

DIN EN ISO 13849-2



ICS 13.110

Entwurf

Einsprüche bis 2026-04-06
Vorgesehen als Ersatz für
DIN EN ISO 13849-2:2013-02

**Sicherheit von Maschinen –
Sicherheitsbezogene Teile von Steuerungen –
Teil 2: Anwendung von Design- und Validierungsprinzipien
(ISO/DIS 13849-2:2026);
Deutsche und Englische Fassung prEN ISO 13849-2:2026**

Safety of machinery –
Safety-related parts of control systems –
Part 2: Application of principles for the design and validation (ISO/DIS 13849-2:2026);
German and English version prEN ISO 13849-2:2026

Sécurité des machines –
Parties des systèmes de commande relatives à la sécurité –
Partie 2: Validation (ISO/DIS 13849-2:2026);
Version allemande et anglaise prEN ISO 13849-2:2026

Anwendungswarnvermerk

Dieser Entwurf mit Erscheinungsdatum 2026-02-06 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nasg@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Sicherheitstechnische Grundsätze (NASG), 10772 Berlin oder Am DIN-Platz, Burggrafenstr. 6, 10787 Berlin.

Es wird gebeten, mit den Kommentaren zu diesem Entwurf jegliche relevanten Patentrechte, die bekannt sind, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 156 Seiten

DIN-Normenausschuss Sicherheitstechnische Grundsätze (NASG)



Nationales Vorwort

Dieses Dokument enthält sicherheitstechnische Festlegungen.

Dieses Dokument (prEN ISO 13849-2:2026) wurde vom Technischen Komitee ISO/TC 199 „Safety of machinery“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 114 „Sicherheit von Maschinen und Geräten“ erarbeitet, dessen Sekretariat von DIN (Deutschland) gehalten wird.

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

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

Für die in diesem Dokument zitierten Dokumente können die entsprechenden deutschen Dokumente kostenlos auf der DIN-Media-Homepage recherchiert werden.

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

Änderungen

Gegenüber DIN EN ISO 13849-2:2013-02 wurden folgende Änderungen vorgenommen:

- a) Anpassung von Titel und Anwendungsbereich;
- b) ehemals Abschnitt 4 bis Abschnitt 12 wurde nach ISO 13849-1:2023 verschoben;
- c) ein neuer Abschnitt 4 führt die Anwendung von grundlegenden und bewährten Sicherheitsprinzipien, bewährten Bauteilen, Fehlern und Fehlerausschlüssen einschließlich Leitlinien für typische Ansätze zur Erfüllung der Prinzipien in einer neuen Tabelle 2 ein;
- d) neue Leitlinien in Tabelle A.3, Tabelle B.3, Tabelle C.3 und Tabelle D.3 für bewährte Bauteile;
- e) neue Tabelle D.22 zu Übertragungsfehlern;
- f) neuer Abschnitt D.3 zu Soft-Errors;
- g) Streichung von Anhang E.

Februar 2026

prEN ISO 13849-2

**Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 2:
Anwendung von Design- und Validierungsprinzipien (ISO/DIS 13849-2:2026)**

Safety of machinery – Safety-related parts of control systems – Part 2: Application of principles for the design and validation (ISO/DIS 13849-2:2026)

Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 2: Validation (ISO/DIS 13849-2:2026)

Inhalt

	Seite
Europäisches Vorwort	5
Anhang ZAA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der abzudeckenden Richtlinie 2006/42/EG	6
Anhang ZBB (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der abzudeckenden Verordnung (EU) 2023/1230	8
Vorwort	10
Einleitung	12
1 Anwendungsbereich	13
2 Normative Verweisungen	13
3 Begriffe	13
4 Entwurf und Validierung	13
4.1 Allgemeines	13
4.2 Integration von Sicherheitsprinzipien und Fehlerausschlüssen	16
Anhang A (informativ) Validierungswerkzeuge für mechanische Systeme	19
Anhang B (informativ) Validierungswerkzeuge für pneumatische Systeme	27
Anhang C (informativ) Validierungswerkzeuge für hydraulische Systeme	46
Anhang D (informativ) Validierungswerkzeuge für elektrische Systeme	63
D.1 Allgemeines	63
D.2 Fehlerausschluss	73
D.2.1 Allgemeines	73
D.2.2 „Zinn-Whisker“	73
D.2.3 Kurzschlüsse an auf Leiterplatten montierten Teilen	74
D.2.4 Fehlerausschlüsse und integrierte Schaltkreise	74
D.3 Soft-Errors	83
D.3.1 Allgemeines	83
D.3.2 Einführung in Soft-Errors	83
D.3.3 Bedeutung von Soft-Errors für die funktionale Sicherheit	83
D.3.4 Vermeiden und Beherrschen von Soft-Errors während des Entwurfs von Teilsystemen	84
D.3.5 Beispiel für die Darstellung des Beitrags von Soft-Errors zur PFH-Abschätzung	86
Literaturhinweise	88

Bilder

Bild 1 — Integration von grundlegenden Sicherheitsprinzipien, bewährten Sicherheitsprinzipien und Fehlerausschlüssen	18
Bild D.1 — Sicherheitsbezogenes Blockdiagramm für ein SRP/CS der Kategorie 2	86

Tabellen

Tabelle ZAA.1 — Übereinstimmung zwischen dieser Europäischen Norm und Anhang I der Richtlinie 2006/42/EG	6
Tabelle ZAA.2 — Anwendbare Normen, die die in diesem Anhang ZAA beschriebene Konformitätsvermutung begründen	6
Tabelle ZBB.1 — Zusammenhang zwischen dieser Europäischen Norm und Anhang III der Verordnung (EU) 2023/1230	8
Tabelle ZBB.2 — Anwendbare Normen, die die in diesem Anhang ZBB beschriebene Konformitätsvermutung begründen	9

Tabelle 1 — Gliederung von Anhang A bis Anhang D von ISO 13849-2	11
Tabelle 2 — Typische Ansätze bei der Erfüllung von grundlegenden und bewährten Sicherheitsprinzipien	15
Tabelle A.1 — Grundlegende Sicherheitsprinzipien	19
Tabelle A.2 — Bewährte Sicherheitsprinzipien	22
Tabelle A.3 — Bewährte Bauteile	24
Tabelle A.4 — Fehler und Fehlerausschlüsse — Mechanische Geräte, Bauteile und Elemente (z. B. Nocken, Stößel, Kette, Kupplung, Bremse, Welle, Schraube, Stift, Führung, Lager)	25
Tabelle A.5 — Fehler und Fehlerausschlüsse — Schraubendruckfedern	26
Tabelle B.1 — Grundlegende Sicherheitsprinzipien	27
Tabelle B.2 — Bewährte Sicherheitsprinzipien	30
Tabelle B.3 — Bewährte Bauteile	33
Tabelle B.4 — Fehler und Fehlerausschlüsse — Wegeventile	35
Tabelle B.5 — Fehler und Fehlerausschlüsse — Absperr-/Abschaltventile/Rückschlagventile/Schnellentlüftungsventile/Wechselventile usw.	36
Tabelle B.6 — Fehler und Fehlerausschlüsse — Stromventile	38
Tabelle B.7 — Fehler und Fehlerausschlüsse — Druckventile	39
Tabelle B.8 — Fehler und Fehlerausschlüsse — Rohrleitungen	40
Tabelle B.9 — Fehler und Fehlerausschlüsse — Schlauchleitungen	41
Tabelle B.10 — Fehler und Fehlerausschlüsse — Verbindungselemente	41
Tabelle B.11 — Fehler und Fehlerausschlüsse — Druckübersetzer und Druckmittelwandler	43
Tabelle B.12 — Fehler und Fehlerausschlüsse — Druckluftbehandlung — Filter	43
Tabelle B.13 — Fehler und Fehlerausschlüsse — Druckluftbehandlung — Öler	43
Tabelle B.14 — Fehler und Fehlerausschlüsse — Druckluftbehandlung — Schalldämpfer	44
Tabelle B.15 — Fehler und Fehlerausschlüsse — Energiespeicher und Druckbehälter	44
Tabelle B.16 — Fehler und Fehlerausschlüsse — Sensoren	44
Tabelle B.17 — Fehler und Fehlerausschlüsse — Informationsverarbeitung — Verknüpfungsglieder	44
Tabelle B.18 — Fehler und Fehlerausschlüsse — Informationsverarbeitung — Verzögerungsglieder	44
Tabelle B.19 — Fehler und Fehlerausschlüsse — Informationsverarbeitung — Umformer	45
Tabelle C.1 — Grundlegende Sicherheitsprinzipien	46
Tabelle C.2 — Bewährte Sicherheitsprinzipien	49
Tabelle C.3 — Bewährte Bauteile	52
Tabelle C.4 — Fehler und Fehlerausschlüsse — Wegeventile	55
Tabelle C.5 — Fehler und Fehlerausschlüsse — Absperr-/Abschaltventile/Rückschlagventile/Wechselventile usw.	57
Tabelle C.6 — Fehler und Fehlerausschlüsse — Stromventile	58
Tabelle C.7 — Fehler und Fehlerausschlüsse — Druckventile	60
Tabelle C.8 — Fehler und Fehlerausschlüsse — Rohrleitungen aus Metall	61
Tabelle C.9 — Fehler und Fehlerausschlüsse — Schlauchleitungen	61
Tabelle C.10 — Fehler und Fehlerausschlüsse — Verbindungselemente	61
Tabelle C.11 — Fehler und Fehlerausschlüsse — Filter	62
Tabelle C.12 — Fehler und Fehlerausschlüsse — Energiespeicher	62
Tabelle C.13 — Fehler und Fehlerausschlüsse — Sensoren	62
Tabelle D.1 — Grundlegende Sicherheitsprinzipien	63
Tabelle D.2 — Bewährte Sicherheitsprinzipien	67
Tabelle D.3 — Bewährte Bauteile	69
Tabelle D.4 — Fehler und Fehlerausschlüsse — Leitungen/Kabel	74
Tabelle D.5 — Fehler und Fehlerausschlüsse — Leiterplatten/bestückte Leiterplatten	75
Tabelle D.6 — Fehler und Fehlerausschlüsse — Klemmstellen	75
Tabelle D.7 — Fehler und Fehlerausschlüsse — Mehrpolige Steckverbindungen	76
Tabelle D.8 — Fehler und Fehlerausschlüsse — Schalter — Elektromechanische Positionsschalter, Handschalter (z. B. Drucktaster, Rücksetzschalter, DIP-Schalter, magnetisch betätigte Kontakte, Reedschalter, Druckschalter, Temperaturschalter)	76

Tabelle D.9 — Fehler und Fehlerausschlüsse — Schalter — Elektromechanische Einrichtungen (z. B. Relais, Schütze und Ventilschalter)	77
Tabelle D.10 — Fehler und Fehlerausschlüsse — Schalter — Näherungsschalter	77
Tabelle D.11 — Fehler und Fehlerausschlüsse — Schalter — Magnetventile	78
Tabelle D.12 — Fehler und Fehlerausschlüsse — Einzelne elektrische Bauteile — Transformatoren	78
Tabelle D.13 — Fehler und Fehlerausschlüsse — Einzelne elektrische Bauteile — Induktivitäten	79
Tabelle D.14 — Fehler und Fehlerausschlüsse — Einzelne elektrische Bauteile — Widerstände	79
Tabelle D.15 — Fehler und Fehlerausschlüsse — Einzelne elektrische Bauteile — Widerstandsnetzwerke	80
Tabelle D.16 — Fehler und Fehlerausschlüsse — Einzelne elektrische Bauteile — Potentiometer	80
Tabelle D.17 — Fehler und Fehlerausschlüsse — Einzelne elektrische Bauteile — Kondensatoren	80
Tabelle D.18 — Fehler und Fehlerausschlüsse — Elektronische Bauteile — Diskrete Halbleiter (z. B. Dioden, Zener-Dioden, Transistoren, Triacs, Thyristoren, Spannungsregler, Quarzkrystall, Phototransistoren, lichtemittierende Dioden [LEDs])	80
Tabelle D.19 — Fehlern und Fehlerausschlüssen — Elektronische Bauteile — Koppler für galvanische Trennung (z. B. Optokoppler, kapazitive Koppler)	81
Tabelle D.20 — Fehler und Fehlerausschlüsse — Elektronische Bauteile — Nicht programmierbare und nicht komplexe integrierte Schaltkreise	81
Tabelle D.21 — Fehler und Fehlerausschlüsse — Elektronische Bauteile — Programmierbare oder komplexe integrierte Schaltkreise	82
Tabelle D.22 — Fehler und Fehlerausschlüsse — Übertragungsfehler in der digitalen Datenkommunikation	82

Europäisches Vorwort

Dieses Dokument (prEN ISO 13849-2:2026) wurde vom Technischen Komitee ISO/TC 199 „Safety of machinery“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 114 „Sicherheit von Maschinen und Geräten“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur parallelen Umfrage vorgelegt.

Dieses Dokument wird EN ISO 13849-2:2013 ersetzen.

Dieses Dokument wurde im Rahmen eines Normungsauftrages erarbeitet, den die Europäische Kommission und die Europäische Freihandelsassoziation CEN erteilt haben, und unterstützt grundlegende Anforderungen der EU-Verordnungen.

Zum Zusammenhang mit EU-Verordnungen siehe informative Anhang ZAA und Anhang ZBB, die Bestandteil dieses Dokuments sind.

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

Anerkennungsnotiz

Der Text von ISO/DIS 13849-2:2026 wurde von CEN als prEN ISO 13849-2:2026 ohne irgendeine Abänderung genehmigt.

Anhang ZAA (informativ)

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

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

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

**Tabelle ZAA.1 — Übereinstimmung zwischen dieser Europäischen Norm und Anhang I der
Richtlinie 2006/42/EG**

Die relevanten grundlegenden Anforderungen der Richtlinie 2006/42/EG	Abschnitt(e)/Unterabschnitt(e) dieser EN	Anmerkungen/Hinweise
1.2.1. Sicherheit und Zuverlässigkeit von Steuerungen	Abschnitt 4	

**Tabelle ZAA.2 — Anwendbare Normen, die die in diesem Anhang ZAA beschriebene
Konformitätsvermutung begründen**

Verweisung in Abschnitt 2	Ausgabe der Internationalen Norm	Titel	Ausgabe der entsprechenden Europäischen Norm
ISO 12100:2010	ISO 12100:2010	<i>Sicherheit von Maschinen — Allgemeine Gestaltungsleitsätze — Risikobeurteilung und Risikominderung</i>	EN ISO 12100:2010
ISO 13849-1:2023	ISO 13849-1:2023	<i>Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen — Teil 1: Allgemeine Gestaltungsleitsätze</i>	EN ISO 13849-1:2023

Die in Spalte 1 der Tabelle ZAA.2 aufgeführten Dokumente werden in diesem Dokument ganz oder teilweise normativ zitiert, d. h. sie sind für seine Anwendung unerlässlich. Das Erreichen der Konformitätsvermutung unterliegt der Anwendung der in Spalte 4 aufgeführten Normausgabe oder, wenn keine Ausgabe einer Europäischen Norm existiert, der in Spalte 2 der Tabelle ZAA.2 angegebenen Ausgabe der Internationalen Norm.

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

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

Anhang ZBB
(informativ)

**Zusammenhang zwischen dieser Europäischen Norm und den
grundlegenden Anforderungen der abzudeckenden
Verordnung (EU) 2023/1230**

Diese Europäische Norm wurde im Rahmen eines von der Europäischen Kommission erteilten Normungsauftrages C(2025)121 final Durchführungsbeschluss (EU) der Kommission vom 20. Januar 2025 an das Europäische Komitee für Normung und das Europäische Komitee für Elektrotechnische Normung für Maschinen zur Unterstützung der Verordnung (EU) 2023/1230 des Europäischen Parlaments und des Rates (M/605) erarbeitet, um ein freiwilliges Mittel zur Erfüllung der grundlegenden Anforderungen der Verordnung (EU) 2023/1230 des Europäischen Parlaments und des Rates vom 14. Juni 2023 über Maschinen (ABl. L 165, 29.6.2023) bereitzustellen.

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

**Tabelle ZBB.1 — Zusammenhang zwischen dieser Europäischen Norm und Anhang III der
Verordnung (EU) 2023/1230**

Die relevanten grundlegenden Anforderungen der Verordnung (EU) 2023/1230	Abschnitt(e)/Unterabschnitt(e) dieser EN	Anmerkungen/Hinweise
1.2.1. Sicherheit und Zuverlässigkeit von Steuerungen	Abschnitt 4	Ausnahmen: 2. Absatz: (a) zweiter Teil: „... sowie beabsichtigten und unbeabsichtigten Fremdeinflüssen, einschließlich vernünftigerweise vorhersehbare böswillige Versuche Dritter, die zu einer Gefährdungssituation führen, standhalten können“, (d), (f) 3. Absatz: (a), (b), (c) 4. Absatz: (c)

**Tabelle ZBB.2 — Anwendbare Normen, die die in diesem Anhang ZBB beschriebene
Konformitätsvermutung begründen**

Verweisung in Abschnitt 2	Ausgabe der Internationalen Norm	Titel	Ausgabe der entsprechenden Europäischen Norm
ISO 12100:2010	ISO 12100:2010	<i>Sicherheit von Maschinen — Allgemeine Gestaltungsleitsätze — Risikobeurteilung und Risikominderung</i>	EN ISO 12100:2010
ISO 13849-1:2023	ISO 13849-1:2023	<i>Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen — Teil 1: Allgemeine Gestaltungsleitsätze</i>	EN ISO 13849-1:2023

Die in Spalte 1 der Tabelle ZBB.2 aufgeführten Dokumente werden in diesem Dokument ganz oder teilweise normativ zitiert, d. h. sie sind für seine Anwendung unerlässlich. Das Erreichen der Konformitätsvermutung unterliegt der Anwendung der in Spalte 4 aufgeführten Normausgabe oder, wenn keine Ausgabe einer Europäischen Norm existiert, der in Spalte 2 der Tabelle ZBB.2 angegebenen Ausgabe der Internationalen Norm.

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

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

Vorwort

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

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

ISO weist auf die Möglichkeit hin, dass die Anwendung dieses Dokuments mit der Verwendung eines oder mehrerer Patente verbunden sein kann. ISO bezieht jedoch in dieser Hinsicht keinerlei Stellung bezüglich Nachweis, Gültigkeit oder Anwendbarkeit jeglicher beanspruchten Patentrechte. Zum Zeitpunkt der Veröffentlichung dieses Dokuments lag ISO keine Mitteilung über ein Patent bzw. mehrere Patente vor, welche/s zur Umsetzung dieses Dokuments erforderlich sein könnte/n. Anwender werden jedoch darauf hingewiesen, dass dies möglicherweise nicht der aktuelle Informationsstand ist. Dieser kann jedoch der Patentdatenbank unter www.iso.org/patents entnommen werden. ISO ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

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

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

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

Diese dritte Ausgabe ersetzt die zweite Ausgabe (ISO 13849-2:2012), die technisch überarbeitet wurde.

Die wesentlichen Änderungen sind folgende:

- Anpassung von Titel und Anwendungsbereich;
- ehemals Abschnitt 4 bis Abschnitt 12 wurde nach ISO 13849-1:2023 verschoben;
- ein neuer Abschnitt 4 führt die Anwendung von grundlegenden und bewährten Sicherheitsprinzipien, bewährten Bauteilen, Fehlern und Fehlerausschlüssen einschließlich Leitlinien für typische Ansätze zur Erfüllung der Prinzipien in einer neuen Tabelle 2 ein;
- neue Leitlinien in Tabelle A.3, Tabelle B.3, Tabelle C.3 und Tabelle D.3 für bewährte Bauteile;
- neue Tabelle D.22 zu Übertragungsfehlern;
- neuer Abschnitt D.3 zu Soft-Errors;

- Streichung von Anhang E, der ein Beispiel für die Validierung von Fehlverhalten und Mitteln zur Diagnose enthält.

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

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

Anhang A, Anhang B, Anhang C und Anhang D, die informativ sind, sind entsprechend Tabelle 1 gegliedert.

Tabelle 1 — Gliederung von Anhang A bis Anhang D von ISO 13849-2

Anhang	Technologie	Liste der grundlegenden Sicherheitsprinzipien	Liste der bewährten Sicherheitsprinzipien	Liste der bewährten Bauteile	Fehlerlisten und Fehlerausschlüsse
		Tabelle(n)			
A	Mechanisch	Tabelle A.1	Tabelle A.2	Tabelle A.3	Tabelle A.4, Tabelle A.5
B	Pneumatisch	Tabelle B.1	Tabelle B.2	Tabelle B.3	Tabelle B.4 bis Tabelle B.19
C	Hydraulisch	Tabelle C.1	Tabelle C.2	Tabelle C.3	Tabelle C.4 bis Tabelle C.13
D	Elektrisch (einschließlich elektronisch)	Tabelle D.1	Tabelle D.2	Tabelle D.3	Tabelle D.4 bis Tabelle D.22

Einleitung

Sicherheitsnormen im Bereich von Maschinen sind wie folgt aufgebaut:

- 1) Typ-A-Normen (Sicherheitsgrundnormen) behandeln Grundbegriffe, Gestaltungsleitsätze und allgemeine Aspekte, die auf Maschinen angewandt werden können;
- 2) Typ-B-Normen (Sicherheitsfachgrundnormen) behandeln einen Sicherheitsaspekt oder eine Art von Schutzeinrichtung, die für eine ganze Reihe von Maschinen verwendet werden kann:
 - Typ-B1-Normen für bestimmte Sicherheitsaspekte (z. B. Sicherheitsabstände, Oberflächentemperatur, Lärm);
 - Typ-B2-Normen für Schutzeinrichtungen (z. B. Zweihandschaltungen, Verriegelungseinrichtungen, druckempfindliche Schutzeinrichtungen, trennende Schutzeinrichtungen);
- 3) Typ-C-Normen (Maschinensicherheitsnormen) behandeln detaillierte Sicherheitsanforderungen an eine bestimmte Maschine oder Gruppe von Maschinen.

Dieses Dokument ist eine Typ-B-Norm, wie in ISO 12100:2010 angegeben.

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

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

Dieses Dokument enthält Anforderungen an die Anwendung grundlegender und bewährter Sicherheitsprinzipien und Bedingungen für mögliche Fehlerausschlüsse.

Dieses Dokument enthält Leitlinien für den Entwurf und die Validierung von mechanischen, pneumatischen, hydraulischen und elektrischen Systemen für die sicherheitsbezogenen Teile einer Steuerung (SRP/CS) nach ISO 13849-1:2023.

Die meisten Angaben in diesem Dokument beruhen auf der Annahme, dass das in ISO 13849-1:2023, 6.1.8, beschriebene vereinfachte Verfahren zur Abschätzung des Performance Level (PL) angewendet wird.

Eine Anleitung zu den allgemeinen Gestaltungsleitsätzen (siehe ISO 12100:2010) von sicherheitsbezogenen Teilen von Steuerungen wird unabhängig von der Art der angewandten Technologie (elektrisch, hydraulisch, pneumatisch, mechanisch usw.) in ISO 13849-1 gegeben. Sie umfasst Beschreibungen einiger typischer Sicherheitsfunktionen, die Ermittlung ihrer erforderlichen Performance Level sowie allgemeine Anforderungen der Kategorien und Performance Level.

Innerhalb dieses Dokuments sind einige Validierungsangaben allgemeiner Art, während andere sich speziell auf die Art der angewandten Technik beziehen.

Die verantwortliche Arbeitsgruppe (ISO/TC 199/WG 8), die die Normenreihe ISO 13849 erarbeitet, wird Anwendungsbeispiele für ISO 13849-1 und ISO 13849-2 entwickeln, die in (einem) eigenständigen Dokument(en) der Normenreihe ISO 13849 veröffentlicht werden sollen, um den Anwender zusätzlich zu unterstützen.

1 Anwendungsbereich

Dieses Dokument enthält Anforderungen an die Anwendung grundlegender und bewährter Sicherheitsprinzipien, Informationen über bewährte Bauteile und Bedingungen für mögliche Fehlerausschlüsse. Dieses Dokument enthält Leitlinien für den Entwurf und die Validierung von mechanischen, pneumatischen, hydraulischen und elektrischen Systemen für die sicherheitsbezogenen Teile einer Steuerung (SRP/CS) nach ISO 13849-1:2023.

ANMERKUNG Zusätzliche Anforderungen an programmierbare elektronische Systeme einschließlich Embedded-Software sind in ISO 13849-1:2023, Abschnitt 7, und IEC 61508 (alle Teile) enthalten.

2 Normative Verweisungen

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

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

ISO 13849-1:2023, *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO 12100 und ISO 13849-1:2023.

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

- ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>
- IEC Electropedia: verfügbar unter <https://www.electropedia.org/>

4 Entwurf und Validierung

4.1 Allgemeines

Dieses Dokument unterstützt den Entwurf und die Validierung von SRP/CS nach ISO 13849-1:2023 durch Bereitstellung von zusätzlichen Informationen zu:

- grundlegenden und bewährten Sicherheitsprinzipien;
- bewährten Bauteilen;
- Fehlern und Fehlerausschlüssen.

