006, Anhang E). Die korrekte Durchführung (Hardware und Software) von Überprüfungen und Diagnosen einschließlich angemessene Fehlerreaktion muss validiert werden, indem unter typischen Umgebungsbedingungen geprüft wird.

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

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

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

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

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

- Überprüfung von Dokumenten zur Gestaltung, die die Gültigkeit bestätigen von:
  - grundlegenden und bewährten Sicherheitsprinzipien (siehe Anhänge A bis D);
  - weitere Maßnahmen zur Vermeidung systematischer Ausfälle (siehe ISO 13849-1:2006, G.3), und
  - weitere Maßnahmen für die Steuerung systematischer Ausfälle wie Diversität der Hardware (siehe ISO 13840-1:2006, G.2), Schutz vor Änderung oder Programmierung zur Fehlererklärung;
- Fehleranalyse (z. B. FMEA);
- Fehlereingabeprüfungen/Fehlerstimulierung;
- Überprüfung und Prüfung von Datenkommunikation, wo verwendet;
- Überprüfung, dass ein Qualitätsmanagementsystem Ursachen systematischer Ausfälle während des Herstellungsprozesses vermeidet.

9.5 Validierung der sicherheitsbezogenen Software

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

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

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

ANMERKUNG Im Fall von kleinen Programmen kann eine Programmanalyse durch Nachprüfungen oder Durchläufe des Kontrollflusses, der Verfahren usw. ausreichend sein, indem die Softwaredokumentation (Kontrollflussdiagramm, Quellcodes von Modulen oder Blöcken, I/O und verschiedene Zuweisungslisten, Querverweislisten) verwendet wird.

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

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

— Black-Box-Test des funktionellen Verhaltens und der Leistungsfähigkeit (z. B. Zeitsteuerungsleistung);

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

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

— Prüffälle, die Fehler simulieren, die vorher analytisch festgelegt werden, wie auch die erwartete Reaktion, um die Eignung der auf der Software beruhenden Maßnahmen für die Steuerung der Ausfälle zu bewerten.

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

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

Die Maßnahmen zur Softwareanwendung nach ISO 13849-1:2006, 4.6.2 (für SRESW) und 4.6.3 (für SRASW), die vom zu erzielenden PL abhängig sind, müssen hinsichtlich ihrer geeigneten Anwendung untersucht werden.

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

9.6 Validierung und Nachweis des Performance Levels

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

— Überprüfung der genauen Bestimmung des PL von der Kategorie, dem DC_{avg} und der $MTTF_d$ nach ISO 13849-1:2006, 4.5.4 und Anhang K);

— Nachweis, dass der von den SRP/CS erreichte PL mit dem erforderlichen PL_r übereinstimmt, der aus der Risikobeurteilung erhalten wurde:

$$PL \geq PL_r$$

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

— den $MTTF_d$-Wert für jedes Baudteil;

— den DC;

— den CCF;

— die Struktur;

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

9.7 Validierung der Kombination von sicherheitsbezogenen Teile

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

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

— Überprüfen der korrekten Festlegung des Gesamt-PL, der auf dem PL der kombinierten SRP/CS beruht (nach ISO 13849-1:2006, 6.3);

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

— Berücksichtigung von Schnittstelleneigenschaften, z. B. Spannung, Strom, Druck, Datenformat der Angaben, Signallevel;

— Fehleranalyse hinsichtlich der Kombination/Integration, z. B. durch FMEA;

— für redundante Systeme Fehlereingabeprüfungen hinsichtlich der Kombination/Integration.

10 Validierung der Umgebungsanforderungen

Die bei der Gestaltung festgelegte Leistungsfähigkeit der SRP/CS muss unter Berücksichtigung der festgelegten Umgebungsbedingungen für die Steuerung validiert werden.

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

Wo anwendbar, muss sich die Validierung beziehen auf:

— zu erwartende mechanische Beanspruchungen durch Schock, Schwingung, das Eindringen von Verschmutzungen;

— mechanische Haltbarkeit;

— elektrische Nennwerte und Energieversorgungen;

— klimatische Bedingungen (Temperatur und Feuchte);

— elektromagnetische Verträglichkeit (Immunität).

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

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

11 Validierung der Instandhaltungsanforderungen

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

ANMERKUNG Die Validierung der Instandhaltungsanforderungen kann folgendermaßen durchgeführt werden:

— Überprüfen der Benutzerinformationen, um zu bestätigen, dass:

  — die Instandhaltungsanleitungen vollständig sind [einschließlich Verfahren, erforderlicher Werkzeuge, Häufigkeit der Überprüfungen, Zeitintervalle für den Austausch von Bestandteilen, die Gegenstand von Abnutzung sind (T_{10d}) usw.], und dass sie verständlich sind;

  — falls zutreffend, dass Richtlinien vorhanden sind, dass die Instandhaltung nur durch sachkundiges Instandhaltungspersonal durchgeführt werden darf;

— Überprüfen der Anwendung von Maßnahmen zur Erleichterung der Instandhaltung (z. B. Bereitstellung von Diagnosewerkzeugen zur Hilfe bei der Fehlererkennung und Reparatur).

Zusätzlich können folgende Maßnahmen angewendet werden:

— Maßnahmen zur Vermeidung von Fehlern während der Instandhaltung (z. B. Erkennung falscher Eingangsdaten durch Überprüfungen der Plausibilität);

— Maßnahmen gegen Veränderung (z. B. ein Passwort, um nicht berechtigte Personen am Zugang zum Programm zu hindern).

12 Validierung der technischen Dokumentation und Benutzerinformation

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

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

Anhang A
(informativ)

Möglichkeiten zur Validierung mechanischer Systeme

Inhalt

A.1 Einleitung

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

A.2 Liste der grundlegenden Sicherheitsprinzipien

Tabelle A.1 — Grundlegende Sicherheitsprinzipien

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

Tabelle A.1 (*fortgesetzt*)

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

A.3 Liste bewährter Sicherheitsprinzipien

Tabelle A.2 — Bewährte Sicherheitsprinzipien

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

Tabelle A.2 (*fortgesetzt*)

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

Tabelle A.2 (*fortgesetzt*)

Bewährte Sicherheitsprinzipien	Bemerkungen
reduzierter Bereich der Geschwindigkeit und ähnlicher Parameter	Festlegen der notwendigen Begrenzung in Abhängigkeit von Erfahrungen und der jeweiligen Anwendung. Beispiele für Begrenzungen sind Fliehkraftregler, sichere Überwachung der Geschwindigkeit oder Wegbegrenzung.
reduzierter Bereich der Umgebungsparameter	Festlegen der notwendigen Begrenzungen. Beispiele für diese Parameter sind Temperatur, Feuchte, 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 Toleranzen.

A.4 Liste der bewährten Bauteile

Die in der folgenden Liste aufgeführten bewährten Bauteile für sicherheitsbezogene Anwendungen beruhen auf der Anwendung von bewährten Sicherheitsprinzipien und/oder einer Norm für deren spezielle Anwendungen.

Ein für bestimmte Anwendungen bewährtes Bauteil kann für andere Anwendungen ungeeignet sein.

Tabelle A.3 — Bewährte Bauteile

Bewährte Bauteile	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 „Liste der bewährten Sicherheitsprinzipien“.	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 „Liste der bewährten Sicherheitsprinzipien“.	Siehe ISO 14119 (Verriegelungseinrichtungen).
Scherstift	Alle Faktoren, die auf die Anwendung Einfluss nehmen, sind zu berücksichtigen. Siehe Tabelle A.2 „Liste der bewährten Sicherheitsprinzipien“.	–

A.5 Fehlerlisten und Fehlerausschlüsse

A.5.1 Einleitung

In den Listen werden einige Fehlerausschlüsse und die dazugehörigen Begründungen angegeben. Weitere Ausschlüsse siehe 4.3.

Der genaue Zeitpunkt, zu dem ein Fehler in ein System eingegeben wird, kann kritisch sein (siehe 8.1).

A.5.2 Verschiedene mechanische Geräte, Bauteile und Elemente

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

Fehlerannahme	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, 7.2.
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).	

A.5.3 Schraubendruckfedern

Tabelle A.5 — Schraubendruckfedern

Fehlerannahme	Fehlerausschluss	Bemerkungen
Verschleiß/Korrosion	Ja, bei Anwendung bewährter Feder(n) und sorgfältig ausgewählter/n Befestigungsart(en) (siehe Tabelle A.2).	Siehe ISO 13849-1:2006, 7.2.
Verringerung der Kraft durch bleibende Verformung und Bruch		
Bruch		
Steifheit/Hängenbleiben		
Lösen		
Verformung durch Überbeanspruchung		

Anhang B
(informativ)

Möglichkeiten zur Validierung pneumatischer Systeme

Inhalt

B.1 Einleitung

Bei Anwendung pneumatischer Systeme in Verbindung mit anderen Technologien sollten auch die zutreffenden Tabellen für grundlegende und bewährte Sicherheitsprinzipien berücksichtigt werden. Wo pneumatische Bauteile elektrisch angesteuert werden, sollten die entsprechenden Fehlerlisten im Anhang D berücksichtigt werden.

ANMERKUNG Anforderungen von spezifischen Richtlinien, wie der Richtlinie für einfache Druckbehälter, der Druckgeräte-Richtlinie, könnten angewendet werden müssen.

B.2 Liste der grundlegenden Sicherheitsprinzipien

Tabelle B.1 — Grundlegende Sicherheitsprinzipien

Grundlegende Sicherheitsprinzipien	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, Toleranzen, Herstellungsverfahren.
Geeignete Auswahl, Kombination, Anordnungen, Zusammenbau und Einbau der Bauteile/des Systems	Berücksichtigen von Anwendungshinweisen des Herstellers, z. B. Katalogblätter, Einbauanweisungen, Festlegungen, sowie von Erfahrungen mit ähnlichen Bauteilen/Systemen.

Tabelle B.1 (*fortgesetzt*)

Grundlegende Sicherheitsprinzipien	Bemerkungen
Anwendung des Prinzips der Energietrennung	Der sichere Zustand wird erreicht, indem alle wichtigen Einrichtungen von der Energiequelle abgetrennt werden. Siehe Primärmaßnahmen zum Anhalten in ISO 12100-2:2003, 4.11.3. Zum Ingangsetzen der Bewegung eines Mechanismus wird Energie benötigt. Siehe Primärmaßnahmen zum Ingangsetzen in ISO 12100-2:2003, 4.11.3. Berücksichtigen von unterschiedlichen Betriebsarten, z. B. Betriebsmodus, Instandhaltungsmodus. Dieses Prinzip darf bei einigen Anwendungen nicht benutzt werden, z. B. wenn der Ausfall des pneumatischen Drucks eine zusätzliche Gefährdung erzeugt.
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.
Begrenzung/Verringerung der Geschwindigkeit	Ein Beispiel ist die Geschwindigkeitsbegrenzung eines Kolbens durch ein Stromventil oder eine Drossel.
ausreichende Maßnahmen zur Vermeidung von Verunreinigung der Druckluft	Berücksichtigen von Filtration der Druckluft/Abtrennung von Feststoffen und Wasser.
geeigneter Schaltzeitbereich	Berücksichtigen von z. B. der Länge der Rohrleitung, Druck, Entlüftungskapazität, Kraft, Verringerung der Federkraft, Reibung, Schmierung, Temperatur, Trägheit bei Beschleunigung und Verzögerung, Zusammenwirken von Toleranzen.
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, arbeitet. 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	Verringern der Anzahl der Bauteile 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).

B.3 Liste der bewährten Sicherheitsprinzipien

Tabelle B.2 — Bewährte Sicherheitsprinzipien

Bewährte Sicherheitsprinzipien	Bemerkungen
Überdimensionierung/Sicherheitsfaktor	Die Sicherheitsfaktoren werden in Normen angegeben oder beruhen auf Erfahrungen mit sicherheitsbezogenen Anwendungen.
gesicherte Position	Das bewegliche Element eines 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 Ventilkolbens in die sichere Position (AUS-Stellung) gegenüber dem Flächenverhältnis für die Bewegung des Ventilkolbens 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.
zwangläufige mechanische Wirkung/Betätigung	Die zwangläufige mechanische Wirkung/Betätigung 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, 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 der Druckluft	Berücksichtigen von hoch wirksamer Filtration der Druckluft/Abscheidung von Feststoffen und Wasser.
ausreichend große positive Überdeckung in Kolbenventilen	Die positive Überdeckung sichert die Stopp-Funktion und verhindert unzulässige Bewegungen.
Hysteresebegrenzung	Die Hysterese erhöht sich z. B. durch stärkere Reibung. Zusammenwirken von Toleranzen beeinflusst die Hysterese ebenfalls.

B.4 Liste der bewährten Bauteile

Zurzeit ist keine Liste von bewährten Bauteilen vorhanden. Die Eigenschaft bewährt zu sein, hängt hauptsächlich von der jeweiligen Anwendung ab. Bauteile können als bewährt bezeichnet werden, wenn sie den in ISO 13849-1:2006, 6.2.2 und in ISO/DIS 4414:2008, Abschnitte 5 bis 7 angegebenen Beschreibungen entsprechen.

Ein für bestimmte Anwendungen bewährtes Bauteil kann für andere Anwendungen ungeeignet sein.

B.5 Fehlerlisten und Fehlerausschlüsse

B.5.1 Einleitung

In den Listen werden einige Fehlerausschlüsse und die zugehörigen Begründungen angegeben. Weitere Ausschlüsse siehe 4.3.

Der genaue Zeitpunkt, zu dem ein Fehler in ein System eingegeben wird, kann kritisch sein (siehe 9.1).

B.5.2 Ventile

Tabelle B.3 — Wegeventile

Fehlerannahme	Fehlerausschluss	Bemerkungen
Veränderung der Schaltzeiten	Ja, bei zwangläufiger mechanischer Betätigung (siehe Tabelle A.2) der bewegten 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 zwangläufiger mechanischer Betätigung (siehe Tabelle A.2) der bewegten Bauteile, sofern die Betätigungskraft ausreichend groß ist.	
selbsttätige Veränderung der Ausgangs-Schaltstellung (ohne Eingangssignal)	Ja, bei zwangläufiger mechanischer Betätigung (siehe Tabelle A.2) der bewegten Bauteile, sofern die Haltekraft ausreichend groß ist, oder ja, wenn bewährte Federn angewendet werden (siehe Tabelle A.2) und wenn übliche Einbau- und Betriebsbedingungen vorliegen (siehe Bemerkung 1)), oder ja, bei Schieberventilen mit elastischer Abdichtung und wenn übliche Einbau- und Betriebsbedingungen vorliegen (siehe Bemerkung 1)).	1) Übliche Einbau- und Betriebsbedingungen liegen vor, wenn: — die vom Hersteller vorgegebenen Bedingungen befolgt werden und — sich die Gewichtskraft des bewegten Bauteils sicherheitstechnisch nicht ungünstig auswirkt (z. B. horizontaler Einbau) und — keine besonderen Massenträgheitskräfte auf die bewegten Bauteile wirken (z. B. Beachtung der Bewegungsrichtung bei Anordnung auf bewegten Maschinenteilen) und — keine extremen Schwingungs- und Schockbeanspruchungen auftreten.
Leckage	Ja, bei Schieberventilen mit elastischer Abdichtung, sofern eine ausreichende positive Überdeckung vorhanden ist (siehe Bemerkung 2)), und wenn übliche Betriebsbedingungen vorliegen und die Druckluft ausreichend aufbereitet und filtriert ist, oder ja, bei Sitzventilen, wenn übliche Betriebsbedingungen vorliegen (siehe Bemerkung 3)) und die Druckluft ausreichend aufbereitet und filtriert ist.	2) 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. 3) Übliche Betriebsbedingungen liegen vor, wenn die vom Hersteller vorgegebenen Bedingungen befolgt werden.