Im Hinblick auf grundlegende und bewährte Sicherheitsprinzipien, bewährte Bauteile und Fehlerausschlüsse enthält ISO 13849-1:2023 Anforderungen an den Entwurf (besonders in 6.1.3, 6.1.10 und 6.1.11) und die Validierung (Abschnitt 10) von SRP/CS und deren Teilsystemen. ISO 13849-1:2023 konzentriert sich darauf, eine allgemeine Verknüpfung zwischen den Anforderungen der Sicherheitsprinzipien und den Kategorien herzustellen (siehe ISO 13849-1:2023, Tabelle 10) und allgemeine Anforderungen und Leitlinien für bewährte Bauteile, zu betrachtende Fehler und mögliche Fehlerausschlüsse anzugeben. Darüber hinaus werden allgemeine Validierungsprinzipien sowie Anforderungen und Leitlinien zur Validierung von SRP/CS und deren Teilsystemen angegeben.

E DIN EN ISO 13849-2:2026-03
prEN ISO 13849-2:2026 (D)

Dieses Dokument unterstützt den Entwurfs- und Validierungsprozess mittels spezifischer Listen von anwendbaren grundlegenden und bewährten Sicherheitsprinzipien, bewährten Bauteilen und möglichen Fehlerauschlüssen für verschiedene Technologien.

Die Listen beruhen auf Erfahrungen und Konsens innerhalb der internationalen Sicherheitsnormungsgemeinschaft und sind auf der Ebene allgemeiner Maschinen so detailliert wie möglich. Für eine bestimmte Anwendung können diese Listen basierend auf einer technischen Begründung ausgelegt und angepasst werden, um die allgemeinen Anforderungen von ISO 13849-1:2023 zu erfüllen.

Die Listen bilden einen umfassenden Ansatz, der auf verschiedene einzelne Anwendungen anwendbar ist, und sie sind nicht vollständig. Jegliche Abweichungen von den Listen in diesem Dokument müssen begründet und dokumentiert werden, siehe 4.2.

Für weitere Informationen siehe Tabelle A.1, Tabelle A.2, Tabelle A.3, Tabelle B.1, Tabelle B.2, Tabelle B.3, Tabelle C.1, Tabelle C.2, Tabelle C.3, Tabelle D.1, Tabelle D.2 und Tabelle D.3 in den Anhängen.

Tabelle 2 enthält Leitlinien zu typischen Ansätzen bei der Erfüllung der grundlegenden und bewährten Sicherheitsprinzipien.

Tabelle 2 — Typische Ansätze bei der Erfüllung von grundlegenden und bewährten Sicherheitsprinzipien

Entwurf und Herstellung von Bauteilen [M]	Entwurf von Teilsystemen [D]	Verwendung der Maschine [U]
— Erfüllung der relevanten Sicherheitsprinzipien bei Entwurf und Herstellung von Bauteilen [z. B. gesicherte Position, Verwendung bewährter Federn, ausreichend große positive Überdeckung in Schieberventilen (en: spool valves)]. — Spezifikation von Betriebsbedingungen und Anwendungsgrenzen für Entwurf und Anwendung, z. B. in Datenblättern sowie Einbau- und Betriebsanleitungen.	— Erfüllung der relevanten Sicherheitsprinzipien bei Integration von Bauteilen in Teilsysteme (z. B. Prinzip der Energietrennung, Druckbegrenzung). — Einhaltung der in den Einbau- und Betriebsanleitungen festgelegten Betriebsbedingungen und Anwendungsgrenzen für Bauteile. — Spezifikation von Betriebsbedingungen und Anwendungsgrenzen der Teilsysteme in der Maschine einschließlich der durch die integrierten Bauteile resultierenden Bedingungen (z. B. richtiger Temperaturbereich, ausreichende Maßnahmen zur Vermeidung von Verunreinigung des Druckmediums).	— Einhaltung der Betriebsbedingungen und Anwendungsgrenzen der Teilsysteme in der Maschine, die in den Benutzerinformationen und in den Einbau- und Betriebsanleitungen der Maschine enthalten sind (z. B. korrekter Temperaturbereich, ausreichende Maßnahmen zur Vermeidung von Verunreinigung des Druckmediums, Wartungsplan).

Tabelle 2 (fortgesetzt)

Entwurf und Herstellung von Bauteilen [M]	Entwurf von Teilsystemen [D]	Verwendung der Maschine [U]
ANMERKUNG 1 Mehrere Sicherheitsprinzipien sind von der Bauteilebene bis zur Verwendung der Maschine maßgebend, z. B. die Verwendung geeigneter Werkstoffe und eine angemessene Herstellung, richtige Dimensionierung und Formgebung, korrekte Auswahl, Kombination, Anordnung, Montage und Einbau von Bauteilen/Systemen. Diese Prinzipien sind üblicherweise für den Entwurf und die Herstellung von Bauteilen (z. B. korrekte Dimensionierung von Gehäusen), den Entwurf und die Integration von Bauteilen in Teilsysteme (z. B. richtige Dimensionierung von Bauteilparametern im Hinblick auf die erwartete Beanspruchung) und den Einbau und die Verwendung von Bauteilen und Teilsystemen (z. B. richtige Dimensionierung von Filtern und Wartungsintervallen) maßgebend. ANMERKUNG 2 Bei Entwurf und Herstellung von Bauteilen kann die Übereinstimmung mit Produktnormen hilfreich sein, um einige grundlegende oder bewährte Sicherheitsprinzipien zu erfüllen. In den meisten Fällen ist eine Übereinstimmung mit Produktnormen erforderlich, um das grundlegende Sicherheitsprinzip „Korrekte Auswahl, Kombination, Anordnungen, Zusammenbau und Einbau von Bauteilen oder Systemen für die jeweilige Anwendung“ zu erfüllen. ANMERKUNG 3 Die Spezifikation von Betriebsbedingungen und Anwendungsgrenzen, z. B. in Datenblättern sowie Einbau- und Betriebsanleitungen, zeigt in der Regel, dass die Sicherheitsprinzipien für den Entwurf und die Konstruktion eines Bauteils für die jeweilige Anwendung angewendet wurden. Weitere Informationen zu sicherheitsbezogenen Werten von Bauteilen oder Komponenten von Steuerungen können ISO 13849-1:2023, Anhang O, entnommen werden.		

Zur Unterstützung von Entwurf und Validierung siehe:

- Anhang A für mechanische Systeme;
- Anhang B für pneumatische Systeme;
- Anhang C für hydraulische Systeme;
- Anhang D für elektrische Systeme.

4.2 Integration von Sicherheitsprinzipien und Fehlerausschlüssen

Anwendbare grundlegende Sicherheitsprinzipien müssen für alle Kategorien angewendet werden.

Anwendbare bewährte Sicherheitsprinzipien müssen für die Kategorien 1, 2, 3 und 4 angewendet werden.

Jede Entscheidung, die besagt, dass ein Sicherheitsprinzip aus technischen Gründen oder aufgrund der Risikobeurteilung nicht anwendbar ist, muss begründet und detailliert dokumentiert werden. Dies bezieht sich auf die spezifische Anwendung und den Industriebereich, in dem das SRP/CS verwendet werden soll.

Es dürfen die maßgebenden Fehlerausschlüsse angewendet werden (siehe Tabelle A.4, Tabelle A.5, Tabelle B.4 bis Tabelle B.19, Tabelle C.4 bis Tabelle C.13 und Abschnitt D.2). Diese Fehlerausschlüsse müssen begründet und dokumentiert werden (siehe ISO 13849-1:2023, 6.1.10.3).

Es muss eine Analyse auf Grundlage der folgenden Kriterien durchgeführt werden, um nachzuweisen, welche Sicherheitsprinzipien für die spezifische Anwendung erforderlich sind:

- Nur die Sicherheitsprinzipien für die maßgebenden Technologien und die Entwurfsart sind erforderlich.

BEISPIEL 1 Für ein Pneumatikventil mit elektronischer Vorsteuerung sind

- Tabelle A.1 und Tabelle A.2 für den mechanischen Teil maßgebend,
- Tabelle B.1 und Tabelle B.2 für den pneumatischen Teil maßgebend, und
- Tabelle D.1 und Tabelle D.2 für den elektronischen Teil maßgebend.

BEISPIEL 2 Für einen elektromechanischen Endschalter sind Tabelle A.1 und Tabelle A.2 für den mechanischen Teil und Tabelle D.1 und Tabelle D.2 für den elektrischen Teil maßgebend.

BEISPIEL 3 Das bewährte Sicherheitsprinzip „ausreichend große positive Überdeckung in Schieberventilen“ gilt für Kolbenventile oder Schieberventile, aber nicht für Sitzventile oder Patronenventile.

BEISPIEL 4 Das bewährte Sicherheitsprinzip „durch den Lastdruck schließendes Ventil“ gilt für Sitzventile oder Patronenventile, aber nicht für Kolbenventile oder Schieberventile.

- Sicherheitsprinzipien, die aus technischen Gründen nicht anwendbar sind, dürfen durch andere Sicherheitsprinzipien oder alternative Maßnahmen ersetzt werden, welche die gleiche Wirkung erzielen. Ein bewährtes Sicherheitsprinzip darf nicht durch ein grundlegendes Sicherheitsprinzip ersetzt werden.

BEISPIEL 5 Wenn die Anwendung des grundlegenden Sicherheitsprinzips „Aufeinander folgendes Schalten bei Stromkreisen mit in Reihe geschalteten Kontakten redundanter Signale“ aus technischen Gründen nicht möglich ist, dann darf stattdessen das bewährte Sicherheitsprinzip „Begrenzung elektrischer Parameter“ (realisiert mittels Überlastschutz der Kontakte, z. B. durch die Verwendung einer Sicherung) angewendet werden, um das Verschweißen beider Kontakte zu verhindern.

Die Anwendung von Sicherheitsprinzipien für Teilsystemelemente kann auf eine der folgenden Weisen validiert werden:

- Die Benutzerinformationen (z. B. Datenblatt oder Anwendungshinweise) des Teilsystemelements enthalten die Bestätigung, dass alle zutreffenden Sicherheitsprinzipien, die für den Entwurf und die Herstellung des Teilsystemelements maßgebend sind, angewendet wurden.
- Die in den Benutzerinformationen (z. B. Datenblatt oder Anwendungshinweise) festgelegten Merkmale des Teilsystemelements bestätigen indirekt die Anwendung einiger Sicherheitsprinzipien für das Teilsystemelement.

ANMERKUNG 1 Üblicherweise ist es nicht erforderlich, die Gültigkeit dieser zugesicherten Eigenschaften während der Integration des Teilsystemelements zu validieren.

BEISPIEL 6 Das bewährte Sicherheitsprinzip „Überdimensionierung/Sicherheitsfaktor“ kann erfüllt werden, indem die maximale Last für eine elektrische Leistung im Verhältnis zur angegebenen maximalen Last unterbewertet wird. Überdimensionierung von umweltbezogenen Merkmalen wie beispielsweise Temperatur ist üblicherweise nicht erforderlich, wenn das Teilsystemelement nicht dauerhaft an den Grenzen der umweltbezogenen Merkmale betrieben wird.

Wenn bereits zuvor validierte Teilsysteme in SRP/CS integriert werden, braucht ihre Übereinstimmung mit den intern angewendeten Sicherheitsprinzipien nicht erneut validiert zu werden. Lediglich die Sicherheitsprinzipien, welche die externe Integration betreffen, müssen angewendet und validiert werden.

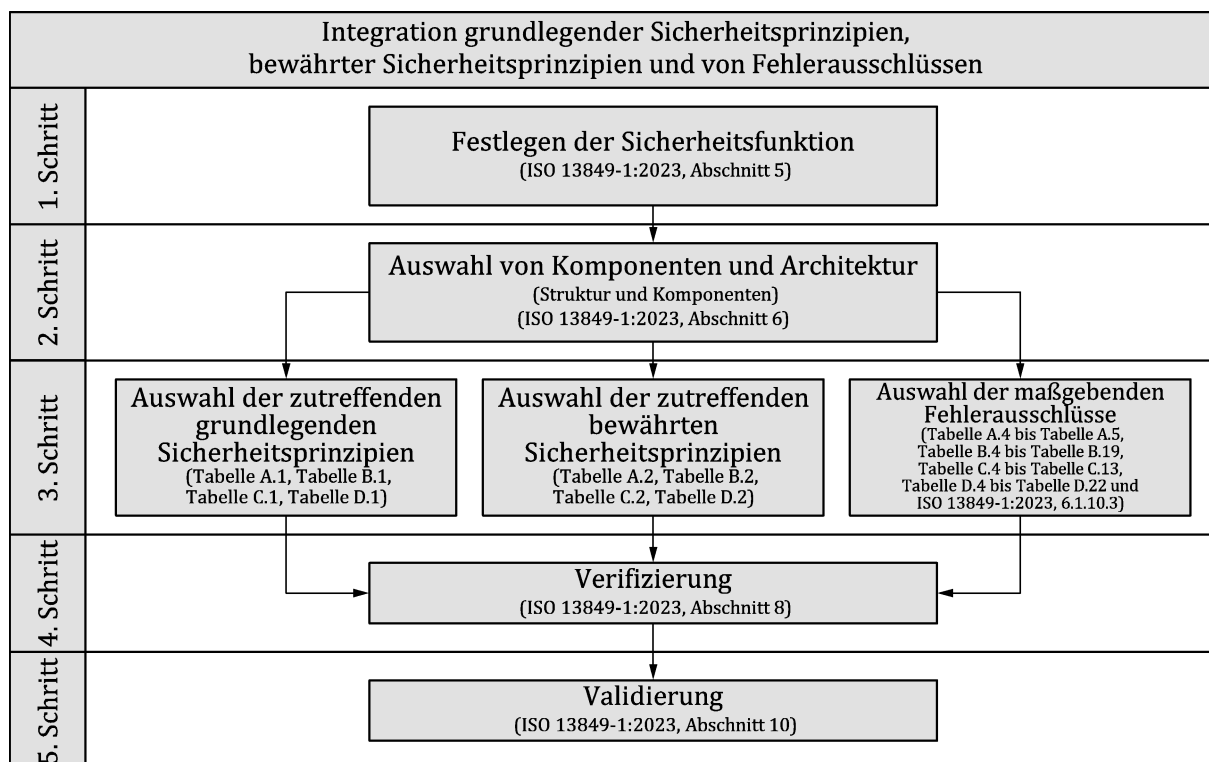
BEISPIEL 7 Die Parametrierung von Eingängen einer zuvor validierten sicherheitsbezogenen SPS wird während der Integration validiert.

ANMERKUNG 2 Ein Bauteil, das einer Typ-B2-Norm entspricht, wie z. B. ISO 14119:2024, *Sicherheit von Maschinen — Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen — Leitsätze für Gestaltung und Auswahl*, unterstützt üblicherweise die grundlegenden Sicherheitsprinzipien „Anwendung geeigneter Werkstoffe und Herstellungsverfahren“ und „richtige Dimensionierung und Formgebung“. Für die Integration dieses Bauteils in eine SRP/CS sind jedoch zahlreiche weitere anwendbare Sicherheitsprinzipien notwendig, z. B. „Anwendung des Prinzips der Energietrennung“, „Verträglichkeit“, „Beständigkeit gegen Umgebungsbedingungen“ oder „sichere Befestigung der Eingabegeräte“.

E DIN EN ISO 13849-2:2026-03
prEN ISO 13849-2:2026 (D)

ANMERKUNG 3 Wörter wie „widerstandsfähig“, „einfach“, „signifikant“, „ausreichend“ und ähnliche Ausdrücke sind dafür vorgesehen, die Anforderungen oder Empfehlungen hervorzuheben, und werden nicht durch Faktoren oder Einzelwerte quantifiziert. Solche Angaben finden sich in produktspezifischen Normen, wie z. B. Typ-C-Normen, und werden nicht in diesem Dokument angegeben. Die Benennung „gute ingenieurmäßige Praxis“ bezeichnet ein Verfahren zum Erreichen eines zuverlässigen SRP/CS durch die systematische Anwendung bewährter Techniken, dokumentierte Verfahren, befähigtes Personal, Risikobeurteilung und -minderung und durch Verifizierungs- und Validierungstätigkeiten.

Bild 1 zeigt den Prozess der Integration von grundlegenden und bewährten Sicherheitsprinzipien sowie von Fehlerausschlüssen.



ANMERKUNG Bewährte Sicherheitsprinzipien sind für Kategorie B nicht obligatorisch, siehe ISO 13849-1:2023, Tabelle 10.

Bild 1 — Integration von grundlegenden Sicherheitsprinzipien, bewährten Sicherheitsprinzipien und Fehlerausschlüssen

Anhang A (informativ)

Validierungswerkzeuge für mechanische Systeme

Anhang A ist für mechanische Systeme anwendbar. Er sollte auch dann beachtet werden, wenn mechanische Systeme in Verbindung mit anderen Technologien verwendet werden.

Tabelle A.1 und Tabelle A.2 führen grundlegende und bewährte Sicherheitsprinzipien auf.

Die Verwendung von Bauteilen, die nach einer Produktnorm ausgelegt sind, kann zur Bestätigung einiger grundlegender oder bewährter Sicherheitsprinzipien hilfreich sein (siehe Tabelle 2, ANMERKUNG 2).

Die Erfüllung von Prinzipien kann von mehreren Beitragenden abhängen, die am SRP/CS-Entwurf beteiligt sind (siehe 4.1, Tabelle 2, umgesetzt in Spalte 3 von Tabelle A.1 und Tabelle A.2).

Der Status „bewährt“ ist in erster Linie anwendungsbezogen. Bauteile können als „bewährt“ beschrieben werden, falls diese ISO 13849-1:2023, 6.1.11, entsprechen. Ein für bestimmte Anwendungen bewährtes Bauteil könnte für andere Anwendungen ungeeignet sein. Der Status „bewährt“ bedeutet nicht, dass bei einem bewährten Bauteil alle Fehler ausgeschlossen werden können.

In Tabelle A.4 und Tabelle A.5 werden Fehlerausschlüsse und die zugehörigen Begründungen aufgeführt.

Tabelle A.1 — Grundlegende Sicherheitsprinzipien

Grundlegendes Sicherheitsprinzip	Bemerkungen	Maßgebend für (siehe Tabelle 2)
Anwendung geeigneter Werkstoffe und Herstellungsverfahren	Auswählen der Werkstoffe, der Herstellungs- und Behandlungsverfahren unter Berücksichtigung von z. B. Belastung, Haltbarkeit, Elastizität, Reibung, Verschleiß, Korrosion, Temperatur.	M, D
Richtige Dimensionierung und Formgebung	Berücksichtigen z. B. von Belastung, Spannung, Ermüdung, Oberflächenrauheit, Toleranzen, Hängenbleiben, Herstellungsverfahren.	M, D
Korrekte Auswahl, Kombination, Anordnungen, Zusammenbau und Einbau von Bauteilen oder Systemen für die jeweilige Anwendung	Anwenden der vom Hersteller bereitgestellten Einbau- und Betriebsanleitungen, z. B. Katalogblätter, Einbauanweisungen, Spezifikationen sowie Anwenden guter ingenieurmäßiger Praxis mit ähnlichen Bauteilen oder Systemen.	M, D, U

Tabelle A.1 (fortgesetzt)

Grundlegendes Sicherheitsprinzip	Bemerkungen	Maßgebend für (siehe Tabelle 2)
Anwendung des Prinzips der Energietrennung Dieses Prinzip ist nicht anwendbar, wenn durch einen Energieverlust eine Gefährdung entsteht, z. B. Lösen eines Werkstücks durch den Verlust der Spann- bzw. Haltekraft.	Der sichere Zustand wird durch Trennen der Energie erreicht. Siehe primärer Vorgang zur Stillsetzung in ISO 12100:2010, 6.2.11.3. Zum Ingangsetzen der Bewegung eines Mechanismus wird Energie zugeführt. Siehe primärer Vorgang zur Inangangsetzung in ISO 12100:2010, 6.2.11.3. Berücksichtigen von unterschiedlichen Betriebsarten, z. B. Betriebsmodus, Instandhaltungsmodus. Zeitverzögernde Funktionen können erforderlich sein, um einen sicheren Zustand des Systems zu erreichen (siehe z. B. IEC 60204-1:2016 + AMD1:2021, 9.2.2).	M, D
Korrekte Befestigung	Für Schraubensicherungen werden die Einbau- und Betriebsanleitungen des Herstellers angewendet. Die Befestigung in der richtigen Orientierung und mit dem richtigen Drehmoment wird berücksichtigt. Durch Anwendung eines geeigneten Verfahrens zum Aufbringen des Drehmoments kann Überbeanspruchung vermieden und eine ausreichende Beständigkeit gegen das Lösen der Verbindung erreicht werden.	M, D, U
Beständigkeit gegen Umgebungsbedingungen (siehe ISO 13849-1:2023, Abschnitt 10, und Einbau- und Betriebsanleitungen des Herstellers befolgen)	Gestalten des Equipments, so dass es innerhalb der Umgebungsgrenzen der vorgesehenen Verwendung und bei allen vernünftigerweise vorhersehbaren ungünstigen Bedingungen, z. B. für Temperatur, Luftfeuchte, Schwingungen, Verunreinigungen, funktionieren kann.	M, D, U
Verhindern des Eindringens von festen Fremdkörpern und Fluiden	Anwenden eines geeigneten Schutzes gegen das Eindringen von festen Fremdkörpern und Fluiden.	M, D, U
Temperaturbereich	Externe und interne Temperatureinwirkungen werden für das gesamte System betrachtet.	M, D, U
Begrenzung von Geschwindigkeit, Beschleunigung und Ruck (um mechanische Beanspruchungen zu vermeiden oder zu begrenzen)	Berücksichtigen von Dämpfungsvorrichtungen, z. B. Feder.	M, D
Verringerung der Reaktionszeit	Minimieren der Verzögerung bei der Energietrennung der zum Schalten verwendeten Bauteile. Berücksichtigen von z. B. Ermüdung der Feder, Reibung, Schmierung, Temperatur, Trägheit bei Beschleunigung und Verzögerung, Kombination von Toleranzen.	M, D

Tabelle A.1 (fortgesetzt)

Grundlegendes Sicherheitsprinzip	Bemerkungen	Maßgebend für (siehe Tabelle 2)
Schutz gegen unerwarteten Anlauf (siehe ISO 12100:2010, 6.2.11.4, ISO 14118:2017)	Berücksichtigen von unerwartetem Anlauf, verursacht durch gespeicherte Energie und nach Wiederherstellung der Energieversorgung für unterschiedliche Betriebsarten, z. B. Betriebsmodus, Instandhaltungsmodus.	M, D
	Eine besondere Einrichtung zum Abbau der gespeicherten Energie kann notwendig sein. Besondere Anwendungen, z. B. zur Beibehaltung der Energie für Spanneinrichtungen oder zur Sicherung einer Position, müssen gesondert betrachtet werden.	M, D, U
Vereinfachung	Vermeiden von unnötigen Bauteilen im sicherheitsbezogenen System.	M, D
Trennung	Trennung der sicherheitsbezogenen Funktionen von anderen Funktionen.	M, D
Begrenzung der Erzeugung und/oder Übertragung von Kraft, Drehmoment (z. B. zur Vermeidung von Verschleiß) Dieses Prinzip ist nicht anwendbar, wenn die kontinuierliche Funktionsfähigkeit der Bauteile unerlässlich dafür ist, den notwendigen Grad der Steuerbarkeit beizubehalten.	Beispiele sind Scherstift, Scherplatte und Drehmomentbegrenzungskupplung.	M, D
Schmierung	Beachten der Notwendigkeit von Schmiervorrichtungen, Angaben zu Schmiermitteln und Schmierintervallen.	M, D, U
Abkürzungen M – Entwurf und Herstellung von Bauteilen D – Entwurf von Teilsystemen U – Verwendung der Maschine		

Tabelle A.2 — Bewährte Sicherheitsprinzipien

Bewährtes Sicherheitsprinzip	Bemerkungen	Maßgebend für (siehe Tabelle 2)
Verwendung sorgfältig ausgewählter Werkstoffe und Herstellungsverfahren	Auswahl der für die jeweilige Anwendung geeigneten Werkstoffe sowie geeigneter Herstellungs- und Behandlungsverfahren.	M, D
Verwendung von Bauteilen mit gerichtetem Ausfallverhalten (siehe ISO 12100:2010, 6.2.12.3)	Nach Möglichkeit Bauteile oder Systeme mit gerichtetem Ausfallverhalten verwenden. Ein sicherer Zustand wird direkt oder indirekt (z. B. durch Fehlererkennung) durch die überwiegend auftretende Ausfallart erzielt.	M, D
Überdimensionierung	Unterbeanspruchung von Bauteilen, die in Sicherheitsschaltkreisen verwendet werden. Sicherheitsfaktoren sind in Normen angegeben oder beruhen auf guter ingenieurmäßiger Praxis in sicherheitsbezogenen Anwendungen.	M, D
Gesicherte Position	Das bewegliche Element des Bauteils wird mechanisch in einer der möglichen Positionen gehalten. Um die Position zu verändern, ist das Aufbringen von Kraft notwendig, insbesondere beim Verlassen einer gesicherten Position. Basiert die Umsetzung auf dem Reibschlussprinzip, ist die Reibkraft immer größer als die Störkräfte für die gesamte Gebrauchsdauer.	M, D
Erhöhte AUS-Kraft	Eine gesicherte Position oder ein sicherer Zustand wird dadurch erreicht, dass die AUS-Kraft gegenüber der EIN-Kraft erhöht ist.	M, D
Sorgfältige Auswahl der Befestigungsart für die jeweilige Anwendung	Vermeiden, sich nur auf Reibung zu verlassen, z. B. Verwendung von eng anliegenden Verbindungen wie festschraubige Befestigungen, von werkstoffgebundenen Verbindungen wie Kleben/Schweißen/Löten/Vulkanisieren, von Sicherungsmuttern.	M, D
Mechanisch zwangsläufige Wirkung (siehe ISO 12100:2010, 6.2.5.)	Um eine mechanisch zwangsläufige (oder direkte) Wirkung zu erreichen, werden mechanische Bauteile, die zur Ausführung der Sicherheitsfunktion erforderlich sind, entweder durch direkten Kontakt oder über starre Elemente bewegt, z. B. ein Nocken öffnet die Kontakte eines elektrischen Schalters direkt, statt auf eine Feder angewiesen zu sein.	M, D
Vervielfachung von Teilen	Verringerung der Auswirkung von Fehlern durch Verwendung mehrerer gleicher Teile, die parallel zueinander wirken, z. B. wenn ein Ausfall, der an einer von mehreren Federn auftritt, keinen gefährlichen Zustand bewirkt.	M, D
Verwendung bewährter Federn	Siehe Tabelle A.3	M, D

Tabelle A.2 (*fortgesetzt*)

Bewährtes Sicherheitsprinzip	Bemerkungen	Maßgebend für (siehe Tabelle 2)
Begrenzter Bereich der Kraft und ähnlicher Parameter Dieses Prinzip ist nicht anwendbar, wenn die kontinuierliche Funktionsfähigkeit der Bauteile unerlässlich dafür ist, den notwendigen Grad der Steuerbarkeit beizubehalten.	Spezifikation der notwendigen Begrenzung in Abhängigkeit von Erfahrungen und der jeweiligen Anwendung. Beispiele sind Scherstift, Scherplatte, Drehmomentbegrenzungskupplung.	M, D
Begrenzter Bereich der Geschwindigkeit und ähnlicher Parameter	Spezifikation der notwendigen Begrenzung in Abhängigkeit von Erfahrungen und der jeweiligen Anwendung. Beispiele sind Fliehkraftregler, sichere Überwachung der Geschwindigkeit und Wegbegrenzung.	M, D, U
Begrenzter Bereich der Umgebungsparameter Siehe ISO 13849-1:2023, 10.7	Spezifikation der notwendigen Begrenzungen. Beispiele sind Temperatur, Luftfeuchte, Verunreinigung beim Einbau. Einhalten der Einbau- und Betriebsanleitungen des Herstellers.	M, D, U
Begrenzter Bereich der Reaktionszeit, Begrenzung der Hysterese	Spezifikation der notwendigen Begrenzungen. Z.B. Ermüdung der Feder, Reibung, Schmierung, Temperatur, Trägheit bei Beschleunigung und Verzögerung, Kombination von Toleranzen.	M, D
Abkürzungen M – Entwurf und Herstellung von Bauteilen D – Entwurf von Teilsystemen U – Verwendung der Maschine		

Tabelle A.3 — Bewährte Bauteile

Bewährtes Bauteil	Bedingungen für „bewährt“	Norm oder Spezifikation
Schraube	Alle Faktoren, die auf die Schraubverbindung und die Anwendung einen Einfluss ausüben, sind zu berücksichtigen. Siehe Tabelle A.2.	Mechanische Verbindungen wie Schrauben, Muttern, Unterlegscheiben, Niete, Stifte, Bolzen usw. sind genormt.
Feder	Bewährte Federn zeichnen sich aus durch: — Verwendung 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, was durch eine Lebensdauerprüfung von z. B. einem Ventil mit eingebauter Feder oder anderweitig nachgewiesen werden kann).	Technische Spezifikationen für Federstähle und andere Sonderanwendungsfälle sind in EN 13906-1:2013 angegeben.
	Bewährte Schraubendruckfedern können auch gestaltet werden durch: — Verwendung sorgfältig ausgewählter Werkstoffe, Herstellungsverfahren (z. B. vor Anwendung vorgenommenes statisches und dynamisches Setzen) und Behandlungsverfahren (z. B. Walzen und Kugelstrahlen); — ausreichende Führung der Feder; — einen Abstand zwischen den Windungen bei unbelasteter Feder, der kleiner als der Drahtdurchmesser ist; und — eine ausreichende Kraft nach einem Bruch oder nach mehreren Brüchen wird aufrechterhalten (d. h. Bruch/Brüche führt/führen nicht zu einem gefährlichen Zustand). ANMERKUNG Druckfedern werden bevorzugt.	
Nocken	Alle Faktoren, die auf die Anordnung des Nockens (z. B. als Teil einer Verriegelung) Einfluss nehmen, sind zu berücksichtigen. Siehe Tabelle A.2.	Siehe ISO 14119:2024

Tabelle A.3 (fortgesetzt)

Bewährtes Bauteil	Bedingungen für „bewährt“	Norm oder Spezifikation
Sollbruchbolzen, Berstscheibe, Scherbolzen	Alle Faktoren, die auf die Anwendung Einfluss nehmen, sind zu berücksichtigen. Siehe Tabelle A.2.	Siehe ISO 4126-2:2018
Kolben	Führung des Kolbens derart, dass Festklemmen/Hängenbleiben ausgeschlossen werden kann. Der Kolben ist derart ausgelegt, dass die Kräfte zuverlässig übertragen werden können.	

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

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Verschleiß/Korrosion	Ja, wenn Werkstoff, (Über-)Dimensionierung, Herstellungsverfahren, Behandlungsverfahren und geeignete Schmierung entsprechend der festgelegten Lebensdauer sorgfältig ausgewählt sind (siehe auch Tabelle A.2).	Siehe ISO 13849-1:2023, 6.1.10
Lockern/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, Behandlungsverfahren und Herstellungsverfahren entsprechend der festgelegten Lebensdauer sorgfältig ausgewählt sind (siehe auch Tabelle A.2).	
Steifheit/Hängenbleiben	Ja, wenn Werkstoff, (Über-)Dimensionierung, Herstellungsverfahren, Behandlungsverfahren und geeignete Schmierung entsprechend der festgelegten Lebensdauer sorgfältig ausgewählt sind (siehe auch Tabelle A.2).	

Tabelle A.5 — Fehler und Fehlerausschlüsse — Schraubendruckfedern

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Verschleiß/Korrosion	Ja, bei Verwendung bewährter Federn und sorgfältig ausgewählter Befestigungsarten (siehe Tabelle A.3).	Siehe ISO 13849-1:2023, 6.1.10
Verringerung der Kraft durch bleibende Verformung und Bruch		
Bruch		
Steifheit/Hängenbleiben		
Lösen		
Verformung durch Überbeanspruchung		

Anhang B (informativ)

Validierungswerkzeuge für pneumatische Systeme

Anhang B ist für pneumatische Systeme anwendbar. Er sollte auch dann beachtet werden, wenn pneumatische Systeme in Verbindung mit anderen Technologien verwendet werden. Wenn pneumatische Bauteile elektrisch verbunden/gesteuert werden, sollten die entsprechenden Fehlerlisten im Anhang D berücksichtigt werden.

ANMERKUNG Zusätzliche Anforderungen können in nationalen Rechtsvorschriften enthalten sein.

Tabelle B.1 und Tabelle B.2 führen grundlegende und bewährte Sicherheitsprinzipien auf.

Die Verwendung von Bauteilen, die nach einer Produktnorm ausgelegt sind, kann zur Bestätigung einiger grundlegender oder bewährter Sicherheitsprinzipien hilfreich sein (siehe Tabelle 2, Anmerkung 2).

Die Erfüllung von Prinzipien kann von mehreren Beitragenden abhängen (siehe 4.1, Tabelle 2, umgesetzt in Spalte 3 von Tabelle B.1 und Tabelle B.2).

Der Status „bewährt“ ist in erster Linie anwendungsbezogen. Bauteile können als „bewährt“ beschrieben werden, falls diese ISO 13849-1:2023, 6.1.11, und ISO 4414:2010, Abschnitt 5 bis Abschnitt 7, entsprechen. Ein für bestimmte Anwendungen bewährtes Bauteil könnte für andere Anwendungen ungeeignet sein. Der Status „bewährt“ bedeutet nicht, dass bei einem bewährten Bauteil alle Fehler ausgeschlossen werden können

In Tabelle B.4 bis Tabelle B.19 werden Fehlerausschlüsse und die zugehörigen Begründungen aufgeführt.

Tabelle B.1 — Grundlegende Sicherheitsprinzipien

Grundlegendes Sicherheitsprinzip	Bemerkungen	Maßgebend für (siehe Tabelle 2)
Anwendung geeigneter Werkstoffe und Herstellungsverfahren	Auswahl des Werkstoffs, der Herstellungs- und Behandlungsverfahren unter Berücksichtigung von z. B. Belastung, Haltbarkeit, Elastizität, Reibung, Verschleiß, Korrosion, Temperatureigenschaften von Druckluft.	M, D
Richtige Dimensionierung und Formgebung	Berücksichtigen z. B. von Belastung, Spannung, Ermüdung, Oberflächenrauheit, Toleranzen, Hängenbleiben, Herstellungsverfahren.	M, D
Korrekte Auswahl, Kombination, Anordnungen, Zusammenbau und Einbau von Bauteilen oder Systemen für die jeweilige Anwendung	Anwenden der vom Hersteller bereitgestellten Einbau- und Betriebsanleitungen, z. B. Katalogblätter, Einbauanweisungen, Spezifikationen sowie Anwenden guter ingenieurmäßiger Praxis mit ähnlichen Bauteilen oder Systemen.	M, D, U

Tabelle B.1 (fortgesetzt)

Grundlegendes Sicherheitsprinzip	Bemerkungen	Maßgebend für (siehe Tabelle 2)
Anwendung des Prinzips der Energietrennung Dieses Prinzip ist nicht anwendbar, wenn durch einen Energieverlust eine Gefährdung entsteht, z. B. Lösen eines Werkstücks durch den Verlust der Spann- bzw. Haltekraft.	Der sichere Zustand wird durch Trennen der Energie an allen relevanten Einrichtungen erreicht. Siehe primärer Vorgang zur Stillsetzung in ISO 12100:2010, 6.2.11.3. Zum Ingangsetzen der Bewegung eines Mechanismus wird Energie zugeführt. Siehe primärer Vorgang zur Ingangsetzung in ISO 12100:2010, 6.2.11.3. Berücksichtigen von unterschiedlichen Betriebsarten, z. B. Betriebsmodus, Instandhaltungsmodus. Zeitverzögernde Funktionen können erforderlich sein, um einen sicheren Zustand des Systems zu erreichen (siehe z. B. IEC 60204-1:2016 + AMD1:2021, 9.2.2).	M, D
Korrekte Befestigung	Für Befestigungsmittel (z. B. Schraubensicherungen, Armaturen, Klebungen oder Spannringe) werden die Einbau- und Betriebsanleitungen des Herstellers angewendet. Die Befestigung in der richtigen Orientierung und mit dem richtigen Drehmoment wird berücksichtigt. Durch Anwendung eines geeigneten Verfahrens zum Aufbringen des Drehmoments kann Überbeanspruchung vermieden werden.	M, D, U
Beständigkeit gegen Umgebungsbedingungen (siehe ISO 13849-1:2023, Abschnitt 10, und Einbau- und Betriebsanleitungen des Herstellers befolgen)	Gestalten des Equipments, so dass es innerhalb der Umgebungsgrenzen der vorgesehenen Verwendung und bei allen vernünftigerweise vorhersehbaren ungünstigen Bedingungen, z. B. für Temperatur, Luftfeuchte, Schwingungen, Verunreinigungen, elektromagnetische Störung (EMI), funktionieren kann.	M, D, U
Verhindern des Eindringens von festen Fremdkörpern und Fluiden	Anwenden eines geeigneten Schutzes gegen das Eindringen von festen Fremdkörpern und Fluiden.	M, D, U
Temperaturbereich	Externe und interne Temperatureinwirkungen werden für das gesamte System betrachtet. (siehe ISO 4414:2010)	M, D, U

Tabelle B.1 (*fortgesetzt*)

Grundlegendes Sicherheitsprinzip	Bemerkungen	Maßgebend für (siehe Tabelle 2)
Begrenzung von Geschwindigkeit, Beschleunigung und Ruck (um mechanische Beanspruchungen zu vermeiden oder zu begrenzen)	Ein Beispiel ist die Geschwindigkeitsbegrenzung eines Kolbens durch ein Stromventil oder eine Drossel.	M, D
Verringerung der Reaktionszeit	Minimieren der Verzögerung bei der Energietrennung der zum Schalten verwendeten Bauteile. Angemessener Bereich der Schaltzeiten, z. B. der Länge der Rohrleitung, Druck, Entlüftungskapazität, Kraft, Ermüdung der Feder, Reibung, Schmierung, Temperatur, Trägheit bei Beschleunigung und Verzögerung, Frequenzen, Stoßwellen, Kombination von Toleranzen.	M, D
Vereinfachung	Vermeiden von unnötigen Bauteilen im sicherheitsbezogenen System.	M, D
Schutz gegen unerwarteten Anlauf (siehe ISO 12100:2010, 6.2.11.4, ISO 14118:2017)	Berücksichtigen von unerwartetem Anlauf, verursacht durch gespeicherte Energie und nach Wiederherstellung der Energieversorgung, für unterschiedliche Betriebsarten, z. B. Betriebsmodus, Instandhaltungsmodus.	M, D
	Eine besondere Einrichtung zum Abbau der gespeicherten Energie kann notwendig sein. Besondere Anwendungen, z. B. zur Beibehaltung der Energie für Spanneinrichtungen oder zur Sicherung einer Position, müssen gesondert betrachtet werden.	M, D, U
Trennung	Trennung der sicherheitsbezogenen Funktionen von anderen Funktionen.	M, D
Druckbegrenzung (z. B. zur Vermeidung von Verschleiß)	Beispiele sind Druckentlastungsventile, Druckminder-/Druckregelventile.	M, D
Grundlegende Maßnahmen gegen eine Verunreinigung des Druckmediums	Berücksichtigen von Filtration und Abtrennung von Feststoffen und Wasser im Druckmedium. Verhindern einer Kontamination des Druckmediums durch externe Quellen während des Einbaus und der Handhabung der Bauteile. Berücksichtigen einer Anzeige, die angibt, dass der Filter ausgewechselt werden muss.	M, D, U

Tabelle B.1 (fortgesetzt)

Grundlegendes Sicherheitsprinzip	Bemerkungen	Maßgebend für (siehe Tabelle 2)
Korrekte Anwendung von vorgeschmierten/selbstschmierenden/mit Lebensdauerschmierung versehenen Ventilen	Verwenden von vorbehandelter ölfreier Luft entsprechend den Einbau- und Betriebsanleitungen des Herstellers, um Fettablagerungen zu vermeiden.	D, U
Abkürzungen M – Entwurf und Herstellung von Bauteilen D – Entwurf von Teilsystemen U – Verwendung der Maschine		

Tabelle B.2 — Bewährte Sicherheitsprinzipien

Bewährtes Sicherheitsprinzip	Bemerkungen	Maßgebend für (siehe Tabelle 2)
Verwendung von Bauteilen mit gerichtetem Ausfallverhalten (siehe ISO 12100:2010, 6.2.12.3)	Nach Möglichkeit Bauteile oder Systeme mit gerichtetem Ausfallverhalten verwenden. Ein sicherer Zustand wird direkt oder indirekt (z. B. durch Fehlererkennung) durch die überwiegend auftretende Ausfallart erzielt.	M, D
Überdimensionierung	Unterbeanspruchung von Bauteilen, die in Sicherheitsschaltkreisen verwendet werden, z. B. im Hinblick auf die Druckstufe, Temperaturstufe, Schalthäufigkeit. Sicherheitsfaktoren sind in Normen angegeben oder beruhen auf guter ingenieurmäßiger Praxis in sicherheitsbezogenen Anwendungen.	M, D
Gesicherte Position	Das bewegliche Element des Bauteils wird mechanisch in einer der möglichen Positionen gehalten. Um die Position zu verändern, ist das Aufbringen von Kraft notwendig. Basiert die Umsetzung auf dem Reibschlussprinzip, ist die Reibkraft immer größer als die Störkräfte für die gesamte Gebrauchsdauer.	M, D
Erhöhte AUS-Kraft	Eine sichere Stellung oder ein sicherer Zustand wird dadurch erreicht, dass die AUS-Kraft gegenüber der EIN-Kraft erhöht ist. Eine Lösung kann sein, dass das Flächenverhältnis für die Bewegung eines Ventilschiebers in die sichere Position (AUS-Stellung) gegenüber der Bewegung des Ventilschiebers in die EIN-Stellung wesentlich größer ist.	M, D

Tabelle B.2 (*fortgesetzt*)

Bewährtes Sicherheitsprinzip	Bemerkungen	Maßgebend für (siehe Tabelle 2)
Durch den Lastdruck schließendes Ventil	Dies sind im Allgemeinen, aber nicht ausschließlich, Sitzventile, z. B. Kegelsitzventile, Kugelventile. Es wird berücksichtigt, wie der Lastdruck aufzubringen ist, um das Ventil auch dann geschlossen zu halten, wenn z. B. die Schließfeder des Ventils bricht. ANMERKUNG Hohe Schließgeschwindigkeiten können Ventilprellen hervorrufen.	M, D
Mechanisch zwangsläufige Wirkung (siehe ISO 12100:2010, 6.2.5.)	Die mechanisch zwangsläufige Wirkung wird für die beweglichen Teile innerhalb der pneumatischen Bauteile angewendet. Um eine mechanisch zwangsläufige (oder direkte) Wirkung zu erreichen, werden mechanische Bauteile, die zur Ausführung der Sicherheitsfunktion erforderlich sind, entweder durch direkten Kontakt oder über starre Elemente bewegt.	M, D
Verwendung bewährter Federn	Siehe Tabelle A.3.	M
Begrenzter Bereich der Kraft und ähnlicher Parameter, um mechanische Beanspruchungen zu vermeiden oder zu begrenzen Dieses Prinzip ist nicht anwendbar, wenn die kontinuierliche Funktionsfähigkeit der Bauteile unerlässlich dafür ist, den notwendigen Grad der Steuerbarkeit beizubehalten.	Spezifikation der notwendigen Begrenzung in Abhängigkeit von Erfahrungen und der jeweiligen Anwendung. Dies kann erreicht werden durch ein bewährtes Druckentlastungsventil, das z. B. mit einer bewährten Feder ausgestattet und richtig dimensioniert und ausgewählt ist.	M, D
Begrenzter Bereich der Geschwindigkeit und ähnlicher Parameter	Spezifikation der notwendigen Begrenzung in Abhängigkeit von Erfahrungen und der jeweiligen Anwendung. Beispiele sind Festblende und Festdrossel, um durch den Widerstand gegenüber einer bestimmten Flüssigkeitsströmung die Geschwindigkeit zu verringern.	M, D, U
Begrenzter Bereich der Umgebungsparameter Siehe ISO 13849-1:2023, 10.7	Spezifikation der notwendigen Begrenzungen. Beispiele sind Temperatur, Luftfeuchte, Verunreinigung beim Einbau. Einhalten der Einbau- und Betriebsanleitungen des Herstellers.	M, D, U
Begrenzter Bereich der Reaktionszeit, Begrenzung der Hysterese	Spezifikation der notwendigen Begrenzungen. Die Hysterese erhöht sich z. B. durch stärkere Reibung. Eine Kombination von Toleranzen beeinflusst die Hysterese ebenfalls.	M, D

Tabelle B.2 (*fortgesetzt*)

Bewährtes Sicherheitsprinzip	Bemerkungen	Maßgebend für (siehe Tabelle 2)
Geeigneter Bereich der Betriebsbedingungen	Die Begrenzung der Betriebsbedingungen, z. B. Druck-, Volumenstrom- und Temperaturbereich, wird berücksichtigt.	M, D, U
Verbesserte Maßnahmen gegen eine Verunreinigung des Druckmediums	Berücksichtigung der Notwendigkeit einer feineren Filtration und Abscheidung von Feststoffen und Wasser im Druckmedium.	M, D, U
Ausreichend große positive Überdeckung in Schieberventilen oder Kolbenschieberventilen	Die positive Überdeckung sichert die Anhaltefunktion und verhindert gefährliche Bewegungen.	M
Ausreichend große Unterdeckung in Schieberventilen	Entlüftungsanwendungen in redundanten Systemen.	M
Regelmäßige Bewertung des Zustandes des Druckmediums	Anwenden einer hoch wirksamen Filtration oder Abscheidung von Feststoffen, Wasser und Verunreinigungen im Druckmedium und ein Hinweis auf die Notwendigkeit des Auswechselns des Filters. Bewerten der physikalischen Eigenschaften des Druckmediums.	M, D, U
Abkürzungen M – Entwurf und Herstellung von Bauteilen D – Entwurf von Teilsystemen U – Verwendung der Maschine		

Tabelle B.3 — Bewährte Bauteile

Bewährtes Bauteil	Bedingungen für „bewährt“	Norm oder Spezifikation
Berstscheibe	Alle Faktoren, die auf die Anwendung Einfluss nehmen, sind zu berücksichtigen. Siehe Tabelle B.1 und Tabelle B.2.	Technische Spezifikationen für Berstscheiben/flache Berstscheiben und andere Sonderanwendungsfälle sind in ISO 4126-2:2018 angegeben.
Wegeventil (elektrisch oder ferngesteuert oder vorgesteuert)	Nur bewährt, wenn: a) das Bauteil die grundlegenden und bewährten Sicherheitsprinzipien im Hinblick auf die vorgesehene Anwendung erfüllt, einschließlich der Verwendung des Bauteils entsprechend den Spezifikationen des Herstellers; b) das Bauteil nachweislich in der Vergangenheit in zahlreichen Fällen mit dokumentierten erfolgreichen Ergebnissen bei ähnlichen Anwendungen im Einsatz war oder das Bauteil mittels Prinzipien, die seine Eignung und Zuverlässigkeit für sicherheitsbezogene Anwendungen entsprechend den Produkt- und Anwendungsnormen belegen, hergestellt, verifiziert und validiert wurde; c) entweder keine Onboard-Elektronik vorhanden ist oder wenn die Onboard-Elektronik, soweit vorhanden, nicht zur Ausführung der Sicherheitsfunktion beiträgt (siehe ANMERKUNG 3); d) das Verhalten des Bauteils unter allen Bedingungen klar definiert ist und vollständig bestimmt werden kann; und e) die folgenden Konstruktionsmerkmale erfüllt sind: — einfache, widerstandsfähige Auslegung; — formschlüssige Verbindung; — ausreichender Schutz gegen das Lösen von abnehmbaren Verbindungen; — ausreichend widerstandsfähig in Bezug auf die Verwendung (Anwendung) und die Umgebungsbedingungen (z. B. Druckschwankungen, Vibration); — von einer Feder aufgebrachte Rückstellkraft zur Rückstellung in eine gesicherte Position; — Verwendung bewährter Federn (siehe Tabelle A.3); und — ausreichende Dichtheit in Sperrrichtung.	ISO 13849-1:2023, 6.1.3.2.3, 6.1.11

Tabelle B.3 (fortgesetzt)

Bewährtes Bauteil	Bedingungen für „bewährt“	Norm oder Spezifikation
Druckschalter	Nur bewährt, wenn: a) das Bauteil die grundlegenden und bewährten Sicherheitsprinzipien im Hinblick auf die vorgesehene Anwendung erfüllt, einschließlich der Verwendung des Bauteils entsprechend den Spezifikationen des Herstellers; b) das Bauteil nachweislich in der Vergangenheit in zahlreichen Fällen mit dokumentierten erfolgreichen Ergebnissen bei ähnlichen Anwendungen im Einsatz war oder das Bauteil mittels Prinzipien, die seine Eignung und Zuverlässigkeit für sicherheitsbezogene Anwendungen entsprechend den Produkt- und Anwendungsnormen belegen, hergestellt, verifiziert und validiert wurde; c) entweder keine Onboard-Elektronik vorhanden ist oder wenn die Onboard-Elektronik, soweit vorhanden, nicht zur Ausführung der Sicherheitsfunktion beiträgt; d) das Verhalten des Bauteils unter allen Bedingungen klar definiert ist und vollständig bestimmt werden kann; und e) die folgenden Konstruktionsmerkmale erfüllt sind: — einfache, widerstandsfähige Auslegung; — formschlüssige Verbindung; — ausreichender Schutz gegen das Lösen von abnehmbaren Verbindungen; — ausreichend widerstandsfähig in Bezug auf die Verwendung (Anwendung) und die Umgebungsbedingungen (z. B. Druckschwankungen, Vibration); und — ausreichende Dimensionierung der Feder.	ISO 13849-1:2023, 6.1.3.2.3, 6.1.11 Für den elektrischen Teil siehe IEC 6094751:2024.
ANMERKUNG 1 Die Bestätigung von grundlegenden und bewährten Sicherheitsprinzipien und der Nachweis für den Einsatz in der Vergangenheit in zahlreichen Fällen mit dokumentierten erfolgreichen Ergebnissen bei ähnlichen Anwendungen können vom Bauteilhersteller oder vom Konstrukteur des Teilsystems erbracht werden. ANMERKUNG 2 Beispiele für Wegeventile können Ventilarten mit diskreten (spezifischen) Positionen sein: Absperr-/Abschaltventil, Schieberventil, UND-Ventil, Wechselventil, Rückschlagventil, Sperrventil, Auslassventil, Druckentlastungsventil. ANMERKUNG 3 Digitale Kommunikationseinheiten für Ventilblöcke oder Druckschalter sind komplex und erfüllen nicht die Bedingungen, um als bewährt zu gelten. Bewirkt eine Unterbrechung der Energiezufuhr einen sicheren Zustand der Ventile und kann ein Fehlerausschluss für Querschluss zwischen der Energiezufuhr und dem Steuerbus erfolgen (siehe Anhang D), und sind für die eingebauten Ventile die Bedingungen für „bewährt“ erfüllt, kann der Ventilblock als bewährtes Bauteil angesehen werden.		