Tabelle B.3 (*fortgesetzt*)

Fehlerannahme	Fehlerausschluss	Bemerkungen
Veränderung des Leckage-volumenstroms 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 den Erfahrungen entsprechen.	
für Servo- und Proportional-ventile: 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.	
ANMERKUNG Werden Steuerfunktionen durch individuelle Einzelfunktionen mehrerer Ventile realisiert, sollte eine Fehlerbetrachtung für jedes Ventil durchgeführt werden. Bei vorgesteuerten Ventilen sollte entsprechend vorgegangen werden.		

Tabelle B.4 — Absperrventile/Rückschlagventile/Schnellentlüftungsventile/Wechselventile usw.

Fehlerannahme	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 die Führungsverhältnisse für das/die bewegte(n) Bauteil(e) etwa denen eines nicht gesteuerten Kugelsitzventils ohne ein Dämpfungssystem entsprechen (siehe Bemerkung 1)) und wenn bewährte Federn angewendet sind (siehe Tabelle A.2).	1) Für ein nicht gesteuertes Kugelsitzventil ohne Dämpfungssystem sind die Führungsverhältnisse 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 2)) und eine ausreichende Schließkraft aufgrund der vorliegenden Drücke und Flächen vorhanden ist.	2) Übliche Einbau- und Betriebsbedingungen werden eingehalten, wenn: — die vom Hersteller festgelegten Bedingungen befolgt werden und — keine besonderen Massenträgheitskräfte auf die bewegten Bauteile wirken, z. B. Beachtung der Bewegungsrichtung bei Anordnung auf bewegten Maschinenteilen, 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 3)) und die Druckluft ausreichend aufbereitet und filtriert ist.	3) Übliche Betriebsbedingungen liegen vor, wenn die vom Hersteller vorgegebenen Bedingungen befolgt werden.

Tabelle B.4 (*fortgesetzt*)

Fehlerannahme	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 den Erfahrungen entsprechen.	

Tabelle B.5 — Stromregelventile

Fehlerannahme	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 bedingt 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 ≥ 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 den Erfahrungen entsprechen.	

Tabelle B.6 — Druckventile

Fehlerannahme	Fehlerausschluss	Bemerkungen
Nichtöffnen oder nicht ausreichendes Öffnen (weg- und zeitmäßig) bei Überschreiten des Einstelldruckes (Hängenbleiben oder Schwergängigkeit des bewegten Bauteils) (siehe Bemerkung 1))	Ja, wenn: — die Führungsverhältnisse 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).	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 Führungsverhältnis im Allgemeinen so gestaltet, dass ein Hängenbleiben des bewegten Bauteils unwahrscheinlich ist.
Nichtschließen oder nicht vollständiges Schließen (weg- und zeitmäßig) bei Unterschreiten des Einstelldruckes (Hängenbleiben oder Schwergängigkeit des bewegten Bauteils) (siehe Bemerkung 1))		
Veränderung des Druck-Regelverhaltens ohne Veränderung der Verstelleinrichtung (siehe Bemerkung 1))	Ja, bei direkt betätigten Druckbegrenzungsventilen sowie Druckschaltventilen, wenn (eine) bewährte Feder(n) eingebaut ist/sind (siehe Tabelle A.2).	
für Proportional-Druckventile: Veränderung des Druck-Regelverhaltens durch unbeabsichtigte Veränderung des Einstellwertes (siehe Bemerkung 1))	Nein	
selbsttätige Veränderung der Verstelleinrichtung	Ja, bei einer wirksamen Sicherung der Verstelleinrichtung entsprechend den Anforderungen der Anwendung, z. B. Plombierung.	–
unbeabsichtigtes Herausdrehen des Stellteils der Verstelleinrichtung	Ja, wenn eine wirksame formschlüssige Sicherung gegen das Herausdrehen vorhanden ist.	
Leckage	Ja, für Sitzventile, Membranventile und Schieberventile mit elastischer Abdichtung, bei üblichen Betriebsbedingungen (siehe Bemerkung 3)) und wenn die Druckluft ausreichend aufbereitet und filtriert ist.	3) Übliche Betriebsbedingungen liegen vor, wenn die vom Hersteller festgelegten Bedingungen befolgt werden.
Veränderung des Leckage-Volumenstroms 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 den Erfahrungen entsprechen.	

B.5.3 Rohrleitungen, Schlauchleitungen und Verbindungselemente

Tabelle B.7 — Rohrleitungen

Fehlerannahme	Fehlerausschluss	Bemerkungen
Bersten und Leckage	Ja, wenn Dimensionierung, Auswahl der Werkstoffe und Befestigung den Erfahrungen entsprechen (siehe Bemerkung 1)).	1) Bei Anwendung von Kunststoffrohren sind die Herstellerangaben zu beachten, insbesondere bezüglich der Umgebungseinflüsse während des Betriebs, z. B. thermische Einflüsse, chemische Einflüsse, 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 den 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 — Schlauchleitungen

Fehlerannahme	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 1)) und den zugehörigen Schlaucharmaturen angewendet werden.	1) 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. Ja, bei Steuer- und Messschlauchleitungen, wenn die Nennweite ≥ 2 mm ist.	–

Tabelle B.9 — Verbindungselemente

Fehlerannahme	Fehlerausschluss	Bemerkungen
Bersten, Schraubenbruch oder Ausreißen von Gewinden	Ja, wenn Dimensionierung, Auswahl der Werkstoffe, Herstellung, Anordnung und Verbindung zur Leitung und/oder zu den fluidtechnischen Bauteilen den Erfahrungen entsprechen.	–
Leckage (Verlust der Dichtwirkung)	Nein (siehe Bemerkung 1))	1) 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. Ja, bei Steuer- und Messverbindungselementen, wenn die Nennweite ≥ 2 mm ist.	–

B.5.4 Druckübersetzer und Druckmittelinverter

Tabelle B.10 — Druckübersetzer und Druckmittelinverter

Fehlerannahme	Fehlerausschluss	Bemerkungen
Verlust oder Veränderung der Dichtwirkung der Druckräume	Nein	–
Bersten der Druckräume sowie Bruch von Befestigungs- oder Deckelschrauben	Ja, wenn Dimensionierung, Auswahl der Werkstoffe, Anordnung und Befestigung den Erfahrungen entsprechen.	

B.5.5 Druckluftaufbereitung

Tabelle B.11 — Filter

Fehlerannahme	Fehlerausschluss	Bemerkungen
Zusetzen/Verstopfen des Filterelements	Nein	–
Bruch oder teilweiser Bruch des Filterelements	Ja, wenn das Filterelement eine ausreichende Druckfestigkeit hat.	
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 den Erfahrungen entsprechen.	

Tabelle B.12 — Öler

Fehlerannahme	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 den Erfahrungen entsprechen.	

Tabelle B.13 — Schalldämpfer

Fehlerannahme	Fehlerausschluss	Bemerkungen
Zusetzen (Verstopfen) des Schalldämpfers	Ja, wenn Konstruktion und Ausführung des Schalldämpferelementes die Bemerkung 1) erfüllen.	1) 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.

B.5.6 Energiespeicher und Druckbehälter

Tabelle B.14 — Energiespeicher und Druckbehälter

Fehlerannahme	Fehlerausschluss	Bemerkungen
Bruch/Bersten des Energiespeichers/ Druckbehälters oder der Verbindungselemente oder Ausreisen der Gewinde von Befestigungsschrauben	Ja, wenn Konstruktion, Auswahl der Ausrüstung, Auswahl der Werkstoffe und Anordnung im System den Erfahrungen entsprechen.	–

B.5.7 Sensoren

Tabelle B.15 — Sensoren

Fehlerannahme	Fehlerausschluss	Bemerkungen
fehlerhafter Sensor (siehe Bemerkung 1))	Nein	1) Sensoren in dieser Tabelle schließen die Signalerfassung, -verarbeitung und -ausgabe besonders für Druck, Volumenstrom, Temperatur usw. ein.
Veränderung der Erfassungs- oder Ausgabecharakteristika	Nein	–

B.5.8 Informationsverarbeitung

Tabelle B.16 — Verknüpfungsglieder

Fehlerannahme	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 für die entsprechenden Bauteile.	–

Tabelle B.17 — Verzögerungsglieder

Fehlerannahme	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 1)) und die Druckluft ausreichend aufbereitet und filtriert ist.	1) 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 den Erfahrungen entsprechen.	–

Tabelle B.18 — Umformer

Fehlerannahme	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 den Erfahrungen entsprechen.	–

Anhang C
(informativ)

Möglichkeiten zur Validierung hydraulischer Systeme

Inhalt

C.1 Einleitung

Bei Anwendung hydraulischer Systeme in Verbindung mit anderen Technologien sollten auch die zutreffenden Tabellen für grundlegende und bewährte Sicherheitsprinzipien berücksichtigt werden. Wo hydraulische Komponenten elektrisch angesteuert werden, sollten die entsprechenden Fehlerlisten im Anhang D berücksichtigt werden.

ANMERKUNG Anforderungen von besonderen Richtlinien, wie der Druckgeräte-Richtlinie, könnten angewendet werden müssen.

C.2 Liste der grundlegenden Sicherheitsprinzipien

ANMERKUNG Luftblasen und Kavitation in der Druckflüssigkeit sollten vermieden werden, weil sie zusätzliche Gefährdungen verursachen können, z. B. unbeabsichtigte Bewegungen.

Tabelle C.1 — Grundlegende Sicherheitsprinzipien

Grundlegende Sicherheitsprinzipien	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, Druckflüssigkeit.
richtige Dimensionierung und Formgebung	Berücksichtigen z. B. von Spannung, Dehnung, Ermüdung, Oberflächenrauheit, Toleranzen, Herstellungsverfahren.
geeignete Auswahl, Kombination, Anordnungen, Zusammenbau und Einbau der Bauteile/des Systems	Berücksichtigen von Anwendungshinweisen des Herstellers, z. B. Katalogblätter, Einbauanweisungen, Festlegungen, sowie von Erfahrungen mit ähnlichen Bauteilen/Systemen.

Tabelle C.1 (*fortgesetzt*)

Grundlegende Sicherheitsprinzipien	Bemerkungen
Anwendung des Prinzips der Energietrennung	Der sichere Zustand wird erreicht, indem alle wichtigen Einrichtungen von der Energiequelle abgetrennt werden. Siehe Primärmaßnahmen zum Anhalten in ISO 12100-2:2003, 4.11.3. Zum Ingangsetzen der Bewegung eines Mechanismus wird Energie benötigt. Siehe Primärmaßnahmen zum Ingangsetzen in ISO 12100-2:2003, 4.11.3. Unterschiedliche Betriebsarten sind zu berücksichtigen, z. B. Betriebsmodus, Wartungsmodus. Dieses Prinzip darf bei einigen Anwendungen nicht benutzt werden, z. B. dann, wenn der Verlust des hydraulischen Drucks eine zusätzliche Gefährdung erzeugt.
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.
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 Druckmediums	Berücksichtigen von Filtration des Druckmediums/ Abtrennung von Feststoffen und Wasser. Eine Anzeige, die auf die Notwendigkeit des Filterwechsels aufmerksam macht, ist auch zu berücksichtigen.
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 Toleranzen.
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, arbeitet. 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, Wartungsmodus. Eine besondere Einrichtung zum Ablassen der gespeicherten Energie kann erforderlich sein. Besondere Anwendungen, z. B. Beibehaltung der Energie für Spanneinrichtungen oder Sicherung einer Stellung, benötigen eine getrennte Betrachtungsweise.
Vereinfachung	Verringern der Anzahl der Bauteile in sicherheitsbezogenen Systemen.
geeigneter Temperaturbereich	Dieser ist überall im gesamten System zu berücksichtigen.
Trennung	Trennung der sicherheitsbezogenen Funktionen von anderen Funktionen.

C.3 Liste der bewährten Sicherheitsprinzipien

Tabelle C.2 — Bewährte Sicherheitsprinzipien

Bewährte Sicherheitsprinzipien	Bemerkungen
Überdimensionierung/Sicherheitsfaktor	Die Sicherheitsfaktoren werden in Normen angegeben oder gehen auf Erfahrungen mit sicherheitsbezogenen Anwendungen zurück.
gesicherte Position	Das bewegliche Element eines 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, das Flächenverhältnis für die Bewegung eines Ventilkolbens in die sichere Position (AUS-Stellung) gegenüber dem Flächenverhältnis für die Bewegung des Ventilkolbens in die EIN-Stellung wesentlich größer zu wählen (ein Sicherheitsfaktor).
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.
zwangläufige mechanische Wirkung/Betätigung	Die zwangläufige mechanische Wirkung/Betätigung 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 zum Erreichen eines definierten Volumenstroms	Beispiele sind Festblende, 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. der Bereiche für Druck, Volumenstrom und Temperatur, sollte berücksichtigt werden.
Überwachung des Zustands des Druckmediums	Berücksichtigen einer hoch wirksamen Filtration des Druckmediums/Abtrennung von Feststoffen und Wasser. Zu berücksichtigen sind auch die chemischen/physikalischen Zustände des Druckmediums. Berücksichtigen einer Anzeige, die auf die Notwendigkeit des Filterwechsels aufmerksam macht.
ausreichend große positive Überdeckung in Kolbenventilen	Die positive Überdeckung sichert die Anhaltefunktion und verhindert unzulässige Bewegungen.
Hysteresebegrenzung	Die Hysterese erhöht sich z. B. durch stärkere Reibung. Zusammenwirken von Toleranzen beeinflusst die Hysterese ebenfalls.

C.4 Liste der bewährten Bauteile

Zurzeit ist keine Liste von bewährten Bauteilen vorhanden. Die Eigenschaft bewährt zu sein, hängt hauptsächlich von der jeweiligen Anwendung ab. Bauteile können als bewährt bezeichnet werden, wenn sie den in ISO 13849-1:2006, 6.2.2 und in ISO/DIS 4413:2008, Abschnitte 5 bis 7 angegebenen Beschreibungen entsprechen.

Ein für bestimmte Anwendungen bewährtes Bauteil kann für andere Anwendungen ungeeignet sein.

C.5 Fehlerliste und Fehlerausschlüsse

C.5.1 Einleitung

In den Listen werden einige Fehlerausschlüsse und die zugehörigen Begründungen angegeben. Weitere Ausschlüsse siehe 4.3.

Der genaue Zeitpunkt, zu dem ein Fehler in ein System eingegeben wird, kann kritisch sein (siehe 9.1).

C.5.2 Ventile

Tabelle C.3 — Wegeventile

Fehlerannahme	Fehlerausschluss	Bemerkungen
Veränderung der Schaltzeiten	Ja, bei zwangläufiger mechanischer Betätigung (siehe Tabelle A.2) der bewegten Bauteile, sofern die Betätigungskraft ausreichend groß ist, oder ja, bezogen auf das Nichtöffnen eines Patronensitzventils besonderer Bauart, wenn es mit mindestens einem weiteren Ventil den Hauptvolumenstrom des Druckmediums steuert (siehe Bemerkung 1)).	1) Ein Patronensitzventil besonderer Bauart liegt vor, wenn: — die aktive Fläche zum Auslösen der sicherheitsbezogenen Schaltbewegung mindestens 90 % der Gesamtfläche des bewegten Bauteils (Ventilkegel) beträgt und — 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 und — 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 und — das bewegte Bauteil (Ventilkegel) mit Entlastungsrillen 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).
Nichtschalten (Hängenbleiben in einer End- oder Nulllage) oder nicht vollständiges Schalten (Hängenbleiben in einer beliebigen Zwischenstellung)	Ja, bei zwangläufiger mechanischer Betätigung (siehe Tabelle A.2) der bewegten Bauteile, sofern die Betätigungskraft ausreichend groß ist, oder ja, bezogen auf das Nichtöffnen eines Patronensitzventils besonderer Bauart, wenn es mit mindestens einem weiteren Ventil den Hauptvolumenstrom des Druckmediums steuert (siehe Bemerkung 1)).	

Tabelle C.3 (*fortgesetzt*)

Fehlerannahme	Fehlerausschluss	Bemerkungen
Selbsttätige Veränderung der Ausgangs-Schaltstellung (ohne Eingangssignal)	Ja, bei zwangläufiger mechanischer 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 ja, bezogen auf das Nichtöffnen eines Patronensitzventils besonderer Bauart, wenn es mit mindestens einem weiteren Ventil den Hauptvolumenstrom des Druckmediums steuert (siehe Bemerkung 1)) und wenn übliche Einbau- und Betriebsbedingungen vorliegen (siehe Bemerkung 2)).	2) Übliche Einbau- und Betriebsbedingungen liegen vor, wenn — die vom Hersteller vorgegebenen Bedingungen befolgt werden, und — sich die Gewichtskraft des bewegten Bauteils sicherheitstechnisch nicht ungünstig auswirkt (z. B. waagerechter Einbau), und — keine besonderen Massenträgheitskräfte auf die bewegten Bauteile wirken (z. B. Beachtung der Bewegungsrichtung bei Anordnung auf bewegten Maschinenteilen) und — keine extremen Schwingungs- und Schockbeanspruchungen auftreten.
Leckage	Ja, bei Sitzventilen, wenn übliche Einbau- und Betriebsbedingungen vorliegen (siehe Bemerkung 3)) und ein ausreichendes Filtrationssystem vorhanden ist.	3) Übliche Einbau- und 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 den 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 Steuerfunktionen durch individuelle Einzelfunktionen mehrerer Ventile realisiert, sollte eine Fehlerbetrachtung für jedes Ventil durchgeführt werden. Bei vorgesteuerten Ventilen sollte entsprechend vorgegangen werden.		

Tabelle C.4 — Absperrventile, Rückschlagventile, Wechselventile usw.

Fehlerannahme	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 die Führungsverhältnisse für das/die bewegte(n) Bauteil(e) etwa denen eines nicht gesteuerten Kugelsitzventils ohne ein Dämpfungssystem entsprechen (siehe Bemerkung 1)) und wenn bewährte Federn angewendet sind (siehe Tabelle A.2).	1) Für ein nicht gesteuertes Kugelsitzventil ohne Dämpfungssystem sind die Führungsverhältnisse im Allgemeinen so gestaltet, dass ein Hängenbleiben des bewegten Bauteils unwahrscheinlich ist.

Tabelle C.4 (*fortgesetzt*)

Fehlerannahme	Fehlerausschluss	Bemerkungen
selbsttätige Veränderung der Ausgangs-Schaltstellung (ohne Eingangssignal)	Ja, wenn übliche Einbau- und Betriebsbedingungen vorliegen (siehe Bemerkung 2)) und eine ausreichende Schließkraft aufgrund der vorliegenden Drücke und Flächen vorhanden ist.	2) Übliche Einbau- und Betriebsbedingungen werden eingehalten, wenn: — die vom Hersteller festgelegten Bedingungen befolgt werden, und — keine besonderen Massenträgheitskräfte auf die bewegten Bauteile wirken, z. B. Beachtung der Bewegungsrichtung bei Anordnung auf bewegten Maschinenteilen 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 3)) und ein ausreichendes Filtrationssystem vorhanden ist.	3) 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 den Erfahrungen entsprechen.	

Tabelle C.5 — Stromventile

Fehlerannahme	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 bedingt 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.	

Tabelle C.5 (*fortgesetzt*)

Fehlerannahme	Fehlerausschluss	Bemerkungen
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 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 den Erfahrungen entsprechen.	

Tabelle C.6 — Druckventile

Fehlerannahme	Fehlerausschluss	Bemerkungen
Nichtöffnen oder nicht ausreichendes Öffnen (weg- und zeitmäßig) bei Überschreiten des Einstelldruckes (Hängenbleiben oder Schwergängigkeit des bewegten Bauteils) (siehe Bemerkung 1))	Ja, bezogen auf das Nichtöffnen eines Patronensitzventils besonderer Bauart, wenn es mit mindestens einem weiteren Ventil den Hauptvolumenstrom des Druckmediums steuert (siehe Bemerkung 1) in Tabelle C.3)	1) Diese Fehlerannahme gilt nur, wenn das Druckventil insbesondere angewendet wird 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. Druckminderung, Druckbegrenzung.
Nichtschließen oder nicht vollständiges Schließen (weg- und zeitmäßig) bei Unterschreiten des Einstelldruckes (Hängenbleiben oder Schwergängigkeit des bewegten Bauteils) (siehe Bemerkung 1))	oder ja, wenn die Führungsverhältnisse 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).	2) Für ein nicht gesteuertes Kugelsitzventil ohne Dämpfungssystem sind die Führungsverhältnisse im Allgemeinen so gestaltet, dass ein Hängenbleiben des bewegten Bauteils unwahrscheinlich ist.
Veränderung des Druck-Regelverhaltens ohne Veränderung der Verstelleinrichtung (siehe Bemerkung 1))	Ja, bei direkt betätigten Druckbegrenzungsventilen, wenn (eine) bewährte Feder(n) eingebaut ist (sind) (siehe Tabelle A.2).	
für Proportional-Druckventile: Veränderung des Druck-Regelverhaltens durch unbeabsichtigte Veränderung des Einstellwertes (siehe Bemerkung 1))	Nein	
selbsttätige Veränderung der Verstelleinrichtung	Ja, bei einer wirksamen und dem Einsatzfall angepassten Sicherung der Verstelleinrichtung unter Beachtung sicherheitstechnischer Festlegungen (z. B. Plombierung).	–
unbeabsichtigtes Herausdrehen des Stellteils der Verstelleinrichtung	Ja, wenn eine wirksame formschlüssige Sicherung gegen das Herausdrehen vorhanden ist.	

Tabelle C.6 (*fortgesetzt*)

Fehlerannahme	Fehlerausschluss	Bemerkungen
Leckage	Ja, für Sitzventile, wenn übliche Betriebsbedingungen vorliegen (siehe Bemerkung 3)) und wenn ein ausreichendes Filtrationssystem vorhanden ist.	3) Übliche Betriebsbedingungen liegen vor, wenn die vom Hersteller festgelegten Bedingungen befolgt werden.
Veränderung des Leckage-Volumenstroms 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 den Erfahrungen entsprechen.	

C.5.3 Rohrleitungen aus Metall, Schlauchleitungen und Verbindungselemente

Tabelle C.7 — Rohrleitungen aus Metall

Fehlerannahme	Fehlerausschluss	Bemerkungen
Bersten und Leckage	Ja, wenn Dimensionierung, Auswahl der Werkstoffe und Befestigung den 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 den Erfahrungen entsprechen.	
Zusetzen (Verstopfen)	Ja, bei Rohrleitungen im Leistungskreis. Ja, bei Steuer- und Messrohrleitungen, wenn die Nennweite ≥ 3 mm ist.	

Tabelle C.8 — Schlauchleitungen

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

Tabelle C.9 — Verbindungselemente

Fehlerannahme	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 den Erfahrungen entsprechen.	–
Leckage (Verlust der Dichtwirkung)	Nein (siehe Bemerkung 1))	1) 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. Ja, bei Steuer- und Messverbindungselementen, wenn die Nennweite ≥ 3 mm ist.	–

C.5.4 Filter

Tabelle C.10 — Filter

Fehlerannahme	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 die Führungsverhältnisse des Bypassventils etwa denen eines nicht gesteuerten Kugelsitzventils ohne ein Dämpfungssystem entsprechen (siehe Tabelle C.4) und wenn bewährte Federn angewendet sind (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 den Erfahrungen entsprechen.	

C.5.5 Energiespeicher

Tabelle C.11 — Energiespeicher

Fehlerannahme	Fehlerausschluss	Bemerkungen
Bruch/Bersten des Energiespeicher-Behälters oder der Verbindungs-elemente oder der Deckelschrauben sowie Ausreißen der Schraubenge-winde	Ja, wenn Konstruktion, Auswahl der Ausrüstung, Auswahl der Werkstoffe und Anordnung im System den Erfahrungen entsprechen.	–
Leckage am Trennglied zwischen Gas und Druckflüssigkeit	Nein	
Ausfall/Bruch des Trennglied es zwischen Gas und Druckflüssigkeit	Ja, bei Zylinder-/Kolbenspeichern (siehe Bemerkung 1)).	1) Eine plötzlich auftretende größere Leckage wird nicht angenommen
Ausfalls des Füllventils auf der Gas-seite	Ja, wenn das Füllventil nach den Erfahrungen eingebaut ist und wenn ein ausreichender Schutz gegen äußere Einflüsse vorhanden ist.	–

C.5.6 Sensoren

Tabelle C.12 — Sensoren

Fehlerannahme	Fehlerausschluss	Bemerkungen
fehlerhafter Sensor (siehe Bemerkung 1))	Nein	1) Sensoren in dieser Tabelle schließen die Signalerfassung, -verarbeitung und -ausgabe ein, insbesondere für Druck, Volumenstrom, Temperatur usw.
Veränderung der Erfassungs- oder Ausgabecharakteristika	Nein	–

Anhang D
(informativ)

Möglichkeiten zur Validierung elektrischer Systeme

Inhalt

D.1 Einleitung

Bei Anwendung elektrischer Systeme in Verbindung mit anderen Technologien sollten auch die zutreffenden Tabellen für grundlegende und bewährte Sicherheitsprinzipien berücksichtigt werden.

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

D.2 Liste der grundlegenden Sicherheitsprinzipien

Tabelle D.1 — Grundlegende Sicherheitsprinzipien

Grundlegende Sicherheitsprinzipien	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, mechanische Festigkeit der Isolierstoffe.
richtige Dimensionierung und Formgebung	Berücksichtigen z. B. von Spannung, Dehnung, Ermüdung, Oberflächenrauheit, Toleranzen, Herstellungsverfahren.
Geeignete Auswahl, Kombination, Anordnungen, Zusammenbau und Einbau der Bauteile/des Systems	Berücksichtigen von Anwendungshinweisen des Herstellers, z. B. Katalogblätter, Einbauanweisungen, Festlegungen, sowie 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 automatisch unterbricht (siehe IEC 60204-1:2005, 6.3.3.

Tabelle D.1 (*fortgesetzt*)

Grundlegende Sicherheitsprinzipien	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 normalerweise geschlossenen Kontakts (NC) für Eingänge (Tast- und Positionsschalter) und eines normalerweise geöffneten Kontakts (NO) für Relais (siehe auch ISO 12100-2:2003), 4.11.3). 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 Wiederanlauf nach Wiederherstellung der Energieversorgung	Vermeiden von unerwartetem Anlauf, z. B. nach Wiederherstellung der Energieversorgung (siehe ISO 12100-2:2003, 4.11.4, 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.

D.3 Liste der bewährten Sicherheitsrichtlinien

Tabelle D.2 — Bewährte Sicherheitsprinzipien

Bewährte Sicherheitsprinzipien	Bemerkungen
Zwangsläufig mechanisch verbundene Kontakte	Anwendung zwangsläufig mechanisch verbundener Kontakte, z. B. für Überwachungsfunktion in Systemen der Kategorie 2, 3 und 4 (siehe EN 50205, IEC 60947-4-1:2001, Anhang F).
Fehlervermeidung in Kabeln	Um Kurzschlüsse zwischen zwei benachbarten Leitungen zu vermeiden: — 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 zum Vermeiden eines unsicheren Zustandes, z. B. durch Drehmoment-begrenzung, versetztes/zeitlich begrenztes Laufenlassen und verringerte Geschwindigkeit.
Vermeidung undefinierter Zustände	Undefinierter 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, vorher-bestimmt werden kann.
zwangsläufiger 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 12100-2:2003, 4.5).
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 12100-2:2003, 4.12.2).

Tabelle D.2 (*fortgesetzt*)

Bewährte Sicherheitsrichtlinien	Bemerkungen
Überdimensionierung	Bauteile, die in Schutzschaltkreisen angewendet werden, sollten 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 zehnmal kleiner ist als die Anzahl der Schaltungen, für die diese elektrische Einrichtung ausgelegt ist. ANMERKUNG Unterbelastung kann von der sinnvollen Gestaltung abhängen.
Verringerung von Fehlermöglichkeiten	Trennung sicherheitsbezogener von anderen Funktionen.
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.

D.4 Liste der bewährten Bauteile

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 dieser Tabelle 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 Komponenten (z. B. PLC, Mikroprozessoren, anwendungsspezifisch integrierter Schaltkreis) können nicht als bewährt angesehen werden.