Tabelle B.4 — Fehler und Fehlerausschlüsse — Wegeventile

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Veränderung der Schaltzeiten	Ja, bei mechanisch zwangsläufiger Wirkung (siehe Tabelle A.2) der beweglichen Bauteile, sofern die Betätigungskraft ausreichend groß ist.	—
Nichtschalten (Hängenbleiben in der End- oder Nulllage) oder nicht vollständiges Schalten (Hängenbleiben in einer beliebigen Zwischenstellung)	Ja, bei mechanisch zwangsläufiger Wirkung (siehe Tabelle A.2) der beweglichen Bauteile, sofern die Betätigungskraft ausreichend groß ist.	
Selbsttätige Veränderung der Ausgangs-Schaltstellung (ohne ein Eingangssignal)	Ja, bei mechanisch zwangsläufiger Wirkung (siehe Tabelle A.2) der beweglichen Bauteile, sofern die Haltekraft ausreichend groß ist, oder wenn bewährte Federn angewendet werden (siehe Tabelle A.3) und wenn übliche Einbau- und Betriebsbedingungen vorliegen (siehe Bemerkung), oder bei Schieberventilen mit elastischer Abdichtung und wenn übliche Einbau- und Betriebsbedingungen vorliegen (siehe Bemerkung).	Übliche Einbau- und Betriebsbedingungen liegen vor, wenn: — die vom Hersteller vorgegebenen Bedingungen befolgt wurden; — sich keine Massenträgheitskräfte nachteilig auf die bewegenden Bauteile auswirken (z. B. Bewegungsrichtung des Ventilbauteils berücksichtigt Größe und Richtung der Trägheitskräfte); und — die Schwingungs- und Schockbeanspruchungen kleiner sind als zulässig, und keine extremen Schwingungs- und Schockbeanspruchungen auftreten.
Leckage	Ja, bei Schieberventilen mit elastischer Abdichtung, sofern eine ausreichende positive Überdeckung vorhanden ist [siehe Bemerkung 1)], und wenn übliche Betriebsbedingungen vorliegen und die Druckluft ausreichend aufbereitet und filtriert ist, oder bei Sitzventilen, wenn übliche Betriebsbedingungen vorliegen [siehe Bemerkung 2)] und die Druckluft ausreichend aufbereitet und filtriert ist.	1) Bei Schieberventilen mit elastischer Abdichtung können Effekte durch eine Leckage in der Regel ausgeschlossen werden. Über eine längere Dauer kann jedoch eine geringe Leckage auftreten. 2) Übliche Betriebsbedingungen liegen vor, wenn die vom Hersteller vorgegebenen Bedingungen berücksichtigt werden.

Tabelle B.4 (fortgesetzt)

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Veränderung des Leckagevolumenstroms über eine lange Einsatzdauer	Nein.	—
Bersten des Ventilgehäuses oder Bruch des/der bewegten Bauteils/Bauteile sowie Bruch der Befestigungs- oder Gehäuseschrauben	Ja, wenn Konstruktion, Dimensionierung und Einbau guter ingenieurmäßiger Praxis entsprechen.	
Für Servo- und Proportionalventile: pneumatische Fehler, die unkontrolliertes Verhalten bewirken	Ja, bei Servo- und Proportionalwegeventilen, wenn sie bedingt durch ihre konstruktive Ausführung sicherheitstechnisch wie konventionelle Wegeventile beurteilt werden können.	—
ANMERKUNG Werden Steuerfunktionen durch individuelle Einzelfunktionen mehrerer Ventile realisiert, sollte eine Fehlerbetrachtung für jedes Ventil durchgeführt werden. Bei vorgesteuerten Ventilen sollte die gleiche Vorgehensweise angewendet werden.		

Tabelle B.5 — Fehler und Fehlerausschlüsse —

Absperr-/Abschaltventile/Rückschlagventile/Schnellentlüftungsventile/Wechselventile usw.

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Veränderung der Schaltzeiten	Nein.	—
Nichtöffnen, nicht vollständiges Öffnen, Nichtschließen oder nicht vollständiges Schließen (Hängenbleiben in einer Endlage oder in einer beliebigen Zwischenstellung)	Ja, wenn das Führungssystem für das/die bewegte(n) Bauteil(e) ähnlich ausgelegt ist wie bei einem nicht gesteuerten Kugelsitzventils ohne ein Dämpfungssystem (siehe Bemerkung) und wenn bewährte Federn verwendet werden (siehe Tabelle A.3).	Für ein nicht gesteuertes Kugelsitzventil ohne ein Dämpfungssystem ist das Führungssystem im Allgemeinen so gestaltet, dass ein Hängenbleiben des bewegten Bauteils unwahrscheinlich ist.

Tabelle B.5 (*fortgesetzt*)

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Selbsttätige Veränderung der Ausgangs-Schaltstellung (ohne ein Eingangssignal)	Ja, wenn übliche Einbau- und Betriebsbedingungen vorliegen (siehe Bemerkung) und eine ausreichende Schließkraft aufgrund der vorliegenden Drücke und Flächen vorhanden ist.	Übliche Einbau- und Betriebsbedingungen werden eingehalten, wenn: — die vom Hersteller festgelegten Bedingungen befolgt werden; — keine besonderen Massenträgheitskräfte die bewegten Bauteile beeinträchtigen, z. B. Bewegungsrichtung berücksichtigt die Orientierung der beweglichen Maschinenteile; und — die Schwingungs- und Stoßbeanspruchungen kleiner sind als zulässig, und keine extremen Schwingungs- oder Stoßbeanspruchungen auftreten.
Für Wechselventile: gleichzeitiger Verschluss beider Eingangsanschlüsse	Ja, wenn gleichzeitiges Schließen unwahrscheinlich ist, bedingt durch Konstruktion und Ausführung des bewegten Bauteils.	—
Leckage	Ja, wenn übliche Betriebsbedingungen vorliegen (siehe Bemerkung) und die Druckluft ausreichend aufbereitet und filtriert ist.	Übliche Betriebsbedingungen liegen vor, wenn die vom Hersteller festgelegten Bedingungen befolgt werden.
Veränderung 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 guter ingenieurmäßiger Praxis entsprechen und die Spezifikationen des Ventilherstellers befolgt werden.	

Tabelle B.6 — Fehler und Fehlerausschlüsse — Stromventile

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Veränderung des Volumenstroms ohne Veränderung der Verstelleinrichtung	Ja, bei Stromregelventilen mit Bauteilen aus Metall, die keine beweglichen Teile besitzen [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 bewegliches Teil betrachtet. Veränderungen des Volumenstroms durch Änderung der Druckdifferenz sind bei diesem Ventiltyp physikalisch begrenzt und nicht Gegenstand dieser Fehlerannahme.
Veränderung des Volumenstroms bei nicht einstellbaren kreisförmigen Blenden und Düsen	Ja, wenn der Durchmesser $\geq 0,8$ mm ist, übliche Betriebsbedingungen vorliegen [siehe Bemerkung 2)] und die Druckluft ausreichend aufbereitet und filtriert ist.	2) Übliche Betriebsbedingungen liegen vor, wenn die vom Hersteller festgelegten Bedingungen befolgt werden.
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 sicherheitstechnischen Spezifikation(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 guter ingenieurmäßiger Praxis entsprechen und die Spezifikationen des Ventilherstellers befolgt werden.	

Tabelle B.7 — Fehler und Fehlerausschlüsse — Druckventile

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Nichtöffnen oder nicht ausreichendes Öffnen bei Überschreiten des Einstelldruckes (Hängenbleiben oder Schwergängigkeit des bewegten Bauteils) [siehe Bemerkung 1)]	Ja, wenn: — das Führungssystem für das/die bewegte(n) Bauteil(e) dem eines nicht gesteuerten Kugelsitz- oder Membranventils entspricht [siehe Bemerkung 2)], z. B. bei einem Druckminderventil mit Sekundärdruckentlastung; und — die eingebauten Federn bewährte Federn sind (siehe Tabelle A.3).	1) Diese Fehlerannahme gilt nur, wenn das/die Druckventil(e) für Kraftwirkungen, z. B. zum Spannen, angewendet wird. Diese Fehlerannahme gilt nicht für die übliche Funktion eines Druckventils in Pneumatiksystemen, z. B. Druckminderung, Druckbegrenzung. 2) Für ein nicht gesteuertes Kugelsitz- oder Membranventil ist das Führungssystem im Allgemeinen so gestaltet, dass ein Hängenbleiben des bewegten Bauteils unwahrscheinlich ist.
Nichtschließen oder nicht vollständiges Schließen bei Unterschreiten des Einstelldruckes (Hängenbleiben oder Schwergängigkeit des bewegten Bauteils) [siehe Bemerkung 1)]		
Veränderung des Druckregelverhaltens 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.3).	—
Für Proportionaldruckventile: Veränderung des Druckregelverhaltens 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.	Übliche Betriebsbedingungen liegen vor, wenn die vom Hersteller festgelegten Bedingungen befolgt werden.
Leckage	Ja, für Sitzventile, Membranventile und Schieberventile mit elastischer Abdichtung bei üblichen Betriebsbedingungen (siehe Bemerkung) und wenn die Druckluft ausreichend aufbereitet und filtriert ist.	

Tabelle B.7 (fortgesetzt)

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Veränderung des Leckagevolumenstroms über eine lange Einsatzdauer	Nein.	—
Bersten des Ventilgehäuses oder Bruch des/der bewegten Bauteils/Bauteile sowie Bruch der Befestigungs- oder Gehäuseschrauben	Ja, wenn Konstruktion, Dimensionierung und Einbau guter ingenieurmäßiger Praxis entsprechen und die Spezifikationen des Ventilherstellers befolgt werden.	

Tabelle B.8 — Fehler und Fehlerausschlüsse — Rohrleitungen

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Bersten und Leckage	Ja, wenn Dimensionierung, Auswahl der Werkstoffe und Befestigung guter ingenieurmäßiger Praxis entsprechen (siehe Bemerkung), z. B. Einbau unter Vermeidung von Wasseransammlung, regelmäßige Entwässerung.	Bei Anwendung von Kunststoffrohren sind die Herstellerangaben zu beachten, insbesondere bezüglich der Umgebungseinflüsse während des Betriebs, z. B. thermische Einflüsse, chemische Einflüsse oder Einflüsse durch Strahlung. Bei Anwendung von Stahlrohren, die nicht mit einem korrosionshemmenden Mittel behandelt wurden, ist es besonders wichtig, die Druckluft ausreichend zu trocknen. Die Berücksichtigung des Taupunkts der Umgebungsluft ist ebenfalls wichtig.
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 guter ingenieurmäßiger Praxis 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.9 — Fehler und Fehlerausschlüsse — Schlauchleitungen

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Bersten, Abreißen am Armaturenanschluss und Leckage	Ja, wenn Schlauchleitungen aus Schläuchen nach ISO 4079:2020, ISO 2398:2024, ISO 5774:2023 oder aus ähnlichen Schläuchen (siehe Bemerkung) und den zugehörigen Schlaucharmaturen verwendet werden. ANMERKUNG ISO 4414:2010 enthält keine Kriterien im Hinblick auf die Herstellspezifikationen von Gummischläuchen und Schlauchleitungen.	Ein Fehlerausschluss wird nicht angenommen, wenn — die vorgesehene Verwendungsdauer überschritten ist; — der Druckträger (die Verstärkungseinlage) durch Ermüdung versagen kann; oder — eine äußere Beschädigung unvermeidbar ist.
Zusetzen (Verstopfen)	Ja, bei Schlauchleitungen im Leistungskreis sowie bei Steuer- und Messschlauchleitungen, wenn die Nennweite ≥ 2 mm ist.	—

Tabelle B.10 — Fehler und Fehlerausschlüsse — Verbindungselemente

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Bersten, Schraubenbruch oder Ausreißen von Gewinden	Ja, wenn Dimensionierung, Auswahl der Werkstoffe, Herstellung, Anordnung und Verbindung zur Leitung und/oder zu den Rohr-/Schlaucharmaturen guter ingenieurmäßiger Praxis entsprechen.	—
Leckage (Verlust der Dichtwirkung)	Nein.	Durch Verschleiß, Alterung, Nachlassen der Elastizität usw. ist kein Fehlerausschluss für eine lange Zeitspanne möglich.

Tabelle B.10 (fortgesetzt)

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Leckage (plötzliche größere Veränderung der Luftdichtheit)	Ja, wenn Maßnahmen zur Minderung des Leckagerisikos angewendet werden, die zum Verlust der vorgesehenen Funktion des Bauteils führen könnten. Die Maßnahmen können unter anderem folgende umfassen: — widerstandsfähige Verbindungen, d. h. Quetscharmaturen oder entsprechend bemessene Druckverschlüsse (en: push-lock fittings) (siehe Bemerkungen 1 bis 3); — widerstandsfähige Schläuche, Rohre und Armaturen; — widerstandsfähige Werkstoffe, die für die vorgesehene Umgebung geeignet sind.	1) Wenn eine Leckage (plötzliche größere Veränderung der Luftdichtheit) zu einer gefahrbringenden Bewegung führen kann, insbesondere an schwerkraftbelasteten (z. B. vertikalen) Achsen, wird ein Fehlerausschluss nicht empfohlen. Ein Fehlerausschluss bei dieser Anwendungsart ist nur in Verbindung mit einer Risikoabschätzung und zusätzlichen Maßnahmen möglich. 2) Rohr-Steckverbindungen, auch bekannt als Steckverschraubungen oder Einsteckverbindungen, werden als ausreichend bemessene Druckverschlüsse angesehen, wenn die Anleitungen zur Überdimensionierung sowie die Einbau- und Betriebsanleitungen des Herstellers befolgt werden, wobei darauf zu achten ist, dass die Steckverbindung mit dem verwendeten Rohr zusammenpasst. 3) Schlauch-Steckanschlüsse, z. B. solche mit einem spitzen Ende, das in den Schlauch eingeführt wird, werden nur dann als ausreichend bemessene Steckanschlüsse angesehen, wenn Hochdruck-Schlauchklemmen verwendet werden.
Zusetzen (Verstopfen)	Ja, bei Anwendungen im Leistungskreis und bei Steuer- und Messverbindungselementen, wenn die Nennweite ≥ 2 mm ist.	—

Tabelle B.11 — Fehler und Fehlerausschlüsse — Druckübersetzer und Druckmittelwandler

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Verlust oder Veränderung der Luft/Öl-Dichtwirkung der Druckräume	Nein.	—
Bersten der Druckräume sowie Bruch von Befestigungs- oder Deckelschrauben	Ja, wenn Dimensionierung, Auswahl der Werkstoffe, Anordnung und Befestigung guter ingenieurmäßiger Praxis entsprechen.	
Zu hoher Ausgangsdruck durch zu hohen Eingangsdruck	Ja, wenn ein internes Druckentlastungsventil im Eingangskreis verwendet wird.	
Änderung des Verhältnisses von Eingangsdruck zu Ausgangsdruck	Ja, wenn das Druckverhältnis feststehend ist, z. B. durch die Auslegung der aktiven Kolbenfläche und andere interne Maßnahmen.	
ANMERKUNG Druckübersetzer und Druckmittelwandler sind Vorrichtungen, mit denen beispielsweise der Ausgangsdruck begrenzt wird oder ein feststehendes Verhältnis von Eingangsdruck zu Ausgangsdruck erzielt wird.		

Tabelle B.12 — Fehler und Fehlerausschlüsse — Druckluftbehandlung — Filter

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

Tabelle B.13 — Fehler und Fehlerausschlüsse — Druckluftbehandlung — Öler

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

Tabelle B.14 — Fehler und Fehlerausschlüsse — Druckluftbehandlung — Schalldämpfer

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

Tabelle B.15 — Fehler und Fehlerausschlüsse — Energiespeicher und Druckbehälter

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

Tabelle B.16 — Fehler und Fehlerausschlüsse — Sensoren

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Fehlerhafter Sensor (siehe Bemerkung)	Nein.	—
Veränderung der Erfassungs- oder Ausgabeeigenschaften	Nein.	
ANMERKUNG Sensoren nach dieser Tabelle sind Vorrichtungen zur Signalerfassung, -verarbeitung und -ausgabe für beispielsweise Druck, Volumenstrom und Temperatur.		

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

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Fehlerhaftes Verknüpfungsglied (z. B. UND-Glied, ODER-Glied, Speicherglied) durch z. B. Veränderung der Schaltzeiten, Nichtschalten oder unvollständiges Schalten	Für entsprechende Fehlerannahmen und Fehlerausschlüsse siehe Tabelle B.4, Tabelle B.5 und Tabelle B.6 und die entsprechenden zugehörigen Bauteile.	—

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

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Fehlerhaftes Verzögerungsglied, z. B. pneumatische und pneumatisch/mechanische Zeit- und Zählglieder	Ja, bei Verzögerungsgliedern ohne bewegte Bauteile, z. B. Festwiderstände, wenn übliche Betriebsbedingungen vorliegen und die Druckluft ausreichend aufbereitet und filtriert ist.	—
Veränderung der Erfassungs- oder Ausgabeeigenschaften		
Bersten des Gehäuses oder Bruch der Deckel- oder Befestigungselemente	Ja, wenn Konstruktion, Dimensionierung und Einbau guter ingenieurmäßiger Praxis entsprechen.	—

Tabelle B.19 — Fehler und Fehlerausschlüsse — Informationsverarbeitung — Umformer

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Fehlerhafter Umformer (siehe Bemerkung)	Ja, bei Umformern ohne bewegte Bauteile, z. B. Reflexdüse, wenn übliche Betriebsbedingungen vorliegen und die Druckluft ausreichend aufbereitet und filtriert ist.	—
Veränderung der Erfassungs- oder Ausgabeeigenschaften		
Bersten des Gehäuses oder Bruch der Deckel- oder Befestigungselemente		
ANMERKUNG Umformer nach dieser Tabelle sind Vorrichtungen, um beispielsweise festzustellen, ob eine bestimmte Position erreicht ist, oder um zwischen binären Zuständen (Position erreicht/nicht erreicht, Druck ein/aus) zu schalten. Sie werden auch verwendet, um pneumatische Signale zu verstärken.		

Anhang C (informativ)

Validierungswerkzeuge für hydraulische Systeme

Anhang C ist für hydraulische Systeme anwendbar. Er sollte auch dann beachtet werden, wenn hydraulische Systeme in Verbindung mit anderen Technologien verwendet werden. Wenn hydraulische Bauteile elektrisch angeschlossen/gesteuert werden, sollten die entsprechenden Fehlerlisten im Anhang D berücksichtigt werden.

ANMERKUNG Zusätzliche Anforderungen können in nationalen Rechtsvorschriften enthalten sein.

Tabelle C.1 und Tabelle C.2 führen grundlegende und bewährte Sicherheitsprinzipien auf.

Die Verwendung von Bauteilen, die nach einer Produktnorm ausgelegt sind, kann zur Bestätigung einiger grundlegender oder bewährter Sicherheitsprinzipien hilfreich sein (siehe Tabelle 2, Anmerkung 2). Die Erfüllung von Prinzipien kann von mehreren Beitragenden abhängen (siehe 4.1, Tabelle 2, umgesetzt in Spalte 3 von Tabelle C.1 und Tabelle C.2).

Der Status „bewährt“ ist in erster Linie anwendungsbezogen. Bauteile können als „bewährt“ beschrieben werden, falls diese ISO 13849-1:2023, 6.1.11, und ISO 4413:2010, Abschnitt 5 bis Abschnitt 7, entsprechen. Ein für bestimmte Anwendungen bewährtes Bauteil könnte für andere Anwendungen ungeeignet sein. Der Status „bewährt“ bedeutet nicht, dass bei einem bewährten Bauteil alle Fehler ausgeschlossen werden können

In Tabelle C.4 bis Tabelle C.13 werden Fehlerausschlüsse und die zugehörigen Begründungen aufgeführt.