Tabelle D.3 — Bewährte Bauteile

Bewährte Bauteile	Zusätzliche Bedingungen für „bewährt“	Norm oder Festlegung
Schalter mit zwangläufigem Betätigungsmodus (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
Sicherung	–	IEC 60269-1
Leistungsschalter	–	IEC 60947-2
Lastschalter, Trennschalter	–	IEC 60947-3

Tabelle D.3 (*fortgesetzt*)

Bewährte Bauteile	Zusätzliche Bedingungen für „bewährt“	Norm oder Festlegung
Differenzialleistungsschalter/RCD (Residual current detection — Reststromerkennung)	–	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
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

Tabelle D.3 (*fortgesetzt*)

Bewährte Bauteile	Zusätzliche Bedingungen für „bewährt“	Norm oder Festlegung
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 611558
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	–	Elektrizitätsseitig siehe EN 60703-1
Druckschalter	–	Elektrizitätsseitig siehe ISO 13856 (alle Teile). Druckseitig siehe Anhänge B und C.
elektromagnetisches Ventil	–	Keine Europäischen oder Internationalen Normen vorhanden.

D.5 Fehlerlisten und Fehlerausschlüsse

D.5.1 Einleitung

In den Listen werden einige Fehlerausschlüsse und die zugehörigen Begründungen angegeben. Weitere Ausschlüsse siehe 4.3.

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

Der genaue Zeitpunkt, zu dem ein Fehler in ein System eingegeben wird, kann kritisch sein (siehe 9.1).

D.5.2 Leitungen und Verbindungen

Tabelle D.4 — Leitungen/Kabel

Fehlerannahme	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 1)), oder — die einzeln durch eine Erdverbindung geschützt sind.	1) 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 1)).	
Unterbrechung eines Leiters	Nein	–

Tabelle D.5 — Leiterplatten/bestückte Leiterplatten

Fehlerannahme	Fehlerausschluss	Bemerkungen
Kurzschluss zwischen benachbarten Leiterbahnen/Kontaktstellen	Kurzschlüsse zwischen benachbarten Leitern, wenn die Bemerkungen 1) bis 3) zutreffen.	1) Es wird Basismaterial nach IEC 61249-2 verwendet. 2) Die Kriech- und Luftstrecken werden mindestens nach IEC 60664-5 bemessen mit Verschmutzungsgrad 2/ Überspannungskategorie III; ANMERKUNG 1 Verstärkte Isolierung zwischen den Leiterbahnen sollte erforderlich sein. 3) Die montierte Platte ist in eine Einfassung eingebaut, die vor leitfähiger Verschmutzung schützt 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 2 Lötmasken sind ausreichend als Schutzschicht, wenn sie die entsprechenden Anforderungen von IEC 60664-3 entsprechen. ANMERKUNG 3 Eine weitere Schutzschicht, die nach IEC 60664-3 abdeckt, kann die Kriech- und Luftstrecken verringern.
Unterbrechung in allen Leiterbahnen	Nein	–

Tabelle D.6 — Klemmstellen

Fehlerannahme	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 60497-7-1 oder IEC 60497-7-2 verwendet, und die Anforderungen von IEC 60204-1:2006, 13.1.1 sind erfüllt. 2) Die Ausführung selbst stellen sicher, dass Kurzschluss verhindert wird, z. B. durch Kunststoff-Schrumpfschlauch über der Verbindungsstelle.
Unterbrechung einzelner Klemmen	Nein	–

Tabelle D.7 — Mehrpolige Steckverbindungen

Fehlerannahme	Fehlerausschluss	Bemerkungen
Kurzschluss zwischen zwei beliebigen benachbarten Steckerstiften	Kurzschluss zwischen benachbarten Steckerstiften, wenn die Bemerkungen 1) und 2) zutreffen. Wenn der Leiter auf eine PCB montiert ist, gelten die Erwägungen zum Fehlerausschluss aus Tabelle D.5.	1) Für mehradrige Drähte durch Anwendung von Aderendhülsen oder anderer geeigneter Mittel. Kriech- und Luftstrecken und alle Abstände sollten mindestens nach IEC 60664-1, Einsatzklasse III, bemessen sein.
vertauschter oder unrichtig eingesteckter Stift, wenn keine mechanische Möglichkeit zur Verhinderung vorgesehen ist	Nein	–
Kurzschluss durch Erd- oder Masseschluss eines Leiters (siehe Bemerkung 2)	Nein	2) Die Drahtader des Kabels wird als Teil der mehrpoligen Steckverbindung angesehen.
Unterbrechung einzelner Steckerstifte	Nein	–

D.5.3 Stromschalter

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

Fehlerannahme	Fehlerausschluss	Bemerkungen
Nichtschließen von Kontakten	Nein	–
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 1)).	1) 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 1)).	
ANMERKUNG 1 Fehlerlisten für mechanische Gesichtspunkte sind im Anhang A enthalten. ANMERKUNG 2 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-Aus-Vorrichtungen nach IEC 60947-5-5 ist ein Fehlerausschluss für mechanische Aspekte zulässig, wenn eine Höchstanzahl von Betätigungen berücksichtigt wird.		

Tabelle D.9 — Elektromechanische Vorrichtungen (z. B. Relais, Schütze)

Fehlerannahme	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 Bemerkungen 1) und 2) zutreffen.	1) Kriech- und Luftstrecken werden mindestens nach IEC 60664-1 Verschmutzungsgrad 2/ Überspannungskategorie III, bemessen.
Kurzschluss zwischen zwei Kontakten untereinander und/oder zwischen Kontakten und Wicklung	Kurzschluss kann ausgeschlossen werden, wenn Bemerkungen 1) und 2) zutreffen.	2) Leitfähige Teile, die sich lösen, können die Isolation zwischen den Kontakten und der Spule nicht überbrücken.
gleichzeitiges Geschlossensein normalerweise offener und normalerweise geschlossener Kontakte	Gleichzeitiges Geschlossensein der Kontakte kann ausgeschlossen werden, wenn Bemerkung 3) zutrifft.	3) Es werden zwangsläufig betätigte (oder mechanisch verbundene) Kontakte angewendet. (Siehe IEC 60947-5-1:2003, Anhang L).

Tabelle D.10 — Näherungsschalter

Fehlerannahme	Fehlerausschluss	Bemerkungen
Ausgang dauernd niederohmig	Nein (siehe Bemerkung 1)).	1) Siehe IEC 60947-5-3.
Ausgang dauernd hochohmig	Nein (siehe Bemerkung 2)).	2) Es sollten Maßnahmen zur Fehlerverhinderung beschrieben werden.
Spannungsversorgung unterbrochen	Nein	–
Nichtbetätigen des Schalters infolge eines mechanischen Ausfalls	Nichtbetätigung infolge eines mechanischen Ausfalls, wenn Bemerkung 3) zutrifft.	3) 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 — Elektromagnetische Ventile

Fehlerannahme	Fehlerausschluss	Bemerkungen
Nicht-Anzug	Nein	–
Nicht-Abfall	Nein	
ANMERKUNG Fehlerlisten für mechanische Aspekte von pneumatischen und hydraulischen Ventilen sind in den entsprechenden Anhängen B und C behandelt.		

D.5.4 Diskrete elektrische Bauteile

Tabelle D.12 — Transformatoren

Fehlerannahme	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 Abschnitt 18 von IEC 61558-1:2005 zu prüfen. Geeignete Prüfspannungen sind in Tabelle 8a von IEC 61558-1:2005 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 der wirksamen Verhältnisse der Windungen kann ausgeschlossen werden, wenn Bemerkung 1) zutrifft. Siehe auch die Anleitung in Bemerkung 3).	

Tabelle D.13 — Induktivitäten

Fehlerannahme	Fehlerausschluss	Bemerkungen
Unterbrechung	Nein	–
Kurzschluss	Kurzschluss kann ausgeschlossen werden, wenn Bemerkung 1) zutrifft.	1) Die Spule ist einlagig gewickelt, glasiert oder vergossen, hat axiale Drahtanschlüsse und ist axial eingebaut.
Veränderung des Wertes $0{,}5\ L_N < L < L_N$ + Abweichung, wobei L_N der Nennwert der Induktivität ist (siehe Bemerkung 2)).	Nein	2) Abhängig von der Art der Bauweise können andere Bereiche in Betracht gezogen werden.

Tabelle D.14 — Widerstände

Fehlerannahme	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) müssen dünne Metallschichten sein, in Verpackungsarten MELF, mini MELF oder μMELF.
Zufällige Veränderung des Wertes $0{,}5\ R_N < R < 2\ R_N$, wobei R_N der Nennwert des Widerstandes ist (siehe Bemerkung 3)).	Nein	3) Abhängig von der Art der Bauweise können andere Bereiche in Betracht gezogen werden.

Tabelle D.15 — Widerstandsnetzwerke

Fehlerannahme	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 (siehe Bemerkung 1)).	Nein	1) Abhängig von der Art der Bauweise können andere Bereiche in Betracht gezogen werden.

Tabelle D.16 — Potentiometer

Fehlerannahme	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 (siehe Bemerkung 1)).	Nein	1) Abhängig von der Art der Bauweise können andere Bereiche in Betracht gezogen werden.

Tabelle D.17 — Kondensatoren

Fehlerannahme	Fehlerausschluss	Bemerkungen
Unterbrechung	Nein	–
Kurzschluss	Nein	
Veränderung des Wertes $0{,}5\ C_N < C < C_N$ + Abweichung, wobei C_N der Nennwert des Kondensators ist (siehe Bemerkung 1)).	Nein	1) Abhängig von der Art der Bauweise können andere Bereiche in Betracht gezogen werden.
Veränderung des Wertes tan δ	Nein	–

D.5.5 Elektronische Bauteile

Tabelle D.18 — Diskrete Halbleiter
(z. B. Dioden, Zener-Dioden, Transistoren, Triacs, Thyristoren, Spannungsregler, Quarzkristall, Fototransistoren, lichtemittierende Dioden [LEDs])

Fehlerannahme	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 — Optokoppler

Fehlerannahme	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 Bemerkung 1) und 2) zutrifft.	1) 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. 2) Es werden Maßnahmen getroffen, um sicherzustellen, dass ein interner Fehler des Optokopplers nicht zu übermäßigem Temperaturanstieg seiner Isolierwerkstoffe führen kann.

Tabelle D.20 — Nicht programmierbare integrierte Schaltkreise

ANMERKUNG In dieser Norm werden integrierte Schaltkreise (ICs) mit weniger als 1 000 Gates und/oder weniger als 24 Steckerstiften, Funktionsverstärker, Schieberegister, Hybridmodule als nicht komplex betrachtet. Diese Festlegung ist willkürlich.

Fehlerannahme	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	

Tabelle D.21 — Programmierbare und/oder komplexe integrierte Schaltkreise

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. Die Analyse kann zusätzlich Fehler aufdecken, die berücksichtigt werden sollten, wenn sie die sicherheitsbezogene Funktion beeinflussen.

Fehlerannahme	Fehlerausschluss	Bemerkungen
Fehler in allen Teilen 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	

D.5.6 Bemerkungen zum Fehlerausschluss

D.5.6.1 Gültigkeit der Ausschlüsse

Alle Fehlerausschlüsse gelten nur dann als gültig, wenn sämtliche Bestandteile innerhalb ihrer festgelegten Nennwerte betätigt werden.

D.5.6.2 Zinn-Whisker-Bildung

Wenn bleifreie Verfahren und Produkte angewendet und verwendet werden, können elektrische Kurzschlüsse durch Zinn-Whisker (siehe Anmerkung 1) vorkommen. Das Whisker-Risiko ist zu ermitteln (siehe Anmerkung 2) und zu berücksichtigen, wenn der Fehlerausschluss „Kurzschluss ...“ eines jeglichen Bauteils (siehe Anmerkung 3 und 4) gilt.

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 folgenden Veröffentlichungen können hilfreich für die Beurteilung sein: siehe [28], [29].

ANMERKUNG 3 Beispiel: Wird das Risiko der Zinn-Whisker-Bildung hoch eingeschätzt, ist der Fehlerausschluss „Kurzschluss eines Widerstands“ sinnlos, da ein Kurzschluss zwischen den Kontakten dieses Bauteils betrachtet werden muss.

ANMERKUNG 4 Whiskers an Leiterplatten wurden noch nicht festgestellt. Die Leiterbahnen bestehen normalerweise aus Kupfer ohne Zinnbeschichtung. Kontaktstellen können mit Zinnlegierung beschichtet sein, doch scheint das Produktionsverfahren die Anfälligkeit für die Whisker-Bildung nicht zu fördern.

D.5.6.3 Kurzschlüsse an PWB-montierten Teilen

Kurzschlüsse an Teilen, die auf einer Leiterplatte (en: **p**rinted **w**iring **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.

Anhang E
(informativ)

Beispiel der Validierung von Fehlverhalten und Mitteln zur Diagnose

E.1 Einleitung

Dieses Beispiel berücksichtigt die Validierung des PL einer Sicherheitsfunktion, mit Ausnahme der Anforderungen an:

— $MTTF_d$-Werte;

— Ausfälle infolge gemeinsamer Ursache (CCF);

— Softwareanalyse;

— systematische Ausfälle.

Dieses Beispiel umfasst nicht die Validierung von:

— Sicherheitsanforderungen (siehe Abschnitt 7);

— Eigenschaften von Sicherheitsfunktionen (siehe Abschnitt 8);

— Umgebungsanforderungen (siehe Abschnitt 10);

— Instandhaltungsanforderungen (siehe Abschnitt 11);

— Dokumentationsanforderungen (siehe Abschnitt 12).

Es stellt eine Anleitung zur Verfügung, wie das Fehlverhalten und der Diagnosedeckungsgrad eines gegebenen Steuerkreises zu untersuchen sind. Die Verfahren, die hier zur Bestimmung des Diagnosedeckungsgrades angewendet werden, beruhen auf der Ausfallarten- und Effektanalyse (FMEA), wobei Anhang E von ISO 13849-1:2006 berücksichtigt wird.

ANMERKUNG Dieses Beispiel umfasst nicht das gesamte Validierungsverfahren sicherheitsbezogener Teile von Steuerungen (SRP/CS). Besonders die notwendige Validierung der Software wurde nicht berücksichtigt.

E.2 Beschreibung der Maschine

Dieses Beispiel beruht auf einer automatischen Montagemaschine, mit manueller Bestückung und Entnahme von Werkstücken. Es ist vorgesehen, dass die Maschine zwei aufeinander folgende Betätigungen (Einsetzen einer Kugel und Eindrehen von Schrauben) an jedem Werkstück durchführt.

Abgesehen von den Stationen zum Bestücken und zur Entnahme besteht die Maschine aus zwei Arbeitsstationen (siehe Bild E.1). Das erste dieser Arbeitsstationen ist der pneumatisch angetriebene Kugeleinsetzvorgang und das zweite ist der pneumatisch angetriebene Schraubendrehvorgang.

Ein elektrisch betriebener Drehtisch bewegt die Werkstücke zu jedem der vier Stationen. Auf dem Drehtisch sind Werkstückhalter angebracht, und die Werkstücke werden von Hand auf diese Halter gesetzt und von den Haltern entnommen. Ein invertergesteuerter Elektromotor betätigt das Umlaufgetriebe und das Riemenantriebssystem, das den Drehtisch bewegt.

Die Maschine ist von mechanischen Schutzeinrichtungen geschützt, die alle befestigt sind, bis auf eine verriegelte trennende Schutzeinrichtung, die den Zugang zu den Stationen zum Bestücken und zur Entnahme gewährt.

An der ersten Arbeitsstation wird eine Kugel mit einem waagerecht montierten pneumatischen Zylinder in das Werkstück eingesetzt, der von einem monostabilen 5/2-Anschlusswegeventil (1V1) 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, und der aufgebrachte Pressdruck wird durch einen Drucksensor in der Luftversorgungsleitung zur Zylinderausdehnung überwacht.

Die Schraubstation besteht aus einem senkrecht montierten, kolbenstangenlosen pneumatischen Zylinder, der eine pneumatisch angetriebene, sich drehende Schraubeinheit befördert. Die Schraubeinheit wird durch den pneumatischen Zylinder angehoben und abgesenkt, was durch ein monostabiles 5/2-Anschluss-wegeventil (1V2) gesteuert wird. Die Grundstellung (Ventil ohne Spannung) des Zylinders ist die obere Stellung, wobei die Schraubeinheit angehoben ist. Zusätzlich befindet sich ein pilotgesteuertes Rückschlag-ventil an der unteren Verbindung mit dem pneumatischen Zylinder.

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

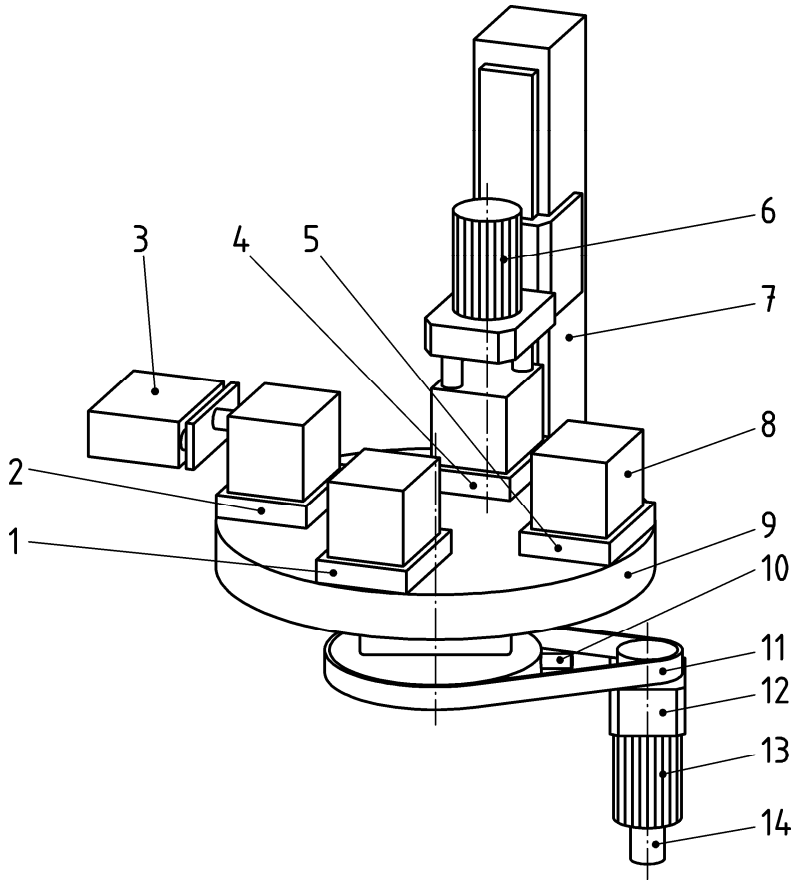
Ein einzelner Zyklus der Maschine wird durch das Betätigen des Anlauf-Tastschalters ausgelöst. Zu Beginn des Zyklus befinden sich drei Werkstücke auf dem Drehtisch: ein neu aufgeladenes Werkstück, ein teilweise fertig gestelltes Werkstück (Kugel eingesetzt) und ein fertig gestelltes Werkstück (Kugel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

Die folgenden Betriebsarten sind vorgesehen:

— automatischer Betrieb mit Bestücken und Entnahme von Hand;

— Einrichtbetrieb für den Drehtisch.

Die Maschine weist mechanische Gefährdungen auf, die aus Bewegungen der pneumatisch angetriebenen Maschinenauslöser (an den Arbeitsstationen zum Einsetzen der Kugel und zum Schrauben) und des elektrisch betriebenen Drehtisches entstehen können.



Legende

1	Aufgabestation	8	Werkstück
2	Arbeitsstation zum Einsetzen der Kugel	9	Drehtisch
3	Kugeleinsetzzylinder (A1)	10	Impulssensor
4	Schraubarbeitsstation	11	Antriebsriemen
5	Entnahmestation	12	Umlaufgetriebe
6	Schraubeinheit (A3)	13	Elektromotor
7	Schraubzylinder (A2)	14	Drehsensor

Bild E.1 — Beispiel — Automatische Montagemaschine

E.3 Festlegung der Anforderungen an Sicherheitsfunktionen

Die Sicherheitsfunktionen im automatischen Betrieb schützen vor gefährlichen Bewegungen, indem sie sicherstellen:

— 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.

Das kann als einzelne Sicherheitsfunktion für jedes (4 ×) einzelne Maschinen-Antriebselemet betrachtet werden:

— SF 1.1: der Drehtisch;

— SF 1.2: der Kugeleinsetzzylinder;

— SF 1.3: die Schraubeinheit;

— SF 1.4: der Schraubzylinder.

ANMERKUNG In diesem Beispiel werden der sicherheitsbezogene Halt und der Schutz gegen unerwarteten Anlauf als eine einzige Sicherheitsfunktion betrachtet, weil beides in dieselbe SRP/CS einbezogen ist.

Während des Einrichtbetriebs für den Drehtisch (mit den pneumatisch angetriebenen Maschinen-Antriebselementen ausgeschaltet), wird der sichere Zustand durch die Kombination folgender Sicherheitsfunktionen erreicht, solange die verriegelte trennende Schutzeinrichtung geöffnet ist:

— SF 2: sicher begrenzte Geschwindigkeit; und

— SF 3: selbsttätiger Rückstellungsbetrieb.

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

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

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

— PL_r c für selbsttätige Rückstellung (SF 3) (unter Berücksichtigung dessen, dass PL d für die Sicherheitsfunktion der sicher begrenzten Geschwindigkeit erforderlich ist).

Wenn SF 1 verlangt wird, muss der Drehtisch ein gesteuertes Abschalten entsprechend der Stoppkategorie 1 nach IEC 60204-1 ausführen. Für dieses Beispiel legt die Risikobeurteilung fest, dass der Ausfall der gesteuerten Verzögerung als Ergebnis einer Fehlfunktion des Inverters annehmbar war. Der senkrecht montierte pneumatische Zylinder (A2) der Schraubarbeitsstation und der waagerecht montierte pneumatische Zylinder (A1) der Arbeitsstation zum Einsetzen der Kugel müssen in ihre Grundstellungen zurückkehren und/oder darin verbleiben (d. h. jeweils oben und eingefahren). Die Schraubeinheit (A3) muss sofort anhalten. Der Mindestabstand zwischen der verriegelten trennenden Schutzeinrichtung und diesen sich bewegenden Teilen der Maschine wurde nach ISO 13855 festgelegt, beruhend auf der Abschaltleistung der Maschine.

Die Maschine ist mit weiteren Sicherheitsfunktionen ausgestattet wie einem Nothalt, einer Wiederanlaufsperre, Zurücksetzung usw., aber diese werden in diesem Beispiel nicht berücksichtigt.

E.4 Gestaltung der SRP/CS

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

Um den PL_r für die verschiedenen Sicherheitsfunktionen (siehe E.3) zu erreichen, wurden die Anforderungen von Kategorie 3 ausgewählt. Deshalb wurde ein unterschiedlicher redundanter und überwachter Aufbau für alle elektrischen und pneumatischen Teile (siehe Bilder E.2 und E.3) übernommen.

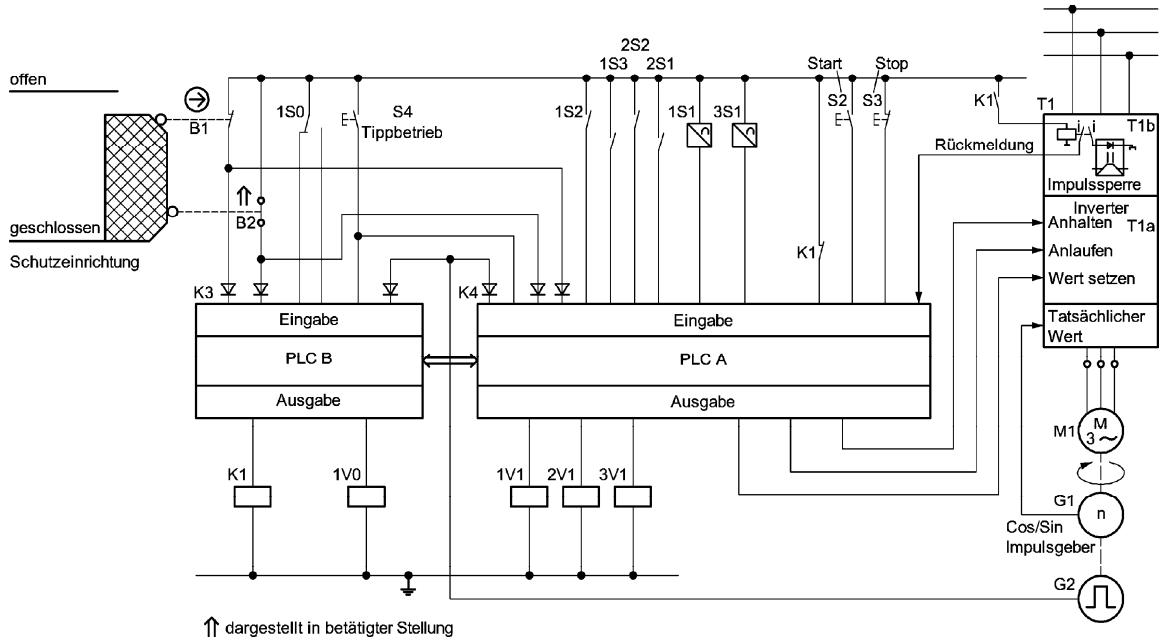


Bild E.2 — Automatische Montagemaschine, elektrisches und pneumatisches Diagramm

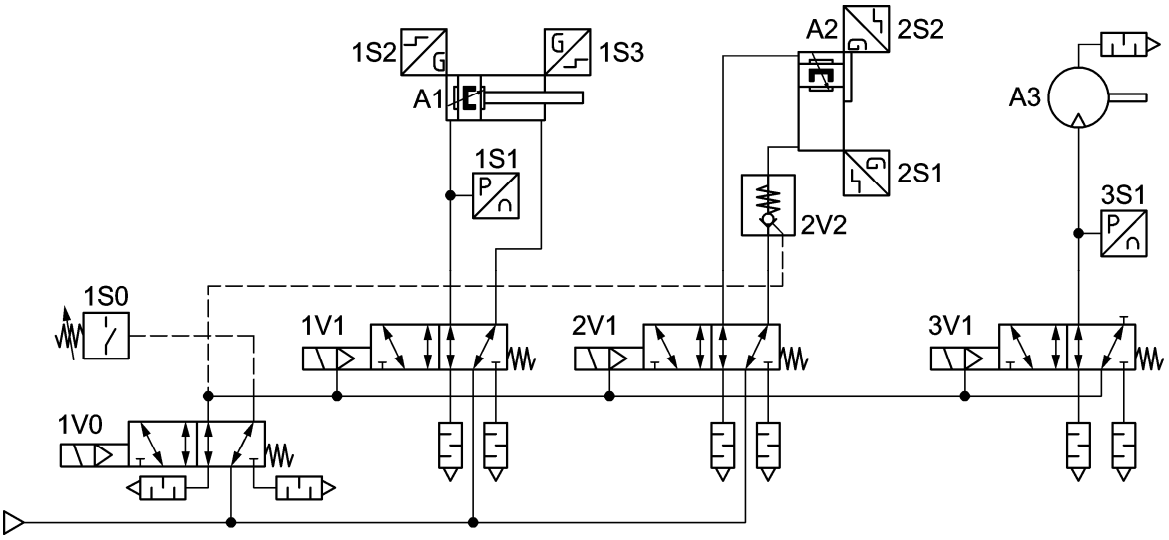


Bild E.3 — Automatische Montagemaschine, pneumatisches Schaltkreisdiagramm

Die Signale von den Sensoren und Steuerungsschaltern (Positionsschalter für die verriegelte trennende Schutzeinrichtung, Tastschalter für Tippbetrieb) wurden verdoppelt und zu zwei verschiedenen PLCs (PLC A und PLC B (unterschiedliche Hardware)) verbunden, die die Signale unter Verwendung von besonderen Softwarefunktionsblöcken (SRASW) ausführen. Diese beiden PLCs steuern ebenfalls die Funktion des Drehtischinverters und der pneumatisch angetriebenen Maschinen-Antriebselemente über zwei verschiedene Schaltstrecken.

Der spezifische Inverter in diesem Beispiel hat eine zusätzliche Vorrichtung (internes Relais), um die Steuersignale der Leistungshalbleiter (Impulssperre) auszuschalten, was als zweiter Abschalteweg betrachtet werden kann.

Im pneumatischen Steuerkreis wird die Luftzufuhr zu jedem Maschinen-Antriebselement (A1, A2 und A3) durch 5/2-Wegeventile (1V1, 2V1 und 3V1) über pilotgesteuerte Magnetventile gesteuert. Die Steuerluft für diese Ventile wird durch ein zusätzliches Ventil (1V0) derselben Bauart geschaltet, das über einen redundanten Kanal für deren Steuerung sorgt. Ein Druckschalter (1S0) ermöglicht die Überwachung des Zustands dieses Auslöseventils. Die Luftzufuhr für die Maschinen-Antriebselemente A1 und A2 wird von der Hauptluftzufuhr entnommen.

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

Die Luftzufuhr für das Maschinen-Antriebselements A3 (pneumatischer Motor) wird eher von der Steuerluftzufuhr (1V0) als von der Hauptluftzufuhr entnommen. Das stellt einen redundanten Kanal für die Steuerung der Luftzufuhr zu A3 sicher, ansonsten würde sich dieser weiterhin drehen, fiele 3V1 in der eingeschalteten Stellung aus.