Tabelle C.1 — Grundlegende Sicherheitsprinzipien

Grundlegendes Sicherheitsprinzip	Bemerkungen	Maßgebend für (siehe Tabelle 2)
Anwendung geeigneter Werkstoffe und Herstellungsverfahren	Auswahl der Werkstoffe, der Herstellungs- und Behandlungsverfahren unter Berücksichtigung von z. B. Belastung, Haltbarkeit, Elastizität, Reibung, Verschleiß, Korrosion, Temperatur, Eigenschaften der Hydraulikflüssigkeit.	M, D
Richtige Dimensionierung und Formgebung	Berücksichtigen z. B. von Belastung, Spannung, Ermüdung, Oberflächenrauheit, Toleranzen, Herstellungsverfahren.	M, D
Korrekte Auswahl, Kombination, Anordnungen, Zusammenbau und Einbau von Bauteilen oder Systemen für die jeweilige Anwendung	Anwenden der vom Hersteller bereitgestellten Einbau- und Betriebsanleitungen, z. B. Katalogblätter, Einbauanweisungen, Spezifikationen sowie Anwenden guter ingenieurmäßiger Praxis mit ähnlichen Bauteilen oder Systemen.	M, D, U

Tabelle C.1 (*fortgesetzt*)

Grundlegendes Sicherheitsprinzip	Bemerkungen	Maßgebend für (siehe Tabelle 2)
Anwendung des Prinzips der Energietrennung Dieses Prinzip ist nicht anwendbar, wenn durch einen Energieverlust eine Gefährdung entsteht, z. B. Lösen eines Werkstücks durch den Verlust der Spann- bzw. Haltekraft.	Der sichere Zustand wird durch Trennen der Energie an allen relevanten Einrichtungen erreicht. Siehe primärer Vorgang zur Stillsetzung in ISO 12100:2010, 6.2.11.3. Zum Ingangsetzen der Bewegung eines Mechanismus wird Energie zugeführt. Siehe primärer Vorgang zur Ingangsetzung in ISO 12100:2010, 6.2.11.3. Berücksichtigen von unterschiedlichen Betriebsarten, z. B. Betriebsmodus, Instandhaltungsmodus. Zeitverzögernde Funktionen können erforderlich sein, um einen sicheren Zustand des Systems zu erreichen (siehe z. B. IEC 60204-1:2016 + AMD1:2021, 9.2.2).	M, D
Korrekte Befestigung	Für Befestigungsmittel (z. B. Schraubensicherungen, Armaturen, Klebungen oder Spannringe) werden die Einbau- und Betriebsanleitungen des Herstellers angewendet. Die Befestigung in der richtigen Orientierung und mit dem richtigen Drehmoment wird berücksichtigt. Durch Anwendung eines geeigneten Verfahrens zum Aufbringen des Drehmoments kann Überbeanspruchung vermieden werden.	M, D, U
Beständigkeit gegen Umgebungsbedingungen (siehe ISO 13849-1:2023, Abschnitt 10, und Einbau- und Betriebsanleitungen des Herstellers befolgen)	Gestalten des Equipments, so dass es innerhalb der Umgebungsgrenzen der vorgesehenen Verwendung und bei allen vernünftigerweise vorhersehbaren ungünstigen Bedingungen, z. B. für Temperatur, Luftfeuchte, Schwingungen, Verunreinigungen, elektromagnetische Störung (EMI), funktionieren kann.	M, D, U
Verhindern des Eindringens von festen Fremdkörpern und Fluiden	Anwenden eines geeigneten Schutzes gegen das Eindringen von festen Fremdkörpern und Fluiden.	M, D, U
Temperaturbereich	Externe und interne Temperatureinwirkungen werden für das gesamte System betrachtet. (siehe ISO 4413:2010)	M, D, U
Begrenzung von Geschwindigkeit, Beschleunigung und Ruck (um mechanische Beanspruchungen zu vermeiden oder zu begrenzen)	Ein Beispiel ist die Geschwindigkeitsbegrenzung eines Kolbens durch ein Stromventil oder eine Drossel.	M, D

Tabelle C.1 (fortgesetzt)

Grundlegendes Sicherheitsprinzip	Bemerkungen	Maßgebend für (siehe Tabelle 2)
Verringerung der Reaktionszeit	Minimieren der Verzögerung bei der Energietrennung der zum Schalten verwendeten Bauteile. Geeigneter Schaltzeitbereich, z. B. der Länge der Rohrleitungen, Druck, Entleerungskapazität, Verringerung der Federkraft, Reibung, Schmierung, Temperatur, Viskosität, Trägheit bei Beschleunigung und Verzögerung, Frequenzen, Stoßwellen, Kombination von Toleranzen.	M, D
Schutz gegen unerwarteten Anlauf (siehe ISO 12100:2010, 6.2.11.4, ISO 14118:2017)	Berücksichtigen von unerwartetem Anlauf, verursacht durch gespeicherte Energie und nach Wiederherstellung der Energieversorgung, für unterschiedliche Betriebsarten, z. B. Betriebsmodus, Instandhaltungsmodus.	M, D
	Eine besondere Einrichtung zum Abbau der gespeicherten Energie kann notwendig sein. Besondere Anwendungen, z. B. zur Beibehaltung der Energie für Spanneinrichtungen oder zur Sicherung einer Position, müssen gesondert betrachtet werden.	M, D, U
Vereinfachung	Vermeiden von unnötigen Bauteilen im sicherheitsbezogenen System.	M, D
Trennung	Trennung der sicherheitsbezogenen Funktionen von anderen Funktionen.	M, D
Druckbegrenzung (z. B. zur Vermeidung von Verschleiß)	Beispiele sind Druckentlastungsventile, Druckminder-/Druckregelventile.	M, D
Grundlegende Maßnahmen gegen eine Verunreinigung des Druckmediums	Berücksichtigen von Filtration von Feststoffen und Abtrennung von Wasser und Gas vom Druckmedium. Verhindern einer Kontamination des Druckmediums durch externe Quellen während des Einbaus und der Handhabung der Bauteile. Berücksichtigen einer Anzeige, die angibt, dass der Filter ausgetauscht werden muss.	M, D, U
Korrektur Umgang mit Druckmedien	Luftblasen und Drosselstellen in der Hydraulikflüssigkeit werden vermieden, weil sie zu Kavitationen führen können, die zusätzliche Gefährdungen verursachen können, z. B. unbeabsichtigte Bewegungen.	M, D, U
Abkürzungen M – Entwurf und Herstellung von Bauteilen D – Entwurf von Teilsystemen U – Verwendung der Maschine		

Tabelle C.2 — Bewährte Sicherheitsprinzipien

Bewährtes Sicherheitsprinzip	Bemerkungen	Maßgebend für (siehe Tabelle 2)
Verwendung von Bauteilen mit gerichtetem Ausfallverhalten (siehe ISO 12100:2010, 6.2.12.3)	Nach Möglichkeit Bauteile oder Systeme mit gerichtetem Ausfallverhalten verwenden. Ein sicherer Zustand wird direkt oder indirekt (z. B. durch Fehlererkennung) durch die überwiegend auftretende Ausfallart erzielt.	M, D
Überdimensionierung	Unterbeanspruchung von Bauteilen, die in Sicherheitsschaltkreisen verwendet werden. Sicherheitsfaktoren sind in Normen angegeben oder beruhen auf guter ingenieurmäßiger Praxis in sicherheitsbezogenen Anwendungen.	M, D
Gesicherte Position	Das bewegliche Element des Bauteils wird mechanisch in einer der möglichen Positionen gehalten. Um die Position zu verändern, ist das Aufbringen von Kraft notwendig, insbesondere beim Verlassen einer gesicherten Position.	M, D
Erhöhte AUS-Kraft	Eine sichere Stellung oder ein sicherer Zustand wird dadurch erreicht, dass die AUS-Kraft gegenüber der EIN-Kraft erhöht ist. Eine Lösung kann sein, dass das Flächenverhältnis für die Bewegung eines Ventilschiebers in die sichere Position (AUS-Stellung) gegenüber der Bewegung des Ventilschiebers in die EIN-Stellung wesentlich größer ist (ein Sicherheitsfaktor).	M, D
Durch den Lastdruck schließendes Ventil	Beispiele sind Ventile in Sitz- und Patronen-Bauart. Es wird berücksichtigt, wie der Lastdruck aufzubringen ist, um das Ventil auch dann geschlossen zu halten, wenn z. B. die Schließfeder des Ventils bricht.	M, D
Mechanisch zwangsläufige Wirkung (siehe ISO 12100:2010, 6.2.5.)	Die mechanisch zwangsläufige Wirkung wird für die beweglichen Teile innerhalb der hydraulischen Bauteile angewendet. Um eine mechanisch zwangsläufige (oder direkte) Wirkung zu erreichen, werden mechanische Bauteile, die zur Ausführung der Sicherheitsfunktion erforderlich sind, entweder durch direkten Kontakt oder über starre Elemente bewegt.	M, D
Verwendung bewährter Federn	Siehe Tabelle A.3.	M

Tabelle C.2 (fortgesetzt)

Bewährtes Sicherheitsprinzip	Bemerkungen	Maßgebend für (siehe Tabelle 2)
Begrenzter Bereich der Kraft und ähnlicher Parameter, um mechanische Beanspruchungen zu vermeiden oder zu begrenzen Dieses Prinzip ist nicht anwendbar, wenn die kontinuierliche Funktionsfähigkeit der Bauteile unerlässlich dafür ist, den notwendigen Grad der Steuerbarkeit beizubehalten.	Spezifikation der notwendigen Begrenzung in Abhängigkeit von Erfahrungen und der jeweiligen Anwendung. Dies kann erreicht werden durch ein bewährtes Druckentlastungsventil, das z. B. mit einer bewährten Feder ausgestattet und richtig dimensioniert und ausgewählt ist.	M, D
Begrenzter Bereich der Geschwindigkeit und ähnlicher Parameter	Spezifikation der notwendigen Begrenzung in Abhängigkeit von Erfahrungen und der jeweiligen Anwendung. Beispiele sind Festblende und Festdrossel, um durch den Widerstand gegenüber einer bestimmten Flüssigkeitsströmung die Geschwindigkeit zu verringern.	M, D, U
Begrenzter Bereich der Umgebungsparameter Siehe ISO 13849-1:2023, 10.7	Spezifikation der notwendigen Begrenzungen. Beispiele sind Temperatur, Luftfeuchte, Verunreinigung beim Einbau. Einhalten der Einbau- und Betriebsanleitungen des Herstellers.	M, D, U
Begrenzter Bereich der Reaktionszeit, Begrenzung der Hysterese	Spezifikation der notwendigen Begrenzungen. Die Hysterese erhöht sich z. B. durch stärkere Reibung. Eine Kombination von Toleranzen beeinflusst die Hysterese ebenfalls.	M, D
Geeigneter Bereich der Betriebsbedingungen	Die Begrenzung der Betriebsbedingungen, z. B. Druck-, Volumenstrom- und Temperaturbereich, wird berücksichtigt.	M, D, U
Verbesserte Maßnahmen gegen eine Verunreinigung des Druckmediums	Berücksichtigung der Notwendigkeit einer feineren Filtration und Abscheidung von Feststoffen und Wasser im Druckmedium.	M, D, U
Ausreichend große positive Überdeckung in Schieberventilen oder Kolbenschieberventilen	Die positive Überdeckung sichert die Anhaltefunktion und verhindert gefährliche Bewegungen.	M

Tabelle C.2 (fortgesetzt)

Bewährtes Sicherheitsprinzip	Bemerkungen	Maßgebend für (siehe Tabelle 2)
Regelmäßige Bewertung des Zustandes des Druckmediums	Anwenden einer hoch wirksamen Filtration oder Abscheidung von Feststoffen, Wasser und Verunreinigungen im Druckmedium und ein Hinweis auf die Notwendigkeit des Auswechselns des Filters. Bewertung der physikalischen und chemischen Zustände des Druckmediums.	M, D, U
Abkürzungen M – Entwurf und Herstellung von Bauteilen D – Entwurf von Teilsystemen U – Verwendung der Maschine		

Tabelle C.3 — Bewährte Bauteile

Bewährtes Bauteil	Bedingungen für „bewährt“	Norm oder Spezifikation
Druckentlastungsventil (federbelastet)	Alle Faktoren, die auf die Anwendung Einfluss nehmen, sind zu berücksichtigen. Siehe Tabelle C.2.	Technische Spezifikationen für Berstscheiben/flache Berstscheiben und andere Sonderanwendungsfälle sind in ISO 4126-1:2013 angegeben.
Wegeventil (elektrisch oder ferngesteuert oder vorgesteuert)	Nur bewährt, wenn: a) das Bauteil die grundlegenden und bewährten Sicherheitsprinzipien im Hinblick auf die vorgesehene Anwendung erfüllt, einschließlich der Verwendung des Bauteils entsprechend den Spezifikationen des Herstellers; b) das Bauteil nachweislich in der Vergangenheit in zahlreichen Fällen mit dokumentierten erfolgreichen Ergebnissen bei ähnlichen Anwendungen im Einsatz war oder das Bauteil mittels Prinzipien, die seine Eignung und Zuverlässigkeit für sicherheitsbezogene Anwendungen entsprechend den Produkt- und Anwendungsnormen belegen, hergestellt, verifiziert und validiert wurde; c) entweder keine Onboard-Elektronik vorhanden ist oder wenn die Onboard-Elektronik, soweit vorhanden, nicht zur Ausführung der Sicherheitsfunktion beiträgt (siehe ANMERKUNG 3); d) das Verhalten des Bauteils unter allen Bedingungen klar definiert ist und vollständig bestimmt werden kann; und	ISO 13849-1:2023, 6.1.3.2.3, 6.1.11

Tabelle C.3 (fortgesetzt)

Bewährtes Bauteil	Bedingungen für „bewährt“	Norm oder Spezifikation
	e) die folgenden Konstruktionsmerkmale erfüllt sind: — einfache, widerstandsfähige Auslegung; — formschlüssige Verbindung; — ausreichender Schutz gegen das Lösen von abnehmbaren Verbindungen; — ausreichend widerstandsfähig in Bezug auf die Verwendung (Anwendung) und die Umgebungsbedingungen (z. B. Druckschwankungen, Vibration); — von einer Feder aufgebrachte Rückstellkraft zur Rückstellung in eine gesicherte Position; — Verwendung bewährter Federn, siehe Tabelle A.3; und — ausreichende Dichtheit in Sperrrichtung.	

Tabelle C.3 (fortgesetzt)

Bewährtes Bauteil	Bedingungen für „bewährt“	Norm oder Spezifikation
Druckschalter	Nur bewährt, wenn: a) das Bauteil die grundlegenden und bewährten Sicherheitsprinzipien im Hinblick auf die vorgesehene Anwendung erfüllt, einschließlich der Verwendung des Bauteils entsprechend den Spezifikationen des Herstellers; b) das Bauteil nachweislich in der Vergangenheit in zahlreichen Fällen mit dokumentierten erfolgreichen Ergebnissen bei ähnlichen Anwendungen im Einsatz war oder das Bauteil mittels Prinzipien, die seine Eignung und Zuverlässigkeit für sicherheitsbezogene Anwendungen entsprechend den Produkt- und Anwendungsnormen belegen, hergestellt, verifiziert und validiert wurde; c) entweder keine Onboard-Elektronik vorhanden ist oder wenn die Onboard-Elektronik, soweit vorhanden, nicht zur Ausführung der Sicherheitsfunktion beiträgt; d) das Verhalten des Bauteils unter allen Bedingungen klar definiert ist und vollständig bestimmt werden kann; und e) die folgenden Konstruktionsmerkmale erfüllt sind: — einfache, widerstandsfähige Auslegung; — formschlüssige Verbindung; — ausreichender Schutz gegen das Lösen von abnehmbaren Verbindungen; — ausreichend widerstandsfähig in Bezug auf die Verwendung (Anwendung) und die Umgebungsbedingungen (z. B. Druckschwankungen, Vibration); und — ausreichende Dimensionierung der Feder.	ISO 13849-1:2023, 6.1.3.2.3, 6.1.11 Für den elektrischen Teil siehe IEC 6094751:2024.

ANMERKUNG 1 Die Bestätigung von grundlegenden und bewährten Sicherheitsprinzipien sowie der Nachweis für den Einsatz in der Vergangenheit in zahlreichen Fällen mit dokumentierten erfolgreichen Ergebnissen bei ähnlichen Anwendungen kann vom Bauteilhersteller oder vom Konstrukteur des Teilsystems erbracht werden.

ANMERKUNG 2 Beispiele für Wegeventile können Ventilarten mit diskreten (spezifischen) Positionen sein: Absperr-/Abschaltventil, Schieberventil, UND-Ventil, Wechselventil, Rückschlagventil, Sperrventil, Auslassventil, Druckentlastungsventil.

ANMERKUNG 3 Digitale Kommunikationseinheiten für Ventilblöcke oder Druckschalter sind komplex und erfüllen nicht die Bedingungen, um als bewährt zu gelten. Bewirkt eine Unterbrechung der Energiezufuhr einen sicheren Zustand der Ventile und kann ein Fehlerausschluss für Querschuss zwischen der Energiezufuhr und dem Steuerbus erfolgen (siehe Anhang D), und sind für die eingebauten Ventile die Bedingungen für „bewährt“ erfüllt, kann der Ventilblock als bewährtes Bauteil angesehen werden.

Tabelle C.4 — Fehler und Fehlerausschlüsse — Wegeventile

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Veränderung der Schaltzeiten	Ja, bei mechanisch zwangsläufiger Wirkung (siehe Tabelle A.2) der bewegten Bauteile, sofern die Betätigungskraft ausreichend groß ist; oder, bezogen auf das Nichtöffnen eines Patronensitzventils besonderer Bauart, wenn es mit mindestens einem weiteren Ventil den Hauptvolumenstrom des 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 (Ventilsitz) beträgt; — der wirksame Steuerdruck auf die aktive Fläche, hervorgerufen durch das Verhalten des betrachteten Sitzventils, bis zum maximalen Betriebsdruck (nach ISO 5598:2020, 3.2.429) ansteigen kann; — der wirksame Steuerdruck auf die der aktiven Fläche gegenüberliegende Fläche des bewegten Bauteils auf einen im Vergleich zum maximalen Betriebsdruck sehr niedrigen Wert verringert wird, z. B. Rücklaufdruck bei abschaltbaren Druckventilen oder Speisedruck bei Saug-/Füllventilen; — das bewegte Bauteil (Ventilsitz) mit Entlastungsnuten am Umfang versehen ist; und — das (die) Vorsteuerventil(e) für dieses Sitzventil gemeinsam mit diesem Sitzventil in Blockbauweise (d. h. ohne Schlauchleitungen und Rohre zur Verbindung dieser Ventile) angeordnet ist (sind).
Nichtschalten (Hängenbleiben in einer End- oder Nulllage) oder nicht vollständiges Schalten (Hängenbleiben in einer beliebigen Zwischenstellung)	Ja, bei mechanisch zwangsläufiger Wirkung (siehe Tabelle A.2) der bewegten Bauteile, sofern die Betätigungskraft ausreichend groß ist; oder, bezogen auf das Nichtöffnen eines Patronensitzventils besonderer Bauart, wenn es mit mindestens einem weiteren Ventil den Hauptvolumenstrom des Druckmediums steuert [siehe Bemerkung 1)].	

Tabelle C.4 (fortgesetzt)

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Selbsttätige Veränderung der Ausgangs-Schaltstellung (ohne ein Eingangssignal)	Ja, bei mechanisch zwangsläufiger Wirkung (siehe Tabelle A.2) der bewegten Bauteile, sofern die Haltekraft ausreichend groß ist; oder ja, wenn bewährte Federn verwendet werden (siehe Tabelle A.3) und wenn übliche Einbau- und Betriebsbedingungen vorliegen [siehe Bemerkung 2)] oder, bezogen auf das Nichtöffnen eines Patronensitzventils besonderer Bauart, wenn es mit mindestens einem weiteren Ventil den Hauptvolumenstrom des Druckmediums steuert [siehe Bemerkung 1)] und wenn übliche Einbau- und Betriebsbedingungen vorliegen [siehe Bemerkung 2)].	3) Übliche Einbau- und Betriebsbedingungen liegen vor, wenn: — die vom Hersteller vorgegebenen Bedingungen befolgt werden; — sich die Gewichtskraft des bewegten Bauteils sicherheitstechnisch nicht ungünstig auswirkt, z. B. waagerechter Einbau; — keine besonderen Massenträgheitskräfte die bewegten Bauteile beeinträchtigen, z. B. Bewegungsrichtung berücksichtigt die Orientierung der beweglichen Maschinenteile; und — keine extremen Schwingungs- und Schockbeanspruchungen auftreten.
Leckage	Ja, bei Sitzventilen, wenn übliche Einbau- und Betriebsbedingungen vorliegen (siehe Bemerkung) und ein angemessenes Filtrationssystem vorhanden ist.	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 guter ingenieurmäßiger Praxis entsprechen.	
Für Servo- und Proportionalventile: Hydraulikfehler, die unkontrolliertes Verhalten bewirken	Ja, bei Servo- und Proportionalwegeventilen, wenn sie bedingt durch ihre konstruktive Ausführung in Bezug auf die Sicherheit 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 die gleiche Vorgehensweise angewendet werden.		

**Tabelle C.5 — Fehler und Fehlerausschlüsse —
Absperr-/Abschaltventile/Rückschlagventile/Wechselventile usw.**

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Veränderung der Schaltzeiten	Nein.	—
Nichtöffnen, nicht vollständiges Öffnen, Nichtschließen oder nicht vollständiges Schließen (Hängenbleiben in einer Endlage oder in einer beliebigen Zwischenstellung)	Ja, wenn das Führungssystem für das/die bewegte(n) Bauteil(e) ähnlich ausgelegt ist wie bei einem nicht gesteuerten Kugelsitzventils ohne ein Dämpfungssystem (siehe Bemerkung) und wenn bewährte Federn verwendet werden (siehe Tabelle A.3).	Für ein nicht gesteuertes Kugelsitzventil ohne Dämpfungssystem ist das Führungssystem im Allgemeinen so gestaltet, dass ein Hängenbleiben des bewegten Bauteils unwahrscheinlich ist.
Selbsttätige Veränderung der Ausgangs-Schaltstellung (ohne ein Eingangssignal)	Ja, wenn übliche Einbau- und Betriebsbedingungen vorliegen (siehe Bemerkung) und eine ausreichende Schließkraft aufgrund der vorliegenden Drücke und Flächen vorhanden ist.	Übliche Einbau- und Betriebsbedingungen werden eingehalten, wenn: — die vom Hersteller festgelegten Bedingungen befolgt werden; — keine besonderen Massenträgheitskräfte die bewegten Bauteile beeinträchtigen, z. B. Bewegungsrichtung berücksichtigt die Orientierung der beweglichen Maschinenteile; und — keine extremen Schwingungs- und Schockbeanspruchungen auftreten.
Für Wechselventile: gleichzeitiger Verschluss beider Eingangsanschlüsse	Ja, wenn dieses gleichzeitige Schließen unwahrscheinlich ist, bedingt durch den Entwurf und die Konstruktion des bewegten Bauteils.	—
Leckage	Ja, wenn übliche Betriebsbedingungen vorliegen (siehe Bemerkung) und ein angemessenes Filtrationssystem vorhanden ist.	Übliche Betriebsbedingungen liegen vor, wenn die vom Hersteller festgelegten Bedingungen befolgt werden.

Tabelle C.5 (*fortgesetzt*)

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

Tabelle C.6 — Fehler und Fehlerausschlüsse — Stromventile

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Veränderung des Volumenstroms ohne Veränderung der Verstelleinrichtung	Ja, bei Stromventilen ohne bewegte Bauteile [siehe Bemerkung 1)], z. B. Drosselventile, wenn übliche Betriebsbedingungen vorliegen [siehe Bemerkung 2)] und ein ausreichendes Filtrationssystem vorhanden ist [siehe Bemerkung 3)].	1) Die Verstelleinrichtung wird nicht als bewegliches Teil betrachtet. Veränderungen des Volumenstroms durch Änderung der Druckdifferenz und der Viskosität sind bei diesem Ventiltyp physikalisch begrenzt und nicht Gegenstand dieser Fehlerannahme.
Veränderung des Volumenstroms bei nicht einstellbaren kreisförmigen Blenden und Düsen	Ja, bei einem Durchmesser $\geq 0,8$ mm, wenn übliche Betriebsbedingungen vorliegen [siehe Bemerkung 2)] und wenn ein ausreichendes Filtrationssystem vorhanden ist.	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.

Tabelle C.6 (*fortgesetzt*)

Betrachteter Fehler	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 der sicherheitstechnischen Spezifikation(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 guter ingenieurmäßiger Praxis entsprechen.	

Tabelle C.7 — Fehler und Fehlerausschlüsse — Druckventile

Betrachteter Fehler	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.4]; oder wenn das Führungssystem für das/die bewegte(n) Bauteil(e) dem eines nicht gesteuerten Kugelsitzventils ohne Dämpfungssystem entspricht [siehe Bemerkung 2)] und wenn bewährte Federn eingebaut sind (siehe Tabelle A.3).	1) Diese Fehlerannahme gilt nur, wenn das/die Druckventil(e) insbesondere angewendet wird (werden) für Kraftwirkungen, z. B. zum Spannen, und für das Steuern von gefahrbringenden Bewegungen, z. B. zum Hochhalten von Lasten. Diese Fehlerannahme gilt nicht für die übliche Funktion eines Druckventils in Hydrauliksystemen, z. B. Druckbegrenzung, Druckminderung.
Nichtschließen oder nicht vollständiges Schließen (weg- und zeitmäßig) bei Unterschreiten des Einstelldruckes (Hängenbleiben oder Schwergängigkeit des bewegten Bauteils) [siehe Bemerkung 1)]		
Veränderung des Druckregelverhaltens ohne Veränderung der Verstelleinrichtung [siehe Bemerkung 1)]	Ja, bei direkt betätigten Druckentlastungsventilen, wenn (eine) bewährte Feder(n) eingebaut ist (sind) (siehe Tabelle A.3).	2) Für ein nicht gesteuertes Kugelsitzventil ohne Dämpfungssystem ist das Führungssystem im Allgemeinen so gestaltet, dass ein Hängenbleiben des bewegten Bauteils unwahrscheinlich ist.
Für Proportionaldruckventile: Veränderung des Druckregelverhaltens 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 Spezifikationen (z. B. Plombierung).	—
Unbeabsichtigtes Herausdrehen des Stellteils der Verstelleinrichtung	Ja, wenn eine wirksame formschlüssige Sicherung gegen das Herausdrehen vorhanden ist.	
Leckage	Ja, für Sitzventile, wenn übliche Betriebsbedingungen vorliegen (siehe Bemerkung) und wenn ein ausreichendes Filtrationssystem vorhanden ist.	Übliche Betriebsbedingungen liegen vor, wenn die vom Hersteller festgelegten 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 guter ingenieurmäßiger Praxis entsprechen.	

Tabelle C.8 — Fehler und Fehlerausschlüsse — Rohrleitungen aus Metall

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Bersten und Leckage	Ja, wenn Dimensionierung, Auswahl der Werkstoffe und Befestigung guter ingenieurmäßiger Praxis entsprechen.	Dimensionierung, mögliche Lasten durch Schwingungen und Druckschwankungen müssen berücksichtigt werden (z. B. durch Getriebepumpen).
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 guter ingenieurmäßiger Praxis entsprechen.	—
Zusetzen (Verstopfen)	Ja, bei Rohrleitungen im Leistungskreis und bei Steuer- und Messrohrleitungen, wenn die Nennweite ≥ 3 mm ist.	

Tabelle C.9 — Fehler und Fehlerausschlüsse — Schlauchleitungen

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Bersten, Abreißen am Armaturenanschluss und Leckage	Nein.	—
Zusetzen (Verstopfen)	Ja, bei Schlauchleitungen im Leistungskreis und bei Steuer- und Messschlauchleitungen, wenn die Nennweite ≥ 3 mm ist.	

Tabelle C.10 — Fehler und Fehlerausschlüsse — Verbindungselemente

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

Tabelle C.11 — Fehler und Fehlerausschlüsse — Filter

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Zusetzen/Verstopfen des Filterelements	Nein.	—
Bruch des Filterelements	Ja, wenn das Filterelement eine ausreichende Druckfestigkeit hat und ein wirksames Bypassventil oder eine wirksame Verschmutzungs-Überwachung vorhanden ist.	
Ausfall des Bypassventils	Ja, wenn das Führungssystem des Bypassventils dem eines nicht gesteuerten Kugelsitzventils ohne ein Dämpfungssystem entspricht (siehe Tabelle C.5) und wenn bewährte Federn angewendet werden (siehe Tabelle A.3).	
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 guter ingenieurmäßiger Praxis entsprechen.	

Tabelle C.12 — Fehler und Fehlerausschlüsse — Energiespeicher

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

Tabelle C.13 — Fehler und Fehlerausschlüsse — Sensoren

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

Anhang D (informativ)

Validierungswerkzeuge für elektrische Systeme

D.1 Allgemeines

Anhang D ist für elektrische Systeme anwendbar. Er sollte auch dann beachtet werden, wenn elektrische Systeme in Verbindung mit anderen Technologien verwendet werden.

Die Umgebungsbedingungen von IEC 60204-1:2016 + AMD1:2021 sind auf den Validierungsprozess anwendbar. Wenn andere Umgebungsbedingungen festgelegt sind, sollten auch sie berücksichtigt werden.

Tabelle D.1 und Tabelle D.2 führen grundlegende und bewährte Sicherheitsprinzipien auf.

Die Erfüllung von Prinzipien kann von mehreren Beitragenden abhängen (siehe 4.1, Tabelle 2, umgesetzt in Spalte 3 von Tabelle D.1 und Tabelle D.2).

Die Verwendung von Bauteilen, die nach einer Produktnorm ausgelegt sind, kann zur Bestätigung einiger grundlegender oder bewährter Sicherheitsprinzipien hilfreich sein (siehe Tabelle 2, Anmerkung 2).

ANMERKUNG 1 Beispiele für Produktnormen sind IEC 61131 (alle Teile) für speicherprogrammierbare Steuerungen und deren Peripheriegeräte, IEC 61800 (alle Teile) für Antriebe und IEC 60947 (alle Teile) für Niederspannungsschaltgeräte.

Die in Tabelle D.3 aufgeführten Bauteile gelten als „bewährt“, wenn sie der in ISO 13849-1:2023, 6.1.11, angegebenen Beschreibung entsprechen. Die in Tabelle D.3 aufgeführten Normen sollten über Eignung und Zuverlässigkeit der Bauteile für eine bestimmte Anwendung Auskunft geben. Ein für bestimmte Anwendungen bewährtes Bauteil kann für andere Anwendungen ungeeignet sein. Der Status „bewährt“ bedeutet nicht, dass bei einem bewährten Bauteil alle Fehler ausgeschlossen werden können.

ANMERKUNG 2 Komplexe elektronische Bauteile, wie speicherprogrammierbare Steuerungen (SPS), Mikroprozessoren und anwendungsspezifisch integrierte Schaltkreise, können nicht als „bewährte“ Bauteile angesehen werden.

In Tabelle D.4 bis Tabelle D.22 werden Fehlerausschlüsse aufgeführt.

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

Tabelle D.1 — Grundlegende Sicherheitsprinzipien

Grundlegendes Sicherheitsprinzip	Bemerkungen	Maßgebend für (siehe Tabelle 2)
Anwendung geeigneter Werkstoffe und Herstellungsverfahren	Auswahl des Werkstoffs, der Herstellungs- und Behandlungsverfahren unter Berücksichtigung von z. B. Belastung, Haltbarkeit, Elastizität, Reibung, Verschleiß, Korrosion, Temperatur, Leitfähigkeit, Spannungsfestigkeit.	M, D
Richtige Dimensionierung und Formgebung	Berücksichtigen z. B. von Belastung, Spannung, Ermüdung, Oberflächenrauheit, Toleranzen, Herstellungsverfahren.	M, D

Tabelle D.1 (fortgesetzt)

Grundlegendes Sicherheitsprinzip	Bemerkungen	Maßgebend für (siehe Tabelle 2)
Korrekte Auswahl, Kombination, Anordnungen, Zusammenbau und Einbau von Bauteilen oder Systemen für die jeweilige Anwendung	Anwenden der vom Hersteller bereitgestellten Einbau- und Betriebsanleitungen, z. B. Katalogblätter, Einbauanweisungen, Spezifikationen sowie Anwenden guter ingenieurmäßiger Praxis mit ähnlichen Bauteilen oder Systemen.	M, D, U
	Anwendung von Bauteilen, die für die angewendeten Spannungen und Ströme geeignet sind.	M, D
Anwendung des Prinzips der Energietrennung Dieses Prinzip ist nicht anwendbar, wenn durch einen Energieverlust eine Gefährdung entsteht, z. B. Lösen eines Werkstücks durch den Verlust der Spann- bzw. Haltekraft.	Der sichere Zustand wird durch Trennen der Energie an allen relevanten Einrichtungen erreicht, z. B. durch Anwendung eines üblicherweise geschlossenen Kontakts (NC) für Eingänge (Tast- und Positionsschalter) und eines üblicherweise geöffneten Kontakts (NO) für Relais (siehe auch ISO 12100:2010, 6.2.11.3). Zeitverzögernde Funktionen können erforderlich sein, um einen sicheren Zustand des Systems zu erreichen (siehe z. B. IEC 60204-1:2016 + AMD1:2021, 9.2.2).	M, D
Korrekte Befestigung	Bei der Befestigung von elektrischen Leitern, z. B. Gleichstromschienen in Frequenzumrichtern, werden die Einbau- und Betriebsanleitungen des Herstellers beachtet. Die Befestigung in der richtigen Orientierung und mit dem richtigen Drehmoment wird berücksichtigt. Durch Anwendung eines geeigneten Verfahrens zum Aufbringen des Drehmoments kann Überbeanspruchung vermieden und eine ausreichende Beständigkeit gegen das Lösen der Verbindung erreicht werden.	M, D, U
Beständigkeit gegen Umgebungsbedingungen (siehe ISO 13849-1:2023, Abschnitt 10, und Einbau- und Betriebsanleitungen des Herstellers befolgen)	Gestalten des Equipments, so dass es innerhalb der Umgebungsgrenzen der vorgesehenen Verwendung und bei allen vernünftigerweise vorhersehbaren ungünstigen Bedingungen, z. B. für Temperatur, Luftfeuchte, Schwingungen und elektromagnetische Störung (EMI), funktionieren kann.	M, D, U
Verhindern des Eindringens von festen Fremdkörpern und Fluiden	Anwenden einer geeigneten Schutzart gegen das Eindringen von festen Fremdkörpern und Fluiden. Es wird die IP-Schutzart berücksichtigt (siehe IEC 60529:1989+AMD1:1999+AMD2:2013+Cor1:2019)	M, D, U
Begrenzung von Geschwindigkeit, Beschleunigung und Ruck (um mechanische Beanspruchungen zu vermeiden oder zu begrenzen)	Ein Beispiel ist die Beschleunigungsgrenze eines Motors durch Begrenzung des Motorstroms in einem Frequenzumrichter.	M, D

Tabelle D.1 (*fortgesetzt*)

Grundlegendes Sicherheitsprinzip	Bemerkungen	Maßgebend für (siehe Tabelle 2)
Verringerung der Reaktionszeit	Minimieren der Verzögerung bei der Energietrennung der zum Schalten verwendeten Bauteile. Geeigneter Schaltzeitbereich, z. B. Reaktionszeit von Geräten und Bauteilen (z. B. Magnetspulen, Schaltschütze, Relais) und die Auswirkungen der EMI-Maßnahmen auf diese Elemente (z. B. Rauschunterdrückungsdioden an Schaltschützen).	M, D
Schutz gegen unerwarteten Anlauf (siehe ISO 12100:2010, 6.2.11.4, ISO 14118:2017)	Berücksichtigen von unerwartetem Anlauf, verursacht durch gespeicherte Energie und nach Wiederherstellung der Energieversorgung, für unterschiedliche Betriebsarten, z. B. Betriebsmodus, Instandhaltungsmodus. (siehe IEC 60204-1:2016 + AMD1:2021).	M, D
	Eine besondere Einrichtung zum Abbau der gespeicherten Energie kann notwendig sein. Besondere Anwendungen, z. B. zur Beibehaltung der Energie für Spanneinrichtungen oder zur Sicherung einer Position, müssen gesondert betrachtet werden.	M, D, U
Vereinfachung	Vermeiden von unnötigen Bauteilen im sicherheitsbezogenen System.	M, D
Trennung	Trennung der sicherheitsbezogenen Funktionen von anderen Funktionen.	M, D
Strombegrenzung (z. B. zur Vermeidung von Verschleiß)	Ein Beispiel ist ein Widerstand (Reihenwiderstand).	M, D
Richtige Schutzleiterverbindung	Eine Seite des Steuerstromkreises, ein Anschluss der Betätigungsspule von jedem elektromagnetisch betätigten Gerät oder ein Anschluss anderer elektrischer Geräte wird mit dem Schutzleiter verbunden. (siehe IEC 60204-1:2016 + AMD1:2021, 9.4.3.1)	M, D, U
Isolationsüberwachung	Verwendung einer Einrichtung zur Isolationsüberwachung, die einen Erdschluss entweder anzeigt oder den Stromkreis nach einem Erdschluss selbsttätig unterbricht. (siehe IEC 60204-1:2016 + AMD1:2021, 6.3.3)	M, D, U
Unterdrückung von Spannungsspitzen	Verwendung einer Einrichtung zur Unterdrückung der Spannungsspitzen (RC-Glied, Diode, Varistor) parallel zur Last, jedoch nicht parallel zu den Kontakten. ANMERKUNG Durch eine Diode wird die Ausschaltzeit erhöht.	M, D
Temperaturbereich	Externe und interne Temperatureinwirkungen werden für das gesamte System betrachtet.	M, D, U

Tabelle D.1 (fortgesetzt)

Grundlegendes Sicherheitsprinzip	Bemerkungen	Maßgebend für (siehe Tabelle 2)
Sichere Befestigung der Eingabegeräte	Eingabegeräte, z. B. Verriegelungsschalter, Positionsschalter, Endschalter, Näherungsschalter, werden so gesichert, dass Stellung, Ausrichtung und Schalttoleranzen unter allen zu erwartenden Bedingungen, z. B. Vibration, üblicher Verschleiß, Eindringen von Fremdkörpern, Temperatur, eingehalten werden. (siehe ISO 14119:2024, Abschnitt 5)	M, D, U
Schutz des Steuerstromkreises	Der Schutz wird nach IEC 60204-1:2016 + AMD1:2021, 7.2 und 9.1.1, erbracht.	M, D
Aufeinanderfolgendes Schalten bei Stromkreisen mit in Reihe geschalteten Kontakten redundanter Signale	Zum Vermeiden gleichartiger Ausfälle durch das Verschweißen beider Kontakte findet das Ein- und Ausschalten nicht gleichzeitig statt, so dass ein Kontakt immer ohne Last schaltet.	M, D
Abkürzungen M – Entwurf und Herstellung von Bauteilen D – Entwurf von Teilsystemen U – Verwendung der Maschine		

Tabelle D.2 — Bewährte Sicherheitsprinzipien

Bewährtes Sicherheitsprinzip	Bemerkungen	Maßgebend für (siehe Tabelle 2)
Verwendung von Bauteilen mit gerichtetem Ausfallverhalten (siehe ISO 12100:2010, 6.2.12.3)	Nach Möglichkeit Bauteile oder Systeme mit gerichtetem Ausfallverhalten verwenden. Ein sicherer Zustand wird direkt oder indirekt (z. B. durch Fehlererkennung) durch die überwiegend auftretende Ausfallart erzielt.	M, D
Überdimensionierung	Unterbeanspruchung von Bauteilen, die in Sicherheitsschaltkreisen verwendet werden, z. B. durch die folgenden Maßnahmen: — der Strom, der durch die Schaltkontakte geleitet wird, sollte kleiner als die Hälfte ihres Bemessungsstroms sein; — die Schaltfrequenz der Bauteile sollte weniger als die Hälfte ihres Bemessungswertes betragen; — die Gesamtanzahl der erwarteten Schaltspiele sollte nicht mehr als 10 % der elektrischen Lebensdauer des Geräts betragen. ANMERKUNG Unterbeanspruchung kann von der sinnvollen Gestaltung abhängen. Sicherheitsfaktoren sind in Normen angegeben oder beruhen auf guter ingenieurmäßiger Praxis in sicherheitsbezogenen Anwendungen.	M, D
Abstände zwischen elektrischen Leitern	Anwenden eines ausreichenden Abstands zwischen Anschlussklemmen, Bauteilen und Leitungen, so dass unbeabsichtigte Verbindungen vermieden werden.	M, D
Verringerung von Fehlermöglichkeiten	Trennung sicherheitsbezogener Funktionen von anderen Funktionen	M, D
Mechanisch zwangsläufige Wirkung (siehe ISO 12100:2010, 6.2.5.)	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 14119:2024, 5.1). Um eine mechanisch zwangsläufige (oder direkte) Wirkung zu erreichen, werden mechanische Bauteile, die zur Ausführung der Sicherheitsfunktion erforderlich sind, entweder durch direkten Kontakt oder über starre Elemente bewegt.	M, D
Vervielfachung von Teilen	Verringerung der Auswirkung von Fehlern durch Verwendung mehrerer gleicher Teile, die parallel zueinander wirken, z. B. wenn ein Ausfall, der an einem von mehreren Widerständen auftritt, keinen gefährlichen Zustand bewirkt.	M, D
Verwendung bewährter Federn	Siehe Tabelle A.3	M

Tabelle D.2 (fortgesetzt)

Bewährtes Sicherheitsprinzip	Bemerkungen	Maßgebend für (siehe Tabelle 2)
Begrenzter Bereich der Kraft und ähnlicher Parameter, um mechanische Beanspruchungen zu vermeiden oder zu begrenzen Dieses Prinzip ist nicht anwendbar, wenn die kontinuierliche Funktionsfähigkeit der Bauteile unerlässlich dafür ist, den notwendigen Grad der Steuerbarkeit beizubehalten.	Spezifikation der notwendigen Begrenzung in Abhängigkeit von Erfahrungen und der jeweiligen Anwendung.	M, D
Begrenzter Bereich der Umgebungsparameter Siehe ISO 13849-1:2023, 10.7	Spezifikation der notwendigen Begrenzungen. Beispiele sind Temperatur, Luftfeuchte, Verunreinigung beim Einbau. Einhalten der Einbau- und Betriebsanleitungen des Herstellers.	M, D, U
Begrenzter Bereich der Reaktionszeit, Begrenzung der Hysterese	Spezifikation der notwendigen Begrenzungen. Zum Beispiel die korrekte Auswahl von Schutzeinrichtungen.	M, D
Mechanisch zwangsläufig verbundene Kontakte	Verwenden von mechanisch zwangsläufig verbundenen Kontakten für beispielsweise die Überwachungsfunktion in Systemen der Kategorie 2, 3 und 4 (IEC 61810-3:2015, IEC 60947-4-1:2023, Anhang F, IEC 60947-5-1:2024, Anhang L).	M, D
Fehlervermeidung oder -erkennung in Kabeln	Um Kurzschlüsse zwischen zwei benachbarten Leitungen zu vermeiden oder zu erkennen, — werden Kabel verwendet, bei denen die Abschirmung jeder einzelnen Leitung mit dem Schutzleitersystem verbunden ist; — wird in Flachkabeln ein Schutzleiter zwischen allen Signalleitungen verwendet; oder — werden Querschlossüberwachungen angewendet, z. B. durch Testimpulse.	M, D
Energiebegrenzungen	Zur Zuführung einer begrenzten Energiemenge wird ein Kondensator angewendet, z. B. bei Anwendung einer Zeittaktsteuerung.	M, D

Tabelle D.2 (fortgesetzt)

Bewährtes Sicherheitsprinzip	Bemerkungen	Maßgebend für (siehe Tabelle 2)
Begrenzung elektrischer Parameter	Begrenzung von Spannung, Strom, Energie oder Frequenz zur Einschränkung der Bewegung, z. B. durch Drehmomentbegrenzung, Zustimmschaltung mit Weg-/Zeitbegrenzung, reduzierte Geschwindigkeit, um einen unsicheren Zustand zu vermeiden.	M, D
Vermeidung undefinierter Zustände	Undefinierte Zustände in der Steuerung werden vermieden. Die Steuerung wird konstruktiv so gestaltet, dass während des üblichen Betriebs und unter allen erwarteten Betriebsbedingungen der Zustand der Steuerung, z. B. Ausgang/Ausgänge, vorherbestimmt werden kann.	M, D
Gerichtetes Ausfallverhalten	Wann immer möglich, sollte das Gerät/die Schaltung im Fehlerfall in einen sicheren Zustand übergehen.	M, D
Gleichgewicht zwischen Komplexität und Einfachheit	Gleichgewicht zwischen Komplexität, um eine bessere Steuerbarkeit zu erreichen, und Vereinfachung, um eine erhöhte Zuverlässigkeit zu erreichen.	M, D
Abkürzungen M – Entwurf und Herstellung von Bauteilen D – Entwurf von Teilsystemen U – Verwendung der Maschine		

Tabelle D.3 — Bewährte Bauteile

Bewährtes Bauteil	Zusätzliche Bedingungen für „bewährt“	Norm oder Spezifikation
Schalter mit zwangsläufiger Betätigung (Zwangsöffnung), z. B.: — Drucktaster; — Positionsschalter; —nockenbetätigte Wahlschalter, z. B. zur Auswahl der Betriebsart	—	IEC 60947-5-1:2024, Anhang K
Not-Halt-Gerät	—	ISO 13850:2015 IEC 60947-5-5:1997+AMD1:2005+AMD2:2016
Sicherung	—	IEC 60269-1:2024
Leistungsschalter	—	IEC 60947-2:2024
Lastschalter, Trennschalter	—	IEC 60947-3:2025

Tabelle D.3 (fortgesetzt)

Bewährtes Bauteil	Zusätzliche Bedingungen für „bewährt“	Norm oder Spezifikation
Fehlerstromschutzeinrichtung oder RCD (Fehlerstromschutzschalter, en: residual current device)	—	IEC 60947-2:2024
Hauptschutz	Nur bewährt, wenn: a) andere Einflüsse berücksichtigt werden, z. B. Schwingungen; b) Ausfall durch geeignete Verfahren vermieden ist, z. B. Überdimensionierung (siehe Tabelle D.2); c) der Kurzschlussstrom zur Last durch eine Schutzeinrichtung begrenzt ist, z. B. Temperatursicherung; und d) die Schaltungen mit einer Sicherung gegen Überlastungen geschützt werden.	IEC 60947-4-1:2023
Steuer- und Schutzschaltgerät oder -einrichtung (CPS, en: control and protective switching device)	—	IEC 60947-6-2:2020
Zwangsgeführte Relais (z. B. Hilfsschutz)	Nur bewährt, wenn: a) andere Einflüsse berücksichtigt werden, z. B. Schwingungen; b) zwangsläufiges Öffnen vorliegt; c) Ausfall durch geeignete Verfahren vermieden ist, z. B. Überdimensionierung (siehe Tabelle D.2); d) der Strom in den Kontakten durch eine Sicherung oder einen Schutzschalter begrenzt ist, um ein Verschweißen der Kontakte zu vermeiden; und e) Kontakte mechanisch zwangsgeführt sind, wenn sie für Überwachungen angewendet werden.	IEC 61810-1:2015/AMD1:2019 IEC 61810-2:2017 IEC 61810-3:2015 IEC 60947-5-1:2024 IEC 60947-4-1:2023, Anhang F

Tabelle D.3 (*fortgesetzt*)

Bewährtes Bauteil	Zusätzliche Bedingungen für „bewährt“	Norm oder Spezifikation
Relais	Nur bewährt, wenn: a) andere Einflüsse berücksichtigt werden, z. B. Schwingungen; b) Zwangsöffnung; 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.	IEC 61810-1:2015+AMD1:2019 IEC 61810-2:2017 IEC 61810-3:2015
Transformator	—	IEC 61558 (alle Teile)
Kabel	Der Schutz der Verkabelung außerhalb umschlossener Einbauträume gegen mechanische Beschädigung (einschließlich z. B. Schwingung oder Biegung) wird berücksichtigt.	IEC 60204-1:2016 + AMD1:2021, Abschnitt 12
Stecker und Steckdose	—	Nach einer elektrischen Norm, die für die vorgesehene Anwendung zutrifft. Zu Verriegelung siehe auch ISO 14119:2024.
Temperaturschalter	Nur bewährt, wenn:	ISO 13849-1:2023, 6.1.11 Für den elektrischen Teil siehe IEC 607301:2022

Tabelle D.3 (fortgesetzt)

Bewährtes Bauteil	Zusätzliche Bedingungen für „bewährt“	Norm oder Spezifikation
	a) das Bauteil die grundlegenden und bewährten Sicherheitsprinzipien im Hinblick auf die vorgesehene Anwendung erfüllt (siehe ANMERKUNG), einschließlich der Verwendung des Bauteils entsprechend den Spezifikationen des Herstellers; b) das Bauteil nachweislich in der Vergangenheit in zahlreichen Fällen mit dokumentierten erfolgreichen Ergebnissen bei ähnlichen Anwendungen im Einsatz war oder das Bauteil mittels Prinzipien, die seine Eignung und Zuverlässigkeit für sicherheitsbezogene Anwendungen entsprechend den Produkt- und Anwendungsnormen belegen, hergestellt, verifiziert und validiert wurde; c) entweder keine Onboard-Elektronik vorhanden ist oder wenn die Onboard-Elektronik, soweit vorhanden, nicht zur Ausführung der Sicherheitsfunktion beiträgt;	

Tabelle D.3 (*fortgesetzt*)

Bewährtes Bauteil	Zusätzliche Bedingungen für „bewährt“	Norm oder Spezifikation
	d) das Verhalten des Bauteils unter allen Bedingungen klar definiert ist und vollständig bestimmt werden kann; und e) die folgenden Konstruktionsmerkmale erfüllt sind: — einfache, widerstandsfähige Auslegung; — formschlüssige Verbindung; — ausreichender Schutz gegen Lösen von abnehmbaren Verbindungen; und — ausreichend widerstandsfähig in Bezug auf die Verwendung (Anwendung) und die Umgebungsbedingungen (z. B. Luftfeuchte, Vibration).	
ANMERKUNG Die Bestätigung von grundlegenden und bewährten Sicherheitsprinzipien sowie der Nachweis für den Einsatz in der Vergangenheit in zahlreichen Fällen mit dokumentierten erfolgreichen Ergebnissen bei ähnlichen Anwendungen können vom Bauteilhersteller oder vom Konstrukteur des Teilsystems erbracht werden.		

D.2 Fehlerausschluss

D.2.1 Allgemeines

Ein Fehlerausschluss ist nur dann gültig, wenn die Teile innerhalb ihrer spezifizierten Bemessungswerte betrieben werden.

D.2.2 „Zinn-Whisker“

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

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

ANMERKUNG 2 Die Literaturhinweise [47] und [48] können zur Beurteilung des Phänomens hilfreich sein.

E DIN EN ISO 13849-2:2026-03
prEN ISO 13849-2:2026 (D)

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

D.2.3 Kurzschlüsse an auf Leiterplatten montierten Teilen

Kurzschlüsse an Teilen, die auf einer Leiterplatte (PCB, en: printed circuit board) montiert sind, können nur dann ausgeschlossen werden, wenn der Fehlerausschluss „Kurzschluss zwischen zwei benachbarten Leiterbahnen/Kontaktstellen“ wie in Tabelle D.5 durchgeführt wurde.