In Übereinstimmung mit Kategorie 3 werden grundlegende und bewährte Sicherheitsprinzipien berücksichtigt, und die Anforderungen von Kategorie 2 werden ebenfalls erfüllt. Speziell gelten die Anforderungen der Normen IEC 60204-1 und ISO 4414.

Der Positionsschalter B1 ist ein Schalter mit direkter Betätigungsart entsprechend IEC 60947-5-1:2003, Anhang K, und ist deshalb nach Tabelle D.3 ein bewährtes Bauteil.

Das Kontaktrelais K1 besitzt mechanisch verbundene Kontaktelemente entsprechend IEC 60947-5-1:2003, Anhang L, und ist deshalb nach Tabelle D.2 ein bewährtes Bauteil.

Die entsprechenden Anwendungsprogramme von PLC A und PLC B enthalten besondere Softwarefunktionsblöcke (SRASW), die nach den Anforderungen von ISO 13849-1:2006, 4.6, für PL d programmiert wurden.

Die Eigenschaften der Steuerungsventile 1V1, 2V1, 3V1, 2V2 und 1V0 werden ausführlich in Tabelle E.1 erklärt.

Tabelle E.1 — Teileliste aus Bild E.3

Kennzeichnung	Funktion	Element	Eigenschaften	Grundlegende Sicherheitsrichtlinien/bewährte Sicherheitsrichtlinien	Möglicher Fehlerausschluss
1V0	Luft für Steuerpilot und Rückschlagventil 2V2	Elektromagnetisches Wegeventil	Federbelastetes Ventil mit 5/2-Funktion, pilotgesteuert, interne Pilotluftversorgung, Schieberventil mit Überdeckung	Tabelle B.1: Anwendung geeigneter Werkstoffe und Herstellungsverfahren (für tribologisches System, d. h. angemessene Schmierung), Anwendung des Prinzips der Energietrennung, Beständigkeit gegenüber Umgebungsbedingungen, Tabelle B.2: Überdimensionierung/Sicherheitsfaktor, gesicherte Stellung (Anwendung bewährter Federn), ausreichend große positive Überdeckung in Kolbenventilen	Druckaufbau bei Anschluss 4 mit geleertem Anschluss 5 in Normalstellung, Versagen der Dichtung durch Fließpressung, Bewegen des Ventilkolbens ohne Betätigung
1V1	Steuern des Zylinders zum Einsetzen der Kugel A1	Elektromagnetisches Wegeventil	Federbelastetes Ventil mit 5/2-Funktion, pilotgesteuert, externe Pilotluftversorgung, Schieberventil mit Überdeckung	Tabelle B.1: Anwendung geeigneter Werkstoffe und Herstellungsverfahren (für tribologisches System, d. h. angemessene Schmierung), Anwendung des Prinzips der Energietrennung, Beständigkeit gegenüber Umgebungsbedingungen, Tabelle B.2: Überdimensionierung/Sicherheitsfaktor, gesicherte Stellung (Anwendung bewährter Federn), ausreichend große positive Überdeckung in Kolbenventilen	Druckaufbau bei Anschluss 4 mit geleertem Anschluss 5 in Normalstellung, Versagen der Dichtung durch Fließpressung, Bewegen des Ventilkolbens ohne Betätigung
2V1	Steuern des Zylinders zum Einschrauben A2	Elektromagnetisches Wegeventil	Federbelastetes Ventil mit 5/2-Funktion, pilotgesteuert, externe Pilotluftversorgung, Schieberventil mit Überdeckung	Tabelle B.1: Anwendung geeigneter Werkstoffe und Herstellungsverfahren (für tribologisches System, d. h. angemessene Schmierung), Anwendung des Prinzips der Energietrennung, Beständigkeit gegenüber Umgebungsbedingungen, Tabelle B.2: Überdimensionierung/Sicherheitsfaktor, gesicherte Stellung (Anwendung bewährter Federn), ausreichend große positive Überdeckung in Kolbenventilen	Druckaufbau bei Anschluss 4 mit geleertem Anschluss 5 in Normalstellung, Versagen der Dichtung durch Fließpressung, Bewegen des Ventilkolbens ohne Betätigung
3V1	Steuern der Schraubeinheit (pneumatischer Motor) A3	Elektromagnetisches Wegeventil	Federbelastetes Ventil mit 5/2-Funktion, pilotgesteuert, externe Pilotluftversorgung, Schieberventil mit Überdeckung	Tabelle B.1: Anwendung geeigneter Werkstoffe und Herstellungsverfahren (für tribologisches System, d. h. angemessene Schmierung), Anwendung des Prinzips der Energietrennung, Beständigkeit gegenüber Umgebungsbedingungen, Tabelle B.2: Überdimensionierung/Sicherheitsfaktor, gesicherte Stellung (Anwendung bewährter Federn), ausreichend große positive Überdeckung in Kolbenventilen	Druckaufbau bei Anschluss 4 mit geleertem Anschluss 5 in Normalstellung, Versagen der Dichtung durch Fließpressung, Bewegen des Ventilkolbens ohne Betätigung
2V2	Absturzschutzeinrichtung für die Vertikalachse A2 der Schraubeinheit	Sperrende Verbindung	Pilotgesteuertes Rückschlagventil, gefedertes Kegelsitzventil	Tabelle B.2: durch die Auflagelast geschlossenes Ventil	Öffnen ohne pilotgesteuerte Luft

Tabelle E.1 (*fortgesetzt*)

Kennzeichnung	Funktion	Element	Eigenschaften	Grundlegende Sicherheitsrichtlinien/bewährte Sicherheitsrichtlinien	Möglicher Fehlerausschluss
1S0	Funktionsüberwachungsschalter für Ventil 1V0	Druckschalter	Fester Schaltpunkt	Nicht erforderlich zur Überwachung (keine Sicherheitsfunktion)	Nein
1S1	Überwachungssensor für das Kugeleinsetzvorgang	Drucksensor	Analoge Ausgabe	Nicht erforderlich zur Überwachung (keine Sicherheitsfunktion)	Nein
3S1	Überwachungssensor für den Einschraubvorgang	Drucksensor	Analoger Ausgabe	Nicht erforderlich zur Überwachung (keine Sicherheitsfunktion)	Nein
1S2, 1S3	Grenzlagenschalter für Zylinder A1 zum Einsetzen der Kugel	Näherungssensor	Magnetisches Messprinzip	Nicht erforderlich zur Überwachung (keine Sicherheitsfunktion)	Nein
2S1, 2S2	Grenzlagenschalter für Schraubendreherzylinder A2	Näherungssensor	Magnetisches Messprinzip	Nicht erforderlich zur Überwachung (keine Sicherheitsfunktion)	Nein
A1	Kugeleinsetzzylinder	Pneumatischer Zylinder	Nicht im Anwendungsbereich dieser Norm		
A2	Schraubzylinder	Kolbenstangenfreier pneumatischer Zylinder mit äußerer Führung	Nicht im Anwendungsbereich dieser Norm		
A3	Schraubeinheit	Pneumatischer Motor	Nicht im Anwendungsbereich dieser Norm		

SF 1: Sicherheitsbezogenes Abschalten durch Öffnen der verriegelten trennenden Schutzeinrichtung und Vermeidung von unerwartetem Anlauf, wenn die verriegelte trennende Schutzeinrichtung geöffnet ist

Entsprechend der Maschinenrichtlinie muss das Öffnen der verriegelten trennenden Schutzeinrichtung das Abschalten der vier Maschinen-Antriebselemente veranlassen: Drehtisch, (angetrieben durch einen inverter-gesteuerten Motor), Zylinder zum Einsetzen der Kugel, Schraubzylinder und Schraubeinheit. Diese Funktion kann deshalb wie in Bild E.4 gezeigt dargestellt werden.

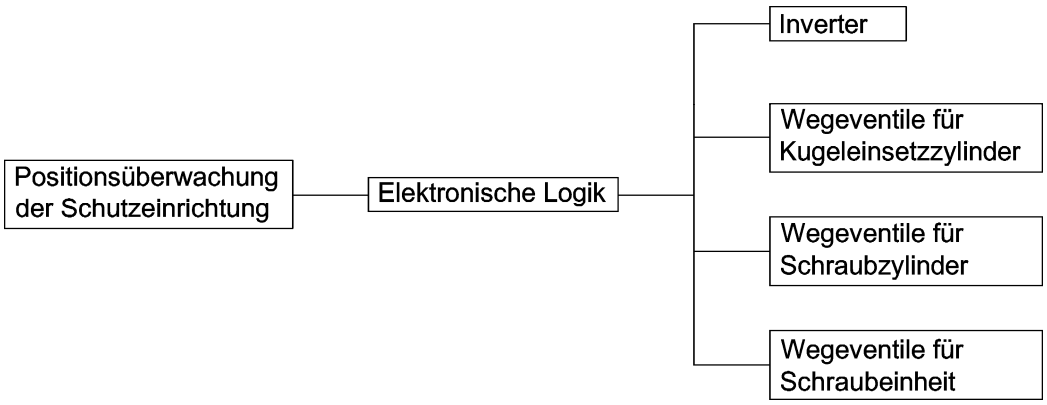


Bild E.4 — Funktionsblöcke von SF 1

Sobald die verriegelte trennende Schutzeinrichtung geöffnet wird, veranlasst PLC A ein Abschalten des Drehtisches, indem ein Abschaltsignal an den Inverter (T1a) abgegeben wird. PLC B überwacht die Verlangsamung des Drehtisches, und wenn dieser den Stillstand erreicht, wird der Hauptschütz K1 abgeschaltet, um die Impulssperre am Inverter (T1b) auszulösen. Wenn der Drehtisch aufgrund eines Fehlers nicht anhält, gibt PLC B noch ein weiteres Abschaltsignal an den Inverter (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.

Das Öffnen der verriegelten Schutzvorrichtung veranlasst PLC A außerdem, ein erstes Abschalten des Kugeleinsetzzylinders, des Schraubzylinders und der Schraubeinheit durch das Abschalten von 1V1, 2V1 und 3V1 herbeizuführen. PLC B veranlasst ein zweites Abschaltesignal für diese drei Schalter durch Abschalten von 1V0.

Wenn der Drehtisch abgeschaltet ist, aber die Station zum Einsetzen der Kugel und die Schraubstation 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 und 1V0 nach einer Verzögerung.

Solange sich die verriegelte trennende Schutzeinrichtung in offener Stellung befindet, muss sichergestellt sein, dass ein Versagen des Freigabepfads von PLC A nicht zu einem ungesteuerten Anlaufen führt. Das lässt sich erreichen, indem PLC B K1 abschaltet, sobald der Drehtisch 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 durchgeführt wie folgt:

a) Erkennung der sicherheitsbezogenen Teile

Die sicherheitsbezogenen Teile der Abschaltfunktion SF 1.1 und deren Aufteilung in Kanäle kann durch das sicherheitsbezogene Blockdiagramm erläutert werden, wie in Bild E.5 gezeigt.

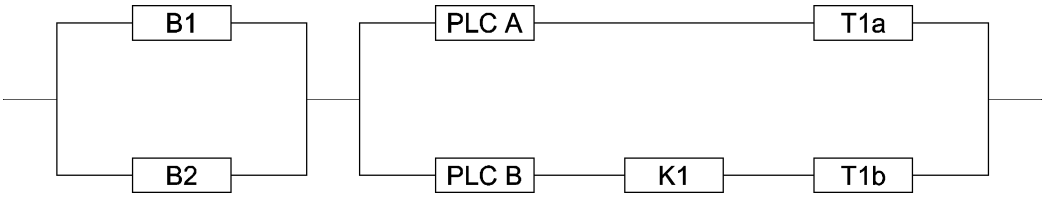
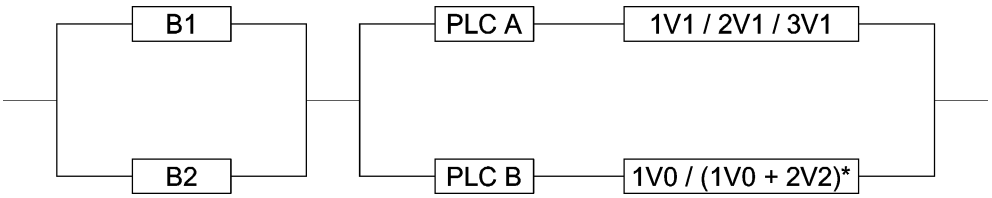


Bild E.5 — Abschalten des Drehtisches

Auf die gleiche Weise können die sicherheitsbezogenen Teile der Abschaltfunktionen SF 1.2, SF 1.3 und SF 1.4 und deren Aufteilung in Kanäle durch das in Bild E.6 gezeigte sicherheitsbezogene Blockdiagramm erläutert werden.



*SF 1.3

Bild E.6 — Abschalten von Kugeleinsetzzylinder, Schraubzylinder und Schraubeinheit

b) Darstellung als logische Blöcke

Die beiden Teile oder logischen Blöcke des Diagramms können in die vorgesehene Architektur für Kategorie 3 aufgenommen werden, also kann die Sicherungskette in zwei SRP/CS (Eingang, Logik/Ausgang) aufgeteilt werden, siehe Bild E.7.

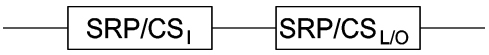


Bild E.7 — Sicherheitsbezogenes Blockdiagramm der Sicherheitsfunktion

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

c) Abschätzung der $MTTF_d$ jedes Kanals

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

Für die Abschätzung 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 ermöglicht die Anwendung der Symmetrisierungsgleichung ein Durchschnittsergebnis des mittleren $MTTF_d$ (mehr als 25 Jahre) für verschiedene Kanäle (siehe ISO 13849-1:2006, D.2).

d) Abschätzung von DC_{avg}

Der DC_{avg} wurde für beide SRP/CS aus dem DC der internen Prüfung und den Überwachungsmaßnahmen berechnet, die an den verschiedenen Teilen durchgeführt wurden.

Eine Überprüfung der Plausibilität der Eingangssignale für die Schutzeinrichtungssensoren B1 und B2 nach ISO 13849-1:2006, Anhang E, ergeben einen hohen DC_{avg} (99 %) für die SRP/CS_I.

Es werden folgende Diagnosemaßnahmen zur Verfügung gestellt:

— direkte Überwachung der Lage der K1-Kontakte durch PLC B;

— indirekte Überwachung des Betriebs von PLC A durch PLC B;

— indirekte Überwachung der Drehtischbewegung für G2, des Inverters T1a und PLC A durch PLC B;

— indirekte Überwachung der Grenzlagenschalter (1S2/1S3, 2S1/2S2) für Zylinder und Druckschalter (1S1, 3S1) für 1V1 und 3V1 durch PLC A;

— direkte Überwachung der Lage der Kontakte für das Sperren des Relais von T1b durch PLC A;

— indirekte Überwachung des Druckschalters (1S0) für 1V0 durch PLC B;

— Fehlererkennung durch das Verfahren für Wegeventile;

— weitere Angaben siehe Tabelle E.3.