D.2.4 Fehlerausschlüsse und integrierte Schaltkreise

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

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

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Kurzschluss zwischen zwei beliebigen Leitern	Kurzschlüsse zwischen Leitern, — die dauerhaft (fest) verlegt und gegen äußere Beschädigung geschützt sind, z. B. durch Kabelkanal, Panzerrohr; — die in unterschiedlichen Mantelleitungen liegen; — die innerhalb eines elektrischen Einbauraumes (siehe Bemerkung) liegen; oder — die einzeln durch eine Erdverbindung geschützt sind.	Voraussetzung ist, dass sowohl die Leitungen als auch der Einbauraum den jeweiligen Anforderungen entsprechen (siehe IEC 60204-1:2016 + AMD1:2021).
Kurzschluss zwischen einem beliebigen Leiter und einem ungeschützten leitenden Teil oder Erde oder einer Schutzleiterverbindung	Kurzschlüsse zwischen Leiter und jedem ungeschützten leitenden Teil innerhalb eines Einbauraumes (siehe Bemerkung).	
Unterbrechung eines Leiters	Nein.	—

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

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Kurzschluss zwischen benachbarten Leiterbahnen/Kontaktstellen	Kurzschlüsse zwischen benachbarten Leitern, wenn die Bemerkungen zutreffen.	Als Basismaterial wird mindestens EP GC nach IEC 60893-1:2004 verwendet. Luft- und Kriechstrecken werden mindestens nach IEC 60664-1:2025 mit Verschmutzungsgrad 2/Überspannungskategorie III bemessen. Wenn beide Leiterbahnen über ein SELV/PELV-Netzgerät versorgt werden, gilt Verschmutzungsgrad 2/Überspannungskategorie II mit einer Mindestluftstrecke von 0,1 mm. Die bestückte Leiterplatte ist in ein Gehäuse eingebaut, das vor leitfähiger Verschmutzung schützt, z. B. ein Gehäuse mit einem Schutzgrad von mindestens IP54, und die bedruckte(n) Seite(n) der bestückten Leiterplatte wird/werden mit einer alterungsbeständigen Lack- oder Schutzschicht so versehen, dass alle Leiterbahnen abgedeckt sind. ANMERKUNG 1 Erfahrungen haben gezeigt, dass Lötmasken als Schutzschicht ausreichen. ANMERKUNG 2 Eine weitere Schutzschicht, die nach IEC 60664-3:2016 abdeckt, kann die Kriech- und Luftstrecken verringern.
Unterbrechung in einer beliebigen Leiterbahn	Nein.	—

Tabelle D.6 — Fehler und Fehlerausschlüsse — Klemmstellen

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Kurzschluss zwischen benachbarten Klemmen	Kurzschluss zwischen benachbarten Klemmen, wenn die Bemerkung 1) oder 2) zutrifft.	1) Es werden Klemmen und Verbindungen nach IEC 60947-7-1:2025 oder IEC 60947-7-2:2009 verwendet, und die Anforderungen von IEC 60204-1:2016 + AMD1:2021, 13.1.1, sind erfüllt. 2) Die Ausführung selbst stellt sicher, dass ein Kurzschluss verhindert wird, z. B. durch Kunststoff-Schrumpfschlauch über der Verbindungsstelle.
Unterbrechung einzelner Klemmen	Nein.	—

Tabelle D.7 — Fehler und Fehlerausschlüsse — Mehrpolige Steckverbindungen

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Kurzschluss zwischen zwei beliebigen benachbarten Steckerstiften	Kurzschluss zwischen benachbarten Steckerstiften, wenn die Bemerkung zutrifft. Wenn der Steckverbinder auf eine PCB montiert ist, gelten die Erwägungen zum Fehlerausschluss aus Tabelle D.5.	Für mehradrige Drähte durch Verwendung von Aderendhülsen oder anderen geeigneten Mitteln. Kriech- und Luftstrecken und alle Abstände sollten mindestens nach IEC 60664-1:2025, Überspannungskategorie III, bemessen sein.
Vertauschter oder nicht richtig eingeführter Steckverbinder, wenn keine mechanische Möglichkeit zur Verhinderung vorgesehen ist	Nein.	—
Kurzschluss zwischen einem beliebigen Leiter (siehe Bemerkung) und Erde oder einem leitenden Teil oder dem Schutzleiter	Nein.	Der Kern des Kabels wird als Teil der mehrpoligen Steckverbindung angesehen.
Unterbrechung einzelner Steckerstifte	Nein.	—

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

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Nichtschließen von Kontakten	Nein.	—
Nichtöffnen von Kontakten	Kontakte nach IEC 60947-5-1:2024, Anhang K, öffnen sich.	—
Kurzschluss von benachbarten Kontakten, die voneinander isoliert sind	Kurzschluss für Schalter nach IEC 60947-5-1:2024 kann ausgeschlossen werden (siehe Bemerkung).	Leitfähige Teile, die sich lösen, sollten die Isolation zwischen Kontakten nicht überbrücken können.
Gleichzeitiger Kurzschluss zwischen den drei Klemmen von Wechselkontakten	Gleichzeitige Kurzschlüsse für Schalter nach IEC 60947-5-1:2024 können ausgeschlossen werden (siehe Bemerkung).	
ANMERKUNG 1 Für PL e ist ein Fehlerausschluss für mechanische (z. B. die mechanische Verbindung zwischen Stellglied und Kontaktelementen) und elektrische Aspekte nicht zulässig. In diesem Fall ist Redundanz erforderlich. Für Not-Halt-Einrichtungen nach IEC 60947-5-5:1997+AMD1:2005+AMD2:2016 ist ein Fehlerausschluss für mechanische Aspekte zulässig, wenn eine Höchstanzahl von Betätigungen berücksichtigt wird.		
ANMERKUNG 2 Die Fehlerlisten für die mechanischen Gesichtspunkte sind im Anhang A enthalten.		

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

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Alle Kontakte bleiben in der eingeschalteten Position, wenn die Spule abgeschaltet ist (z. B. durch einen mechanischen Fehler)	Nein.	—
Alle Kontakte bleiben abgeschaltet, wenn Energie ansteht (z. B. durch einen mechanischen Fehler, Unterbrechung der Spule)	Nein.	
Nichtöffnen von Kontakten	Nein.	
Nichtschließen von Kontakten	Nein.	
Gleichzeitiger Kurzschluss zwischen den drei Klemmen eines Wechselkontaktes	Gleichzeitiger Kurzschluss kann ausgeschlossen werden, wenn die Bemerkungen zutreffen.	Die Kriech- und Luftstrecken werden mindestens nach IEC 60664-1:2025 mit mindestens Verschmutzungsgrad 2/Überspannungskategorie III bemessen. Leitfähige Teile, die sich lösen, können die Isolation zwischen den Kontakten und der Spule nicht überbrücken.
Kurzschluss zwischen zwei Kontakten untereinander und/oder zwischen Kontakten und Anschlüssen der Spule	Kurzschluss kann ausgeschlossen werden, wenn die Bemerkungen zutreffen.	
Gleichzeitiges Geschlossensein von Schließer- und Öffnerkontakten	Gleichzeitiges Geschlossensein der Kontakte kann ausgeschlossen werden, wenn die Bemerkung zutrifft.	Es werden zwangsläufig betätigte (oder mechanisch verbundene) Kontakte verwendet (siehe IEC 60947-5-1:2024, Anhang L).

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

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Ausgang dauernd niederohmig	Nein (siehe Bemerkung).	Siehe IEC 60947-5-3:2013.
Ausgang dauernd hochohmig	Nein (siehe Bemerkung).	Es sollten Maßnahmen zur Fehlerverhinderung beschrieben werden.
Spannungsversorgung unterbrochen	Nein.	—

Tabelle D.10 (fortgesetzt)

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Nichtbetätigen des Schalters infolge eines mechanischen Ausfalls	Nichtbetätigung infolge eines mechanischen Ausfalls, wenn die Bemerkung zutrifft.	Alle Teile des Schalters sollten mechanisch ausreichend gut befestigt sein. Für mechanische Aspekte siehe Anhang A.
Kurzschluss zwischen den drei Anschlüssen eines Wechselkontaktes	Nein.	—

Tabelle D.11 — Fehler und Fehlerausschlüsse — Schalter — Magnetventile

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

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

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Unterbrechung einer Wicklung	Nein.	—
Kurzschluss zwischen verschiedenen Wicklungen	Kurzschluss zwischen verschiedenen Wicklungen kann ausgeschlossen werden, wenn Bemerkung 1) und Bemerkung 2) zutreffen.	1) Es sollten die Anforderungen der zutreffenden Teile von IEC 61558 (alle Teile) erfüllt sein. 2) Zwischen unterschiedlichen Wicklungen werden doppelte oder verstärkte Isolierungen oder eine Schutzabdeckung angewendet. Es gilt z. B. die Prüfung nach IEC 61558-1:2017, Abschnitt 18. Geeignete Prüfspannungen sind in IEC 61558-1:2017, Tabelle 8 a), oder in anderen zutreffenden Produktnormen angegeben. Windungs- und Wicklungsschlüsse sind durch geeignete Maßnahmen zu verhindern, z. B. durch:
Kurzschluss in einer Wicklung	Ein Kurzschluss in einer Wicklung kann ausgeschlossen werden, wenn Bemerkung 1) zutrifft.	
Veränderung des wirksamen Windungsverhältnisses	Veränderung des wirksamen Verhältnisses der Windungen kann ausgeschlossen werden, wenn Bemerkung 1) zutrifft. Siehe auch Bemerkung 3).	

Tabelle D.12 (fortgesetzt)

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
		— Imprägnierung der Windungen und Wicklungen, so dass alle Hohlräume zwischen Wickelkörper und Wicklung ausgefüllt sind; — Verwendung von Wickeldrähten deutlich innerhalb ihrer Isolations- und Hochtemperaturbemessungswerte. 3) Bei sekundärem Kurzschluss sollte keine Erwärmung über die festgelegte Betriebstemperatur hinaus auftreten.

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

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

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

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Unterbrechung	Nein.	—
Kurzschluss	Kurzschluss kann ausgeschlossen werden, wenn Bemerkung 1) oder Bemerkung 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 (en: surface-mounted device) müssen vom Typ Metallschicht, Gehäusotypen MELF, mini MELF oder μMELF sein. 3) Z.B., wenn das Risiko der Zinn-Whisker-Bildung als hoch eingestuft wird, ist der Fehlerausschluss „Kurzschluss eines Widerstands“ nutzlos, da ein Kurzschluss zwischen den Kontakten dieses Bauteils betrachtet werden muss.
Zufällige Veränderung des Wertes $0,5 R_N < R < 2 R_N$, wobei R_N der Nennwert des Widerstandes ist	Nein.	Abhängig von der Art der Bauweise können andere Bereiche in Betracht gezogen werden.

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

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

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

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

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

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

Tabelle D.18 — Fehler und Fehlerausschlüsse — Elektronische Bauteile — Diskrete Halbleiter (z. B. Dioden, Zener-Dioden, Transistoren, Triacs, Thyristoren, Spannungsregler, Quarzkristall, Phototransistoren, lichtemittierende Dioden [LEDs])

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

Tabelle D.19 — Fehlern und Fehlerausschlüssen — Elektronische Bauteile — Koppler für galvanische Trennung (z. B. Optokoppler, kapazitive Koppler)

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Unterbrechung eines einzelnen Anschlusses	Nein.	—
Kurzschluss zwischen zwei beliebigen eingangsseitigen Anschlüssen	Nein.	
Kurzschluss zwischen zwei beliebigen ausgangsseitigen Anschlüssen	Nein.	
Kurzschluss zwischen zwei beliebigen Anschlüssen des Ein- und Ausgangs	Kurzschluss zwischen Ein- und Ausgang kann ausgeschlossen werden, wenn die Bemerkungen zutreffen.	Der Optokoppler ist entsprechend Überspannungskategorie III nach IEC 60664-1:2025 gebaut. Wird ein SELV/PELV-Netzanschluss verwendet, gelten Verschmutzungsgrad 2/Überspannungskategorie II. ANMERKUNG Siehe Tabelle D.5. Es werden Maßnahmen getroffen, um sicherzustellen, dass ein interner Fehler des Kopplers für galvanische Trennung nicht zu übermäßigem Temperaturanstieg seines Isoliermaterials führen kann.

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

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Unterbrechung eines einzelnen Anschlusses	Nein.	—
Kurzschluss zwischen zwei beliebigen Anschlüssen	Nein.	—
Stuck-at-Fehler (d. h. Kurzschluss zu 1 und 0 bei isoliertem Eingang oder unterbrochenem Ausgang). Statisches „0“- und „1“-Signal an allen Ein- und Ausgängen, einzeln oder gleichzeitig	Nein.	—
Störschwingung der Ausgänge	Nein.	—
Veränderung von Kennwerten (z. B. Eingangs-/Ausgangsspannung analoger Bauteile oder Änderung von Informationen infolge Soft-Error, wenn dies relevant erscheint)	Nein.	Siehe Abschnitt D.3.
ANMERKUNG In diesem Dokument werden integrierte Schaltkreise (IC) mit entweder weniger als 1 000 Gates oder weniger als 24 Pins oder beidem, Operationsverstärker, Schieberegister und Hybridmodule als nicht komplex betrachtet. Diese Festlegung ist willkürlich.		

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

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Fehler in allen Teilen der Funktion oder in einem Teil der Funktion einschließlich Software-Fehler	Nein.	—
Unterbrechung eines einzelnen Anschlusses	Nein.	—
Kurzschluss zwischen zwei beliebigen Anschlüssen	Nein.	—
Stuck-at-Fehler (d. h. Kurzschluss zu 1 und 0 bei isoliertem Eingang oder unterbrochenem Ausgang). Statisches „0“- und „1“-Signal an allen Ein- und Ausgängen, einzeln oder gleichzeitig	Nein.	—
Störschwingung der Ausgänge	Nein.	—
Veränderung des Wertes, z. B. — Eingangs-/Ausgangsspannung analoger Bauteile — Änderung der Informationen infolge Soft-Error, wenn dies als maßgebend gilt, z. B. für RAM, FPGA	Nein.	Siehe Abschnitt D.3
Unerkannte Fehler in der Hardware, die wegen der Komplexität des integrierten Schaltkreises nicht entdeckt werden	Nein.	—
ANMERKUNG 1 Die Analyse sollte zusätzliche Fehler aufdecken, die berücksichtigt werden sollten, wenn sie die Ausführung der Sicherheitsfunktion beeinflussen.		
ANMERKUNG 2 In diesem Dokument wird ein IC als komplex betrachtet, wenn er aus entweder mehr als 1 000 Gates oder mehr als 24 Pins oder beidem besteht. Diese Festlegung ist willkürlich.		

Tabelle D.22 — Fehler und Fehlerausschlüsse — Übertragungsfehler in der digitalen Datenkommunikation

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Kommunikationsfehler (Verfälschung, unbeabsichtigte Wiederholung, falsche Reihenfolge, Verlust, unzulässige Verzögerung, Einfügung, Maskerade, Adressierung)	Nein	Maßnahmen zur Beherrschung der Auswirkungen von Fehlern und anderen Auswirkungen durch die Datenkommunikation, einschließlich Übertragungsfehler (wie Verfälschung, unbeabsichtigte Wiederholung, falsche Reihenfolge, Verlust, unzulässige Verzögerung, Einfügung, Maskerade, Adressierung) sollten angewendet werden. ANMERKUNG 1 Weitere Informationen können IEC 61784-3:2021+AMD1:2024, 5.3, Tabelle 1 und IEC 61508-2:2010, 7.4.11.2, entnommen werden. ANMERKUNG 2 Der Begriff „Maskerade“ bedeutet, dass der wahre Inhalt einer Nachricht nicht korrekt identifiziert wird. Eine Nachricht von einem nicht sicherheitsrelevanten Bauteil wird zum Beispiel fälschlicherweise als eine Nachricht von einem sicherheitsrelevanten Bauteil eingestuft.

D.3 Soft-Errors

D.3.1 Allgemeines

Soft-Errors sind relevant für Hardware, die Halbleiter mit flüchtigen Speichern und sequenzieller Logik enthält.

Bauteile können ohne Berücksichtigung von Soft-Error-Raten verwendet werden, wenn in Hardware, SRESW oder SRASW implementierte Minderungsmaßnahmen (siehe D.3.4.3) integriert sind. Der Beitrag von Soft-Errors zur PFH wird üblicherweise auf Teilsystemebene in den folgenden drei Schritten betrachtet: Analyse, Vermeidung und Beherrschung. Soft-Errors werden üblicherweise bis zur Teilsystemebene betrachtet. Während der Entwurfsphase für die Integration von Teilsystemen in SRP/CS besteht in der Regel keine Notwendigkeit, Soft-Errors zu berücksichtigen.

Für weitere Informationen zu Soft-Errors siehe auch IEC 61508-2-1, 1. Ausgabe (in Vorbereitung), und IEC 61508-4:2010.

D.3.2 Einführung in Soft-Errors

Soft-Errors:

- sind nicht dauerhafte, unbeabsichtigte Hardware-Zustände, z. B. Umkehrung oder Umschaltung des Datenzustands einer Halbleiterspeicherzelle, eines Latches oder eines Flip-Flops, was als latenter Fehler bestehen bleiben kann;
- sind Arten von Fehlern, bei denen ein Signal oder ein Datenwert verfälscht ist, aber keine dauerhafte Schädigung der Hardware vorliegt;
- werden hauptsächlich durch Ladungsstörungen aufgrund von Strahlungsereignissen verursacht (Alpha-Teilchen aus dem Zerfall von Gehäusematerial und kosmische Strahlung, die energiereiche Neutronen erzeugt);
- sind zufällige Hardware-Fehler, die mit einem probabilistischen Verfahren, das von Messwerten gestützt wird, quantifiziert werden können;
- betreffen hauptsächlich flüchtige Speicher und die sequenzielle Logik;
- können als Single-Event-Upset (SEU) oder Multiple-Bit-Upset (MBU) eingestuft werden.

D.3.3 Bedeutung von Soft-Errors für die funktionale Sicherheit

Dieses Dokument gibt in Abschnitt D.1 (Allgemeines) an, dass für die Validierung sowohl die dauerhaft auftretenden Fehler als auch die kurzzeitigen Störungen berücksichtigt werden sollten.

Besonders digitale Schaltkreise, z. B. RAM, FPGA, Mikrocontroller, sind sehr anfällig für Soft-Errors. Flash-Speicher sind nicht flüchtig und sind deshalb normalerweise weniger anfällig.

Bei bestimmten Technologien können Soft-Error-Raten gegenüber den Raten von dauerhaft auftretenden zufälligen Hardware-Fehlern überwiegen. Dies hängt von der Anzahl und Dichte der Speicherzellen im RAM-Speicher ab.

Für Hardware-Fehler wirksame Diagnosemaßnahmen sind für Soft-Errors möglicherweise nicht wirksam. Die Auswirkungen von Soft-Errors können durch entsprechende Sicherheitsmaßnahmen während der Laufzeit beherrscht werden. RAM-Tests wie Walkpath, Galpat usw. sind nicht wirksam, wohingegen überwachende Verfahren wie Parity und Fehlerkorrekturcode (ECC, en: error correcting code) mit dem wiederholenden Auslesen der Speicherzellen wirksam sind.

Es wird davon ausgegangen, dass Soft-Errors auch in der Zukunft relevant bleiben. Dies ist auf die Geräteskalierung sowie auf die fortlaufende Verringerung der Größe des Technologieknotens und der Versorgungsspannung des integrierten Schaltkreises zurückzuführen.

Für weitere Informationen siehe IEC 61508-7:2010, A.5.

D.3.4 Vermeiden und Beherrschen von Soft-Errors während des Entwurfs von Teilsystemen

D.3.4.1 Analyse

Jeder integrierte Schaltkreis, der z. B. Flip-Flops, Latches, flüchtige Speicherelemente oder analoge Bauteile enthält, sollte auf potentielle Anfälligkeit gegenüber Soft-Errors untersucht werden.

Die in den integrierten Schaltkreisen umgesetzten Diagnosemaßnahmen, wie z. B. ECC, können die Wahrscheinlichkeit, dass ein Soft-Error zu einem gefahrbringenden Ausfall der Sicherheitsfunktion führt, verringern.

Offline-CPU-Selbsttests oder RAM-Tests sind im Fall von Soft-Errors nicht wirksam. Die Auswirkungen von Soft-Errors können nur durch Sicherheitsmaßnahmen während der Laufzeit beherrscht werden. Das Bereinigen (en:scrubbing) von Daten in Speichern ist eine Möglichkeit, um die Ansammlung von Multibit-Fehlern zu verringern.

D.3.4.2 Vermeiden und Reduzieren von Soft-Errors

Die Wahrscheinlichkeit für das Auftreten von Soft-Errors kann verringert werden, indem elektronische Bauteile mit hoher Anfälligkeit für Soft-Errors vermieden werden oder indem diese elektronischen Bauteile durch Bauteile mit einer geringen Anfälligkeit ersetzt werden. Geeignete Bauteile mit niedrigen Soft-Error-Raten sollten entsprechend ihren Datenblättern oder entsprechend den Informationen ihres Herstellers ausgewählt werden.

ANMERKUNG In Abhängigkeit von der Anwendung ist es manchmal nicht möglich, Soft-Errors vollständig zu vermeiden, wenn komplexe elektronische Bauteile verwendet werden (die Speicherelemente enthalten).

Abhängig von der Anwendung können Entwurfsmaßnahmen auf Teilsystem- oder SRP/CS-Ebene, z. B. durch Abschirmungen gegen kosmische Strahlen, die Wahrscheinlichkeit für das Auftreten von Soft-Errors verringern. Eine Abschirmung wirkt nicht gegen radioaktive Verunreinigungen im Chipgehäuse oder in dem Halbleitermaterial selbst.

D.3.4.3 Beherrschen von Soft-Errors

Zur Verbesserung der Beherrschung von Soft-Errors können zusätzliche Maßnahmen wie z. B. strahlungsfeste Ausführung oder Softwaremaßnahmen (z. B. On-Chip-ECC oder redundante Datenspeicherung) angewendet werden.

Für einkanalige Architekturen wie die Kategorien B und 2 sind softwareseitige Minderungsmaßnahmen, z. B. basierend auf Redundanz von Informationen (z. B. durch Hinzufügen zusätzlicher Informationen zu den Daten mittels Fehlerkorrekturcodes) oder zeitliche Redundanz (z. B. durch Ausführung desselben Programms zweimal nacheinander; SEU werden durch Vergleich erkannt), wirksam gegen gefahrbringende Ausfälle durch Soft-Errors.

ANMERKUNG Für Informationen zu Lösungen für die Minderung von Soft-Errors siehe [50].

Redundante Funktionskanäle mit Fehlererkennung durch Vergleich sind sehr wirksam gegen gefahrbringende Ausfälle infolge von Soft-Errors. Da Soft-Errors lokale Ursachen besitzen, weist selbst eine homogene Redundanz eine hohe Wirksamkeit auf. Dies unterscheidet sie von Ausfällen aufgrund gemeinsamer Ursache (CFF, en: common cause failures), bei denen homogene Redundanz in einigen Fällen weniger wirksam ist.

Soft-Errors sind für einkanaligen Architekturen wie die Kategorien B und 1 kritischer, aber Kategorie B ist begrenzt auf einen PL b. Des Weiteren werden komplexe Bauteile nach D.3.2 in Kategorie 1 nicht mit bewährten Bauteilen gleichgestellt.

Soft-Errors können einkanalige Strukturen wie Kategorie 2 mit niedrigem Diagnosedeckungsgrad erheblich beeinflussen. In diesem Fall ist der PL auf PL c oder, in seltenen Fällen, auf PL d begrenzt.

Soft-Errors sind für einkanalige Architekturen wie Kategorie 2 mit mindestens mittlerem Diagnosedeckungsgrad oder für Architekturen mit redundanten Kanälen wie Kategorie 3 und 4 weniger kritisch.

D.3.4.4 Bestimmung von Soft-Error-Raten zur Abschätzung der PFH

Für die Bestimmung der PFH können relevante Soft-Error-Raten auf die gleiche Weise wie die Hardware-Fehlerraten betrachtet werden.

Es wird nicht davon ausgegangen, dass Soft-Errors beide Kanäle in einem System der Kategorie 2, 3 oder 4 auf die gleiche Weise beeinflussen. Aus diesem Grund braucht die Soft-Error-Rate üblicherweise nicht im CCF-Teil der PFH-Berechnung berücksichtigt zu werden.

In der Regel hängt der Anteil der Soft-Error-Rate, die von kosmischer Strahlung hervorgerufen wird, von der Höhe über dem Meeresspiegel ab. Für Anwendungen, deren Durchführung in höheren Höhenlagen vorgesehen ist, siehe [49] für weitere Informationen.

D.3.4.5 Priorität bei der Bestimmung von Soft-Error-Raten

Die Hauptquelle für Soft-Error-Raten sind die Daten, die vom Halbleiterhersteller bereitgestellt werden, z. B. Datenblätter und White Papers.

ANMERKUNG 1 Es ist wünschenswert, dass der Halbleiterhersteller die grundlegenden Ausfallraten, die durch Alpha-Teilchen und Neutronen hervorgerufen werden, dem Teilsystemhersteller zur Verfügung stellt, z. B. in einem Sicherheits-handbuch [49]. Sie dienen als Hauptbezugswerte für die Prüfung und Berechnung der Soft-Error-Rate durch die Halbleiterhersteller. Auf Halbleiterebene ist logische und elektrische Maskierung möglich. Des Weiteren können Prozessmaßnahmen, Gestaltungsmaßnahmen oder Entwurfstechniken Soft-Errors verhindern oder reduzieren.