Nach ISO 13849-1:2006, Anhang E, bieten diese Diagnosemaßnahmen einen mittleren DC_{avg} (90 %) für die $SRP/CS_{L/O}$.

e) Abschätzung 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 getroffen wurden, die nach ISO 13849-1:2006, Anhang F, einen Wert von 75 Punkten für jede SRP/CS erreichen.

f) Bestimmung des PL für jede SRP/CS

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

SRP/CS_{I}

— Kategorie 3;

— mittlere $MTTF_d$ jedes Kanals;

— hoher DC_{avg};

— 75 Punkte für Maßnahmen gegen CCF.

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

$SRP/CS_{L/O}$

— Kategorie 3;

— mittlere $MTTF_d$ jedes Kanals;

— mittlerer DC_{avg},

— 75 Punkte für Maßnahmen gegen CCF.

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

Nach ISO 13849-1.2006, 6.3, wird der PL der gesamten Kombination der SRP/CS bestimmt wie folgt:

— $PL_{niedrig} = d$;

— $N_{niedrig} = 2$;

PL für die Kombination ist PL d.

g) Systematische Ausfälle

Es wird geschätzt, dass geeignete Maßnahmen nach ISO 13849-1:2006, Anhang G, gegen systematische Ausfälle der SRP/CS getroffen wurden.

SF 2: sicher begrenzte Geschwindigkeit (SLS – en: **s**afely-**l**imited **s**peed**)**

Wenn sich die verriegelte trennende Schutzeinrichtung in offener Stellung befindet, muss sichergestellt sein, dass der Drehtisch sich nur mit sicher begrenzter Geschwindigkeit (SLS) bewegen kann, die durch den Tachogenerator G2 überwacht wird. Jede der PLCs überwacht das Signal von G2 und sie führen den Vergleich erwünschte/tatsächliche Geschwindigkeit unabhängig voneinander aus. Wird die Geschwindigkeit durch den Inverter T1a nicht erfolgreich auf den begrenzten Wert verringert, können die PLCs reagieren, indem sie das Anlauf-/Abschaltsignal des Inverters und den Impuls des Inverters T1b sperren.

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

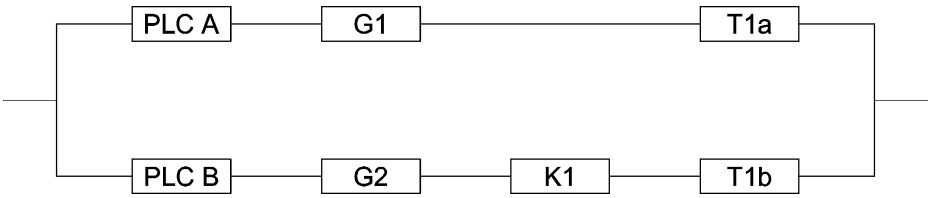


Bild E.8 — Blockdiagramm für die sicher begrenzte Geschwindigkeit (SLS)

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

a) Abschätzung der $MTTF_d$ jeden Kanals

Für die Abschätzung der $MTTF_d$-Werte der Bauteile wurden die Verlässlichkeitsdaten des Herstellers verwendet.

Für die Abschätzung der $MTTF_d$ eines Kanals wurde das „Parts-Count"-Verfahren angewendet (siehe ISO 13849-1:2006, Anhang D). Der unterschiedliche 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.

b) Abschätzung des DC_{avg}

Der DC_{avg} für die SRP/CS wurde aus dem DC der internen Prüfungen und Überwachungsmaßnahmen berechnet, die an verschiedenen Teilen ausgeführt wurden.

Die Plausibilitätsüberprüfung der Eingangssignale für die Sensoren der Schutzeinrichtung B1 und B2 nach ISO 13849-1:2006, Anhang E, ergibt einen hohen (99 %) DC für die SRP/CS_I.

Es werden folgende Diagnosemaßnahmen zur Verfügung gestellt:

— direkte Überwachung der Lage der Kontakte K1 durch PLC A;

— indirekte Überwachung des Betriebs von PLC A durch PLC B;

— indirekte Überwachung der Drehtischbewegung für G2, des Inverters T1a und PLC A durch PLC B;

— direkte Überwachung der Lage der Kontakte für das Sperren des Relais von T1b durch PLC B;

— indirekte Überwachung des Tachogenerators G2 in PLC A und PLC B;

— für weitere Angaben siehe Tabelle E.2.

Nach ISO 13849-1:2006, Anhang E, bieten diese Diagnosemaßnahmen ein hohes (99 %) DC_{avg}-Ergebnis für die $SRP/CS_{L/O}$.

c) Abschätzung 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 getroffen wurden, die nach ISO 13849-1:2006, Anhang F, einen Wert von 75 Punkten für jede SRP/CS erreichen.

d) Bestimmung des PL für jede SRP/CS

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

SRP/CS_I

— Kategorie 3;

— mittlere $MTTF_d$ jedes Kanals;

— hoher DC_{avg};

— 75 Punkte für Maßnahmen gegen CCF.

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

$SRP/CS_{L/O}$

— Kategorie 3;

— mittlere $MTTF_d$ jedes Kanals;

— mittlerer DC_{avg},

— 75 Punkte für Maßnahmen gegen CCF.

Werden diese Werte auf ISO 13849 1:2006, Bild 5 angewendet, ergibt sich PL d.

Nach ISO 13849-1:2006, 6.3, wird der PL der gesamten Kombination wie folgt bestimmt:

— $PL_{niedrig} = d$;

— $N_{niedrig} = 2$;

PL für die Kombination ist PL d.

e) Systematische Ausfälle

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

SF 3: selbsttätiger Rückstellungsbetrieb

Die Bewegung des Drehtisches (bei sicher begrenzter Geschwindigkeit) bei geöffneter verriegelter Schutzvorrichtung ist zulässig, wenn der Tastschalter S4 betätigt wird. Das Signal des Tastschalters S4 wird in beiden PLCs verarbeitet.

Die sicherheitsbezogenen Teile der Sicherheitsfunktion SF 3 und deren Unterteilung in Kanäle kann durch das in Bild E.9 dargestellte sicherheitsbezogene Blockdiagramm erläutert werden:

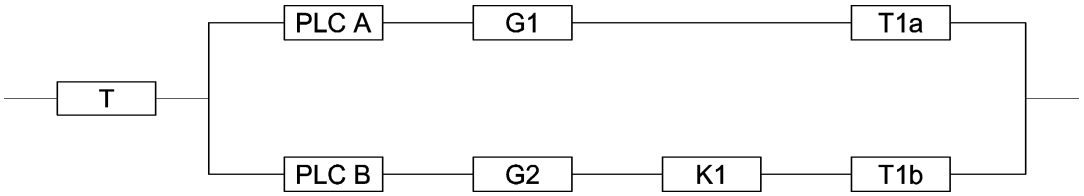


Bild E.9 — Blockdiagramm für den selbsttätigen Rückstellungsbetrieb

Die beiden Teile oder logischen Blöcke des Diagramms können in die vorgesehene Architektur für Kategorie 3 und Kategorie 1 aufgenommen werden, also kann die Sicherungskette in zwei SRP/CS (Eingabe, Logik/Ausgabe) aufgeteilt werden, siehe Bild E.10.

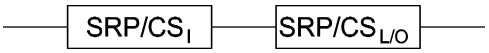


Bild E.10 — Sicherheitsbezogenes Blockdiagramm für den selbsttätigen Rückstellungsbetrieb

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

Der Diagnosedeckungsgrad (DC) und die $MTTF_d$-Werte für die $SRP/CS_{L/O}$ wurden bereits bestimmt (siehe SF 2). Die Bestimmung der $MTTF_d$ für die SRP/CS_I (Tastschalter für den selbsttätigen Rückstellungsbetrieb) wurde auf der Grundlage des B_{10d}-Wertes des Herstellers berechnet, der PL = c für die gesamte Sicherheitsfunktion erfüllt.

E.5 Validierung

Wie in E.1 angegeben, ist das Beispiel auf die Validierung von Fehlverhalten und Mitteln zur Diagnose beschränkt.

Nach 9.3 sollte die Validierung der Mittel zur Diagnose durch eine Überprüfung der Gestaltungsdokumentation und einige ergänzende Fehlereingabeprüfungen durchgeführt werden.

Folgende Schritte werden ausgeführt:

a) Die Diagnosemaßnahmen und die geprüften Einheiten (Bauteile, Blöcke) sind zu identifizieren.

b) Der auf jeden Diagnoseschaltkreis für eine bestimmte/bezogene Einheit übertragene DC-Wert ist nachzuweisen.

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

SF 1.1: Abschaltfunktion des Drehtisches, ausgelöst durch Öffnen der verriegelten trennenden Schutzeinrichtung und Vermeidung von unerwartetem Anlauf

Tabelle E.2 — FMEA der Abschaltfunktion und Vermeidung von unerwartetem Anlauf des Drehtisches

	Systeme/ Eigenschaften	Mögliche Ausfälle	Fehlererkennung	Effekt/ Reaktion	Prüfmaßnahme
F1	Ausfall des Verriegelungsschalters B1	Kurzschluss, mechanischer Ausfall, elektrischer Ausfall, Erdschluss	Wird erkannt durch fehlende Signaländerung, wenn die Sicherheitsfunktion erforderlich ist (Öffnen der verriegelten trennenden Schutzeinrichtung) Überwachung der Plausibilität wird in beiden Bewertungssystemen ausgeführt DC = 99 %	Abschalten bei Erkennung, Wiederanlauf verhindert	Am Eingang beider PLCs muss ein statisches Signal verwendet werden.
F2	Ausfall des Verriegelungsschalters B2	Kurzschluss, mechanischer Ausfall, elektrischer Ausfall, Erdschluss	Wird erkannt durch fehlende Signaländerung, wenn die Sicherheitsfunktion erforderlich ist (Öffnen der verriegelten trennenden Schutzeinrichtung) Überwachung der Plausibilität wird in beiden Bewertungssystemen ausgeführt DC = 99 %	Abschalten bei Erkennung, Wiederanlaufen verhindert	Am Eingang beider PLCs muss ein statisches Signal verwendet werden
F3	Ausfall von PLC A	Ausfälle der Eingabekarte, vielschichtige Ausfälle der CPU, Ausfälle der Ausgabekarte	Lesen von G2 und Vergleich mit der erwarteten Veränderung der Anzahl an Umdrehungen; zeitbezogen in PLC B. DC = 99 %	Der Inverter wird nach einer Zeitverzögerung abgeschaltet. Dieses Abschalten wird von K1 ausgeführt, das von PLC B gesteuert ist.	Die Ausgabe von PLC A ist auf hoher Ebene abzuschalten.
F4	Ausfall von PLC B	Ausfälle der Eingabekarte, vielschichtige Ausfälle der CPU, Ausfälle der Ausgabekarte	Durch Rückmeldung von K1 wird erkannt, dass PLC B nicht reagiert. DC = 99 %	Inverter wird von PLC A sofort abgeschaltet; Wiederanlaufen wird verhindert	K1-Ausgaben von PLC B sind zu hoch einzustellen.
F5	Ausfall des Inverters	Keine Reaktion auf den STOPP-Befehl	Erkennen durch Lesen von G2 in PLC A und PLC B. DC = 99 %	Sperren des Wiederanlaufens mittels PLC B	Anhalte-Eingabe des Inverters ist zu hoch einzustellen.
F6	Ausfall des Impulsgebers (G1)	Fehlende oder falsche Impulse werden erzeugt	Vergleich der Impulshäufigkeit mit dem gegebenen Wert. DC = 99 %	Inverter wird sofort von PLC A abgeschaltet, Wiederanlaufen wird verhindert.	Impulsabfolge ist auf PLC-Eingabe aufgedruckt
F7	Ausfall des Hauptschützes K1	Verschweißte Kontakte	Rückmeldung bei PLC A	Wiederanlaufen verhindert	K1 ist in EIN-Stellung zu belassen
F8	Ausfall des Antriebsriemens	Bruch des Antriebsriemens, Abnutzung der Riemenscheibe, Springen der Zähne	Ausfall in die sichere Richtung, keine Bewegung möglich. DC = 99 %	Nicht erforderlich	Nicht erforderlich
F9	Ausfall von PLC B (Vermeidung von unerwartetem Anlauf)	Ausfälle der Eingabekarte, vielschichtige Ausfälle der CPU, systematische Ausfälle in der Software	Ausfälle werden mittels Plausibilitätsprüfung in PLC A erkannt. DC = 99 %	Wiederanlaufen wird von PLC A verhindert	K1 ist mechanisch zu schalten
F10	Ausfall des Inverters (Vermeidung von unerwartetem Anlauf)	Interner Ausfall des Inverters	Ausfall wird in dieser Betriebsart nicht erkannt	Ausfall ist in dieser Betriebsart nicht wesentlich, da das Anlaufen von K1 gesperrt ist	

Tabelle E.2 (*fortgesetzt*)

	Systeme/ Eigenschaften	Mögliche Ausfälle	Fehlererkennung	Effekt/ Reaktion	Prüfmaßnahme
F11	Ausfall von G1 (Vermeidung von unerwartetem Anlauf)	Impulse werden erzeugt, obwohl Inverter still steht, Einsetzen äußerer Drehmomente	Ausfall wird durch Lesen von G2 (Plausibilitätsprüfung) in PLC A und PLC B erkannt	Ausfall ist in dieser Betriebsart nicht wesentlich, da das Anlaufen von K1 gesperrt ist	
Schlussfolgerung: Jeder aufgelistete Ausfall wird sicher erkannt. Deshalb kann der DC_{avg} auf 99 % gechätzt werden (ISO 13849-1:2006, Gleichung E.1).					

SF 1.2 bis SF 1.4: Abschaltfunktion der pneumatisch betriebenen Maschinenschalter, ausgelöst durch Öffnen der verriegelten trennenden Schutzeinrichtung und Vermeidung von unerwartetem Anlauf

Tabelle E.3 — FMEA der Abschaltfunktion und die Vermeidung von unerwartetem Anlauf der pneumatischen Antriebe

	Systeme/ Eigenschaften	Mögliche Ausfälle	Fehlererkennung	Effekt/Reaktion	Prüfmaßnahme
F1	Ausfall des Verriegelungsschalters B1	Kurzschluss, mechanischer Ausfall, elektrischer Ausfall, Erdschluss	Wird erkannt durch fehlende Signaländerung, wenn die Sicherheitsfunktion erforderlich ist (Öffnen der verriegelten trennenden Schutzeinrichtung) Überwachung der Plausibilität wird in beiden Bewertungssystemen ausgeführt DC = 99 %	Abschalten bei Erkennung, Wiederanlaufen verhindert	Am Eingang beider PLCs muss ein statisches Signal verwendet werden.
F2	Ausfall des Verriegelungsschalters B2	Kurzschluss, mechanischer Ausfall, elektrischer Ausfall, Erdschluss	Wird erkannt durch fehlende Signaländerung, wenn die Sicherheitsfunktion erforderlich ist (Öffnen der verriegelten trennenden Schutzeinrichtung) Überwachung der Plausibilität wird in beiden Bewertungssystemen ausgeführt DC = 99 %	Abschalten bei Erkennung, Wiederanlaufen verhindert	Am Eingang beider PLCs muss ein statisches Signal verwendet werden.
F3	Ausfall von PLC A	Ausfälle der Eingabekarte, vielschichtige Ausfälle der CPU, Ausfälle der Ausgabekarte	Lesen von G2 und Vergleich mit der erwarteten Veränderung der Umdrehungen; zeitbezogen in PLC B. DC = 99 %	Der Inverter wird nach einer Zeitverzögerung abgeschaltet. Dieses Abschalten wird von K1 ausgeführt, das von PLC B gesteuert ist.	Die Ausgabe von PLC A ist auf hoher Ebene abzuschalten.
F4	Ausfall von PLC B	Ausfälle der Eingabekarte, vielschichtige Ausfälle der CPU, Ausfälle der Ausgabekarte	Durch Rückmeldung von K1 wird erkannt, dass PLC B nicht reagiert. DC = 99 %	Inverter wird von PLC A sofort abgeschaltet; Wiederanlaufen wird verhindert	K1-Ausgaben von PLC B sind zu hoch einzustellen.
F5	Ausfall des elektromagnetischen Wegeventils 1V0	Keine Rückschaltung, bleibt in Zwischenstellung[a]	Wird erkannt durch fehlende Signaländerung am Druckschalter 1S0, wenn die Sicherheitsfunktion erforderlich ist (Öffnen der verriegelten trennenden Schutzeinrichtung). DC = 99 %	Abschalten bei Erkennung, Wiederanlaufen verhindert	Am Eingang von PLC B muss ein statisches Signal erzeugt werden.
F6	Ausfall des Druckschalters 1S0	Kurzschluss, mechanischer Ausfall, elektrischer Ausfall, Erdschluss	Wird erkannt durch fehlende Signaländerung am Druckschalter 1S0, wenn die Sicherheitsfunktion erforderlich ist (Öffnen der verriegelten trennenden Schutzeinrichtung). DC = 99 %	Abschalten bei Erkennung, Wiederanlaufen verhindert	Am Eingang beider PLCs muss ein statisches Signal erzeugt werden.
F7	Ausfall des elektromagnetischen Wegeventils 1V1	Keine Rückschaltung, bleibt in Zwischenstellung[a]	Lesen des Sensorsignals 1S1 und Endschalters 1S2/1S3 in PLC A. DC = 99 %	Abschalten bei Erkennung, Wiederanlaufen verhindert	Schwaches Signal zu 1S2, statisches Signal stärker als 1 V[c] am Eingang von 1S1.
F8	Ausfall des pneumatischen Zylinders A1	Steckenbleiben in Außenstellung, mechanischer Ausfall, Abfall von Druckluft	Durch Lesen des Endschalters 1S2. DC = 99 %	Wiederanlaufen verhindert, falls erforderlich, durch Unterbrechung der Hauptluftzufuhr[b].	Schwaches Signal zu 1S2, statisches Signal stärker als 1 V am Eingang von 1S1.
F9	Ausfall des Näherungssensors 1S2	Kurzschluss, mechanischer Ausfall, elektrischer Ausfall, Erdschluss	Erkannt aufgrund fehlender Signaländerung (stark > schwach). DC = 99 %	Abschalten bei Erkennung, Wiederanlaufen verhindert	Unterbrechung der Eingabe bei PLC A.

Tabelle E.3 (*fortgesetzt*)

	Systeme/ Eigenschaften	Mögliche Ausfälle	Fehlererkennung	Effekt/Reaktion	Prüfmaßnahme
F10	Ausfall des Näherungssensors 1S3	Nichtöffnen, Verschweißen der Kontakte	Erkannt aufgrund fehlender Signaländerung (stark > schwach). DC = 99 %	Abschalten bei Erkennung, Wiederanlaufen verhindert	Eingabe der PLC A zu 24 V
F11	Ausfall des elektromagnetischen Wegeventils 2V1	Keine Rückschaltung, zeitverzögerte Rückschaltung, bleibt in Zwischenstellung[a]	Lesen des Endschalters 2S2 in PLC A. DC = 99 %	Abschalten bei Erkennung, Wiederanlaufen verhindert	Schwaches Signal zu 2S2
F12	Ausfall des pneumatischen Zylinders A2	Steckenbleiben in Außenstellung, mechanischer Ausfall, Abfall von Druckluft	Lesen des Endschalters 2S2 in PLC A. DC = 99 %	Wiederanlaufen verhindert, falls erforderlich, durch Unterbrechung der Hauptluftzufuhr[b]	Schwaches Signal zu 2S2
F13	Ausfall des Näherungssensors 2S2	Kurzschluss, mechanischer Ausfall, elektrischer Ausfall, Erdschluss	Erkannt aufgrund fehlender Signaländerung (stark > schwach). DC = 99 %	Abschalten bei Erkennung, Wiederanlaufen verhindert	Unterbrechung der Eingabe bei PLC A.
F14	Ausfall des Näherungssensors 2S1	Nichtöffnen/Verkleben der Kontakte	Erkannt aufgrund fehlender Signaländerung (stark > schwach). DC = 99 %	Abschalten bei Erkennung, Wiederanlaufen verhindert	Eingabe der PLC A zu 24 V
F15	Ausfall des Rückschlagventils 2V2	Steckenbleiben, Bruch der Feder, Leckage	Ausfall kann in dieser Betriebsart nicht erkannt werden. DC = 0 %		
F16	Ausfall des elektromagnetischen Wegeventils 3V1	Keine Rückschaltung, zeitverzögerte Rückschaltung, bleibt in Zwischenstellung[a]	Lesen des Sensorsignals 3S1 in PLC A. DC = 99 %	Abschalten bei Erkennung, Wiederanlaufen verhindert	Statisches Signal stärker als 1 V am Eingang von 3S1
F17	Ausfall des elektromagnetischen Wegeventils 1V0 (Schutz vor unerwartetem Anlauf)	Selbständiges Schalten	Wird aufgrund der Signaländerung am Druckschalter 1S0 erkannt. DC = 99 %	Wiederanlaufen wird verhindert	1V0 wird über manuelle Vorrangsteuervorrichtung geschaltet
F18	Ausfall des Näherungssensors 1S3	Kurzschluss, mechanischer Ausfall, elektrischer Ausfall, Erdschluss	Nur „einschalten“ wird erkannt. DC = 99 %	Ausfall in dieser Betriebsart nicht wesentlich. Wiederanlaufen wird verhindert.	Eingabe von PLC A zu 24 V

Schlussfolgerung: Nicht jeder behandelte Ausfall wird erkannt. Deshalb kann der DC_{avg} auf 90 % geschätzt werden (ISO 13849-1:2006, Gleichung E.1). Ausfall F15 ist nicht relevant für diese Betriebsart.

[a] Magnetventile mit Kolbenventilen und positiver Überdeckung können in einer Stellung steckenbleiben, in der alle Verbindungen gesperrt sind

[b] oder sonstige geeignete Maßnahmen, um möglicherweise eingeklemmte Antriebe kräftefrei zu schalten, um Gefährdungen aufgrund von plötzlichen Zustandsänderungen auszuschließen.

[c] Spannungswerte und/oder Strom höher als die Ansprechschwelle am analogen Eingang.

SF 2 und SF3: sicher begrenzte Geschwindigkeit (SLS) und selbsttätiger Rückstellungsbetrieb

Tabelle E.4 — FMEA der sicher begrenzten Geschwindigkeit des Drehtisches

	Systeme/ Eigenschaften	Mögliche Ausfälle	Fehlererkennung	Effekt/Reaktion	Prüfmaßnahme
F1	Ausfall des Antriebs-riemens	Bruch des Antriebs-riemens, Abnutzung der Riemenscheibe, Springen der Zähne	Fehlererkennung während des Vorgangs. DC = 99 %	Anlaufsperre durch PLC B	Simulieren einer fehlerhaften Anzeige des Zielwertes
F2	Ausfall von PLC A	Vielschichtige Ausfälle innerhalb der CPU, Ausfälle der Ausgabe-karte, systematische Ausfälle in der Software	Lesen von G2 und Vergleich mit der erwarteten Veränderung der Zunahmen; zeitbezogen in PLC B. DC = 99 %	Der Antrieb wird nach einer Zeitver-zögerung abge-schaltet. Dieses Abschalten wird von K1 ausgeführt, das von PLC B gesteuert ist.	Simulieren einer fehlerhaften Anzeige des Zielwertes
F3	Ausfall von PLC B	Ausfälle der Eingabe-karte, vielschichtige Ausfälle der CPU, Ausfälle der Ausgabe-karte systematische Ausfälle in der Software	Bei dieser Betriebsart werden Ausfälle mittels Plausibilitäts-prüfung in PLC A erkannt. DC = 99 %	Abschalten des Hauptantriebs durch PLC A	Datenverfälschung (z. B. Unterbrechung der Kommunikation zwischen beiden PLCs)
F4	Ausfall des Inverters	Interner Ausfall des Inverters	Erkennung durch Lesen von G2 in PLC A und PLC B erkannt. DC = 99 %	Wiederanlaufsperre durch PLC B	Simulieren einer fehlerhaften Anzeige des Zielwertes
F5	Ausfall von G1	Nachgeben des Antriebs (Kupplung lose)	Fehler wird durch Lesen von G2 (Plausibilitätsprüfung) erkannt	Abschalten des Hauptantriebs durch PLC A	Simulieren einer fehlerhaften Anzeige des Zielwertes
F6	Ausfall von G2	Fehlende Impulse, Impulse werden erzeugt	Fehler wird durch Vergleich mit dem Zielwert erkannt. DC = 99 %	Wiederanlaufsperre durch PLC B	Simulieren einer fehlerhaften Anzeige des Zielwertes
Schlussfolgerung: Der DC_{avg} kann auf mittel geschätzt werden (siehe ISO 13849-1:2006).					

Tabelle E.5 — FMEA des selbsttätigen Rückstellungsbetriebs des Drehtisches

	Systeme/ Eigenschaften	Mögliche Ausfälle	Fehlererkennung	Effekt/Reaktion	Prüfmaßnahme
F1	Ausfall des Antriebs-riemens	Bruch des Antriebs-riemens, Abnutzung der Riemenscheibe, Springen der Zähne	Fehlererkennung während des Vorgangs. DC = 99 %	Anlaufsperre durch PLC B	Simulieren einer fehlerhaften Anzeige des Zielwertes
F2	Ausfall von PLC A	Vielschichtige Ausfälle innerhalb der CPU, Ausfälle der Ausgabe-karte, systematische Ausfälle in der Software	Lesen von G2 und Vergleich mit der erwarteten Veränderung der Zunahmen; zeitbezogen in PLC B. DC = 99 %	Der Antrieb wird nach einer Zeitver-zögerung abge-schaltet. Dieses Abschalten wird von K1 ausgeführt, das von PLC B gesteuert ist.	Simulieren einer fehlerhaften Anzeige des Zielwertes
F3	Ausfall von PLC B	Ausfälle der Eingabe-karte, vielschichtige Ausfälle der CPU, Aus-fälle in der Ausgabe-karte, systematische Ausfälle in der Software	Bei dieser Betriebsart werden Ausfälle mittels Plausibilitäts-prüfung in PLC A erkannt. DC = 99 %	Abschalten des Inverters durch PLC A	Datenverfälschung (z. B. Unterbrechung der Kommunikation zwischen beiden PLCs)
F4	Ausfall des Inverters	Interner Ausfall des Inverters	Fehler wird durch Lesen von G2 in PLC A und PLC B erkannt. DC = 99 %	Wiederanlaufsperre durch PLC B	Simulieren einer fehlerhaften Anzeige des Zielwertes
F5	Ausfall von G1	Nachgeben des Antriebs (Kupplung lose)	Fehler wird durch Lesen von G2 (Plausibilitätsprüfung) erkannt. DC = 99 %	Abschalten des Inverters durch PLC A	Simulieren einer fehlerhaften Anzeige des Zielwertes
F6	Ausfall des Tast-schalters für selbst-tätige Rückstellung	Verschweißen von Kontakten	Ausfall kann durch Zeitüber-wachung erkannt werden (niedrig-hoch-Wechsel in einem Zeitrahmen/-fenster). Möglicherweise ist Fehler-erkennung nicht erforderlich (aufgrund der Maßnahme „sichere Geschwindigkeit“). DC = 75 %	Abschalten des Inverters durch PLC A	Überbrückung des Schalters ("permanentes Drücken")
F7	Ausfall von G2	Fehlende Impulse, Impulse werden erzeugt	Fehler wird durch Vergleich mit dem Zielwert erkannt. DC = 99 %	Wiederanlaufsperre durch PLC B	Simulieren einer fehlerhaften Anzeige des Zielwertes

Anhang ZA
(informativ)

Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der 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 der Richtlinie und der zugehörigen EFTA-Vorschriften gegeben ist.

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

Literaturhinweise

[1] EN 982:1996, *Sicherheit von Maschinen — Sicherheitstechnische Anforderungen an fluidtechnische Anlagen und deren Bauteile — Hydraulik*

[2] EN 983:1996, *Sicherheit von Maschinen — Sicherheitstechnische Anforderungen an fluidtechnische Anlagen und deren Bauteile — Pneumatik*

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

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

[5] ISO/DIS 4413:2008, *Hydraulic fluid power — General rules relating to systems*

[6] ISO/DIS 4414:2008, *Pneumatic fluid power — General rules and safety requirements for systems and their components*

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

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

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

[10] ISO 12100-2:2003, *Safety of machinery — Basic concepts, general principles for design — Part 2: Technical principles*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[25] IEC 61249-2, *Materials for printed boards and other interconnecting structures*

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

[27] IEC 61810 (alle Teile), *Electromechanical elementary relays — Part 1: General and safety requirements*

[28] Test Method for Measuring Whisker Growth on Tin and Alloy Surfaces Finishes, JESD22A121.01, JEDEC Solid State Technology Association, 2500 Wilson Boulevard Arlington, VA 22201-3834, www.jedec.org/download/search/22a1121-01.pdf

[29] Environmental Acceptance Requirements for Tin Whisker Susceptibility of Tin and Alloy Surface Finishes, JESD201, JEDEC Solid State Technology Association, 2500 Wilson Boulevard Arlington, VA 22201-3834, www.jedec.org/download/search/JESD201.pdf