Wenn der Halbleiterhersteller keine Soft-Error-Raten angibt, können alternativ Schätzwerte verwendet werden. Die Dokumente, die von der International Roadmap for Devices and Systems (IRDS) gepflegt werden, wie die International Technology Roadmap for Semiconductors (ITRS), enthalten prognostizierte Werte für die Soft-Error-Rate für jede Chip-Generation.

Als letzte Option können SN 29500-2:2010 (Soft-Error-Rate 1 000 FIT/Mbit für SRAM-Komponenten) oder andere generische Quellen zur groben Schätzung genutzt werden.

ANMERKUNG 2 SN 29500-1:2016, Abschnitt 3, legt die Ausfallraten in FIT (Ausfälle je Zeiteinheit) fest, d. h. die Anzahl an Ausfällen in 10^9 Bauteil-Stunden. Somit ist $\lambda = 1$ FIT gleich $\lambda = 10^{-9} \text{ h}^{-1}$ ($\lambda = 1/\text{MTTF}$, somit ist $\lambda = 1$ FIT gleich $\text{MTTF} = 114\,155 \text{ a}$).

D.3.4.6 Nicht zugängliche Hardware

Im Zusammenhang mit Soft-Errors bedeutet eine nicht zugängliche Hardware beispielsweise, dass Bauteile ohne Sicherheitsbewertung durch den Hersteller als „Black-Box“-Bauteile während des Entwurfs von Teilsystemen verwendet werden. Der Beitrag von Soft-Error-Raten zum PFH-Wert eines Teilsystems kann üblicherweise nicht ermittelt werden, da die notwendigen ausführlichen internen Hardware-Informationen (z. B. Art, Anzahl, Ausfallrate und Umfang der beteiligten programmierbaren Logik und der Anteil der Speicher-Bits, die für die ordnungsgemäße Ausführung der Sicherheitsfunktion sicherheitsrelevant sind) dem Integrator oder Konstrukteur des Teilsystems nicht zu Verfügung stehen. Diese Bauteile können ohne Berücksichtigung von Soft-Error-Raten verwendet werden, wenn die in Hardware, SRESW oder SRASW integrierten softwareseitigen Minderungsmaßnahmen (siehe D.3.4.3) in die nicht zugängliche Hardware aufgenommen wurden. Wenn keine Informationen über die Umsetzung von softwareseitigen Minderungsmaßnahmen verfügbar sind oder

wenn es nicht möglich ist, softwareseitige Minderungsmaßnahmen in Hardware, SRESW oder SRASW umzusetzen, können als letzte Möglichkeit diese Bauteile unter Berücksichtigung von Soft-Error-Raten verwendet werden, die als eine um 10 % reduzierte berechnete $MTTF_D$ für zufällige Hardware-Fehler abgeschätzt wurde.

ANMERKUNG 1 Der 10 %-Schätzwert basiert auf der Annahme, dass üblicherweise nur ein kleiner Teil des flüchtigen Speichers sicherheitsrelevant ist und zu einem gefahrbringenden Ausfall führen kann. Außerdem nutzen die meisten modernen Speichertechnologien interne Soft-Error-Korrekturmechanismen.

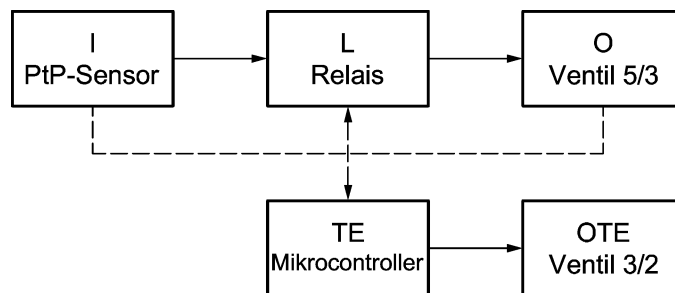
Siehe auch ISO 13849-1:2023, 7.3.2, wenn die nicht zugängliche Hardware nicht zugängliche Embedded-Software enthält.

ANMERKUNG 2 Soft-Errors leisten üblicherweise keinen Beitrag zum PFH-Anteil infolge CCF, der normalerweise den größten PFH-Beitrag in den Kategorien 3 und 4 ausmacht (siehe D.3.4.4).

ANMERKUNG 3 Für Bauteile ohne eine Sicherheitsbewertung durch den Hersteller ist der vom Bauteilhersteller erhältliche Zuverlässigkeitswert üblicherweise nur eine grobe Schätzung.

D.3.5 Beispiel für die Darstellung des Beitrags von Soft-Errors zur PFH-Abschätzung

Das Beispiel für ein SRP/CS der Kategorie 2 in Bild D.1 dient der Darstellung des Beitrags von Soft-Errors zur Abschätzung der PFH entsprechend den in D.3.4 festgelegten Verfahren. Die Beschreibung sämtlicher Einzelheiten, die für Soft-Errors nicht relevant sind, wurde weggelassen.



Legende

- > Verbindungsmittel
- - -> Überwachung/Testung

Bild D.1 — Sicherheitsbezogenes Blockdiagramm für ein SRP/CS der Kategorie 2

Eine Analyse der Relevanz von Soft-Errors in diesem Beispiel zeigt, dass nur der Mikrocontroller (TE) anfällig für Soft-Errors ist.

Für dieses Beispiel wurde ein 64-Bit-Mikrocontroller mit ARM-Architektur gewählt, der in vielen Steuerungskonstruktionen zur Anwendung kommt. Entsprechend dem Datenblatt des Herstellers besitzt er einen 2-GByte-Arbeitsspeicher (DRAM), einen internen physischen 4-GByte-Solid-State-Speicher (eMMC) sowie einen internen remanenten 128-kByte-Solid-State-Speicher (NVRAM).

Nur der flüchtige Speicher (DRAM) leistet einen Beitrag zur Soft-Error-Rate, da die Solid-State-Speicher (eMMC und NVRAM) nicht von den Soft-Errors betroffen sind.

Fehler in der Datenübertragung zwischen einem PtP-Sensor (ein Sensor, der mittels eines Punkt-zu-Punkt-Protokolls kommuniziert) und einem Mikrocontroller infolge von Soft-Errors werden erfolgreich mithilfe von Fehlererkennungsmechanismen im Datenübertragungsprotokoll durch zyklische Redundanzprüfungen (CRC, en: cyclic redundancy checks) und andere typische Maßnahmen beherrscht. Die Verbindung zwischen dem PtP-Sensor und dem Relais basiert auf einem 24 V Gleichspannungssignal, das nicht anfällig ist für Soft-Errors. Das gleiche gilt für die Verbindungen zu den Ventilen.

Die Vermeidung und Reduzierung von Soft-Errors wurde in diesem Beispiel durch die Wahl eines Mikrocontrollers berücksichtigt, der für diese Anwendung geeignet ist und eine geringe Anfälligkeit für Soft-Errors zeigt (niedrige Soft-Error-Rate). Aufgrund der Trennung der sicherheitsbezogenen Embedded-Software (SRESW) von der nicht sicherheitsbezogenen Software kann durch Analyse des Maschinencodes abgeschätzt werden, dass nur etwa 1 MByte der gesamten 2 GByte DRAM SRESW enthält.

Im Datenblatt legt der Hersteller des Mikrocontrollers eine Soft-Error-Rate von 100 FIT/MByte für den integrierten flüchtigen Speicher fest. Mittels einer Worst-Case-Abschätzung von 50 % gefahrbringender Ausfälle führt dies zu einer gefahrbringenden Ausfallrate infolge Soft-Errors von $\lambda_D = 50$ FIT (oder $MTTF_D = 2\,283$ a, siehe D.3.4.5, ANMERKUNG 2) Da das Auftreten von Soft-Errors und dauerhaft auftretenden zufälligen Hardware-Fehlern statistisch voneinander unabhängig ist, sind beide zugehörigen Ausfallraten zu addieren, um die gesamte gefahrbringende Ausfallrate von TE zu erhalten.

Dieser zusätzliche Soft-Error-Beitrag wird für den PFH-Anteil infolge CCF nicht berücksichtigt.

ANMERKUNG 1 Das vereinfachte Verfahren zur Abschätzung des PL für Teilsysteme (siehe ISO 13849-1:2023, 6.1.8) ist nicht in der Lage, eine separate gefahrbringende Ausfallrate für den PFH-Anteil infolge CCF zu berücksichtigen. Das alternative Verfahren, das in ISO/TR 13849-3 (derzeit in Vorbereitung) beschrieben wird, ermöglicht eine separate Berücksichtigung.

ANMERKUNG 2 Die Ergänzung von 2 283 Jahren infolge Soft-Errors zur $MTTF_D$ von Block TE ist sehr gering im Vergleich zum Beitrag von dauerhaft auftretenden zufälligen Hardware-Fehlern.

Literaturhinweise

- [1] IEC 61508 (alle Teile), *Functional safety of electrical/electronic/programmable electronic safety-related systems*
- [2] IEC 60204-1:2016 + AMD1:2021, *Safety of machinery — Electrical equipment of machines — Part 1: General requirements*
- [3] ISO 14118:2017, *Safety of machinery — Prevention of unexpected start-up*
- [4] EN 13906-1:2013, *Zylindrische Schraubenfedern aus runden Drähten und Stäben — Berechnung und Konstruktion — Teil 1: Druckfedern*
- [5] ISO 14119:2024, *Safety of machinery — Interlocking devices associated with guards — Principles for design and selection*
- [6] ISO 4126-2:2018, *Safety devices for protection against excessive pressure — Part 2: Bursting disc safety devices*
- [7] ISO 4414:2010, *Pneumatic fluid power — General rules and safety requirements for systems and their components*
- [8] IEC 6094751:2024, *Low-voltage switchgear and controlgear — Part 5-1: Control circuit devices and switching elements — Electromechanical control circuit devices*
- [9] ISO 4079:2020, *Rubber hoses and hose assemblies — Textile-reinforced hydraulic types for oil-based or water-based fluids — Specification*
- [10] ISO 2398:2024, *Rubber hoses, textile-reinforced, for compressed air — Specification*
- [11] ISO 5774:2023, *Plastics hoses — Textile-reinforced types for compressed-air applications — Specification*
- [12] ISO 4413:2010, *Hydraulic fluid power — General rules and safety requirements for systems and their components*
- [13] ISO 4126-1:2013, *Safety devices for protection against excessive pressure — Part 1: Safety valves*
- [14] ISO 5598:2020, *Fluid power systems and components — Vocabulary*
- [15] IEC 60947 (alle Teile), *Low-voltage switchgear and controlgear*
- [16] IEC 61131 (alle Teile), *Programmable controllers*
- [17] IEC 61800 (alle Teile), *Adjustable speed electrical power drive systems*
- [18] IEC 60529:1989+AMD1:1999+AMD2:2013+Cor1:2019, *Degrees of protection provided by enclosures (IP Codes)*
- [19] IEC 61810-3:2015, *Electromechanical elementary relays — Part 3: Relays with forcibly guided (mechanically linked)*
- [20] IEC 60947-4-1:2023, *Low-voltage switchgear and controlgear — Part 4-1: Contactors and motor-starters — Electromechanical contactors and motor-starters*

- [21] IEC 60947-5-1:2024, *Low-voltage switchgear and controlgear — Part 5: Control circuit devices and switching elements — Section one: Electromechanical control circuit devices*
- [22] ISO 13850:2015, *Safety of machinery — Emergency stop function — Principles for design*
- [23] IEC 60947-5-5:1997+AMD1:2005+AMD2:2016, *Low-voltage switchgear and controlgear — Part 5-5: Control circuit devices and switching elements — Electrical emergency stop device with mechanical latching function*
- [24] IEC 60269-1:2024, *Low-voltage fuses — Part 1: General requirements*
- [25] IEC 60947-2:2024, *Low-voltage switchgear and controlgear — Part 2: Circuit-breakers*
- [26] IEC 60947-3:2025, *Low-voltage switchgear and controlgear — Part 3: Switches, disconnectors, switch-disconnectors and fuse-combination units*
- [27] IEC 60947-6-2:2020, *Low-voltage switchgear and controlgear — Part 6-2: Multiple function equipment — Control and protective switching devices (or equipment) (CPS)*
- [28] IEC 60947-4-1:2023, *Low-voltage switchgear and controlgear — Part 4-1: Contactors and motor-starters — Electromechanical contactors and motor-starters*
- [29] IEC 61810-1:2025+AMD1:2019, *Electromechanical elementary relays — Part 1: General and safety requirements*
- [30] IEC 61810-3:2015, *Electromechanical elementary relays — Part 3: Relays with forcibly guided (mechanically linked) contacts*
- [31] IEC 61810-4:2020, *Electromechanical elementary relays — Part 4: General and safety requirements for reed relays*
- [32] IEC 61558 (alle Teile), *Safety of power transformers, power supply units and similar devices*
- [33] IEC 607301:2022, *Automatic electrical controls for household and similar use — Part 1: General requirements*
- [34] IEC 60893-1:2004, *Insulating materials — Industrial rigid laminated sheets based on thermosetting resins for electrical purposes — Part 1: Definitions, designations and general requirements*
- [35] IEC 60664-1:2025, *Insulation coordination for equipment within low-voltage systems — Part 1: Principles, requirements and tests*
- [36] IEC 60947-7-1:2025, *Low-voltage switchgear and controlgear — Part 7-1: Ancillary equipment — Terminal blocks for copper conductors*
- [37] IEC 60947-7-2:2009, *Low-voltage switchgear and controlgear — Part 7-2: Ancillary equipment — Protective conductor terminal blocks for copper conductors*
- [38] IEC 60947-5-3:2013, *Low-voltage switchgear and controlgear — Part 5-3: Control circuit devices and switching elements — Requirements for proximity devices with defined behaviour under fault conditions*
- [39] IEC 61558-1:2017, *Safety of power transformers, power supply units and similar — Part 1: General requirements and tests*
- [40] IEC 61784-3:2021+AMD1:2024, *Industrial communication networks — Profiles — Part 3: Functional safety fieldbuses — General rules and profile definitions*

E DIN EN ISO 13849-2:2026-03
prEN ISO 13849-2:2026 (D)

- [41] IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*
- [42] IEC 61508-2-1, (ED1 under development), *Functional safety of electrical/electronic/ programmable electronic safety-related systems — Part 2-1: Requirements for complex semiconductors*
- [43] IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations*
- [44] IEC 61508-7:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures*
- [45] SN 29500-1:2016, *Failure rates of components, Part 1: Expected values, general*
- [46] SN 29500-2:2010, *Failure rates of components, Part 2: Expected values for integrated circuits*
- [47] JESD22A121.01, *Test Method for Measuring Whisker Growth on Tin and Alloy Surfaces Finishes*
- [48] JESD201, *Environmental Acceptance Requirements for Tin Whisker Susceptibility of Tin and Alloy Surface Finishes*
- [49] JEDEC JESD89A, *Measurement and Reporting of Alpha Particle and Terrestrial Cosmic Ray-Induced Soft Errors in Semiconductor Devices. Arlington, VA 22201-2107. 2012-01*
- [50] Michael Nicolaidis – *Soft Errors in Modern Electronic Systems*, Springer 2011

Contents

Page

Foreword	iv
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Design and validation	1
4.1 General.....	1
4.2 Integration of safety principles and fault exclusions.....	3
Annex A (informative) Validation tools for mechanical systems	6
Annex B (informative) Validation tools for pneumatic systems	12
Annex C (informative) Validation tools for hydraulic systems	26
Annex D (informative) Validation tools for electrical systems	38
Annex ZAA (informative) Relationship between this European Standard and the essential requirements of Directive 2006/42/EC aimed to be covered	56
Annex ZAB (informative) Relationship between this European Standard and the essential requirements of Regulation (EU) 2023/1230 aimed to be covered	57
Bibliography	58

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 199, Safety of machinery.

This third edition cancels and replaces the second edition (ISO 13849-2:2012), which has been technically revised.

The main changes are as follows:

- alignment of Title and Scope;
- former Clause 4 to Clause 12 have been moved to ISO 13849-1:2023;
- new Clause 4 introduces the application of basic and well-tried safety principles, well-tried components, faults and fault exclusions including guidance on typical approaches for fulfilling the principles in a new Table 2;
- new guidance in Table A.3, Table B.3, Table C.3 and Table D.3 for well-tried components;
- new Table D.22 on transmission errors;
- new Annex D.3 on soft errors;
- deletion of Annex E on an example of validation of fault behavior and diagnostic means.

A list of all parts in the ISO 13849 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Annex A, Annex B, Annex C and Annex D, which are informative, are structured according to Table 1.

Table 1 — Structure of Annex A to Annex D of ISO 13849-2

Annex	Technology	List of basic safety principles	List of well-tried safety principles	List of well-tried components	Fault lists and fault exclusions
		Table(s)			
A	Mechanical	A.1	A.2	A.3	A.4, A.5
B	Pneumatic	B.1	B.2	B.3	B.4 to B.19
C	Hydraulic	C.1	C.2	C.3	C.4 to C.13
D	Electrical (includes electronics)	D.1	D.2	D.3	D.4 to D.22

Introduction

The structure of safety standards in the field of machinery is as follows:

- 1) type-A standards (basic safety standards) giving basic concepts, principles for design and general aspects that can be applied to machinery;
- 2) type-B standards (generic safety standards) dealing with one safety aspect or one type of safeguard that can be used across a wide range of machinery:
 - type-B1 standards on particular safety aspects (for example safety distances, surface temperature, noise);
 - type-B2 standards on safeguards (for example two-hand controls, interlocking devices, pressure-sensitive devices, guards);
- 3) type-C standards (machine safety standards) dealing with detailed safety requirements for a particular machine or group of machines.

This document is a type-B standard as stated in ISO 12100:2010.

The requirements of this document can be supplemented or modified by a type-C standard.

For machines which are covered by the scope of a type-C standard, and which have been designed and built according to the requirements of that standard, the requirements of that type-C standard take precedence.

This document provides requirements for the application of basic and well-tried safety principles and conditions for possible fault exclusions.

This document provides guidance for the design and the validation of mechanical, pneumatic, hydraulic, and electrical systems for the safety-related parts of a control system (SRP/CS) in accordance with ISO 13849-1:2023.

Most of the information in this document is based on the assumption that the simplified procedure for estimating the performance level (PL) described in ISO 13849-1:2023, 6.1.8, is used.

Guidance on the general principles for the design (see ISO 12100:2010) of safety-related parts of control systems, regardless of the type of technology used (electrical, hydraulic, pneumatic, mechanical, etc.), is provided in ISO 13849-1. This includes descriptions of some typical safety functions, determination of their required performance levels, and general requirements of categories and performance levels.

Within this document, some of the validation information is general, whereas some is specific to the type of technology used.

The responsible working group (ISO/TC 199/WG 8) developing the ISO 13849 series will develop application examples for ISO 13849-1 and ISO 13849-2 to be considered for publication in (a) separate document(s) in the ISO 13849 series to further support the user.

Safety of machinery — Safety-related parts of control systems —

Part 2: Application of principles for the design and validation

1 Scope

This document provides requirements for the application of basic and well-tried safety principles, information on well-tried components and conditions for possible fault exclusions. This document provides guidance for the design and the validation of mechanical, pneumatic, hydraulic, and electrical systems for the safety-related parts of a control system (SRP/CS) in accordance with ISO 13849-1:2023.

NOTE Additional requirements for programmable electronic systems, including embedded software, are given in ISO 13849-1:2023, Clause 7, and IEC 61508 (all parts).

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

ISO 13849-1:2023, *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 12100 and ISO 13849-1:2023 apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

4 Design and validation

4.1 General

This document supports the design and validation for SRP/CS as specified in ISO 13849-1:2023 in providing additional information on

- basic and well-tried safety principles;
- well-tried components;
- faults and fault exclusions.

E DIN EN ISO 13849-2:2026-03
ISO/DIS 13849-2:2026(en)

Concerning basic and well-trying safety principles, well-trying components and fault exclusions ISO 13849-1:2023 gives requirements on the design (especially in 6.1.3, 6.1.10 and 6.1.11) and validation (Clause 10) of SRP/CS and their subsystems. The focus in ISO 13849-1:2023 is to generally link the requirements for safety principles to the categories (see ISO 13849-1:2023, Table 10) and to give general requirements and guidelines for well-trying components, faults to be considered and possible fault exclusions. Additionally general validation principles as well as requirements and guidelines how to validate SRP/CS and their subsystems are given.

This document supports the design and validation process by specific lists of applicable basic and well-trying safety principles, well-trying components and possible fault exclusions for several technologies.

The lists are based on experience and consensus in the international safety standardisation community and are as detailed as possible on the level of general machinery. For a specific application these lists can be interpreted and adapted based on technical justification to fulfil the general requirements in ISO 13849-1:2023.

The lists form a comprehensive approach that is applicable throughout different individual applications and are non-exhaustive. Any deviations from the lists in this document shall be justified and documented, see 4.2.

For further information, see Table A.1, Table A.2, Table A.3, Table B.1, Table B.2, Table B.3, Table C.1, Table C.2, Table C.3, Table D.1, Table D.2 and Table D.3 in the Annexes.

Table 2 provides guidance on typical approaches for fulfilling the basic and well-trying safety principles.

Table 2 — Typical approaches for fulfilling basic and well-tries safety principles

Design and manufacturing of components [M]	Design of subsystems [D]	Use of the machine [U]
— Fulfill the relevant safety principles for the design and manufacturing of components (e.g., safe position, use of well-tries spring, sufficient positive overlapping in spool valves). — Specify the operating conditions and limits of use for the design and use, e.g., in data sheets and installation and operation instructions.	— Fulfill the relevant safety principles for the integration of components into subsystems (e.g., de-energization principle, pressure limitation). — Adhere to the operating conditions and limits of use of components defined in the installation and operation instructions. — Specify the operating conditions and limits of use of the subsystems in the machine including the resulting conditions from the integrated components (e.g., proper temperature range, sufficient avoidance of contamination of the fluid).	— Adhere to the operating conditions and limits of use of subsystems in the machine, included in the information for use and installation and operation instructions of the machine (e.g., proper temperature range, sufficient avoidance of contamination of the fluid, maintenance plan).

NOTE 1 Several safety principles are relevant from component level up to the use of the machine, e.g., use of suitable materials and adequate manufacturing, correct dimensioning and shaping, proper selection, combination, arrangements, assembly, and installation of components/system. These principles typically are relevant for the design and manufacturing of components (e.g., correct dimensioning of housing), the design and integration of components into subsystems (e.g., correct dimensioning of component parameters with respect to the expected load) and the installation and use of components and subsystems (e.g., correct dimensioning of filters and maintenance intervals).

NOTE 2 For the design and manufacturing of components fulfilment of product standards can be helpful for the confirmation of some basic or well-tries safety principles. In most cases the fulfilment of product standards is necessary to fulfil the basic safety principle proper selection, combination, arrangement, assembly, and installation of components/system.

NOTE 3 The specification of operating conditions and limits of use, e.g., in data sheets and installation and operation instructions, usually show that the safety principles for the construction and design of a component for the specified application are applied. Further information on safety related values of components or parts of control systems can be found in ISO 13849-1:2023, Annex O.

To support design and validation see

- Annex A for mechanical systems;
- Annex B for pneumatic systems;
- Annex C for hydraulic systems;
- Annex D for electrical systems.

4.2 Integration of safety principles and fault exclusions

Applicable basic safety principles shall be applied for all categories.

Applicable well-tries safety principles shall be applied for category 1, 2, 3 and 4.

Any decision that a safety principle is not applicable for technical reasons or based on the risk assessment shall be justified and documented in detail. This is related to the specific application and the industrial sector in which the SRP/CS is intended to be used.

Relevant fault exclusions may be applied (see Tables A.4, A.5, B.4 – B.19, C.4 – C.13, and Clause D.2). These fault exclusions shall be justified and documented (see ISO 13849-1:2023, 6.1.10.3).

E DIN EN ISO 13849-2:2026-03
ISO/DIS 13849-2:2026(en)

An analysis based on the following criteria shall be done to demonstrate which safety principles are required in the specific application:

- Only the safety principles for the relevant technologies and type of design are required.

Example 1 For a pneumatic valve with electronic pilot control,

- Table A.1 and Table A.2 are relevant for the mechanical part;
- Table B.1 and Table B.2 are relevant for the pneumatic part; and
- Table D.1 and Table D.2 are relevant for the electronic part.

Example 2 For an electromechanical limit switch, Table A.1 and Table A.2 are relevant for the mechanical part and Table D.1 and Table D.2 are relevant for the electrical part.

Example 3 The well-tried safety principle “sufficient positive overlap in spool valves” applies to spool or gate valves but not to seat or cartridge valves.

Example 4 The well-tried safety principle “valve closed by load pressure” applies to seat or cartridge valves but not to spool or gate valves.

- Safety principles which are not applicable for technical reasons may be substituted by other safety principles or alternative measures which have the same effect. A well-tried safety principle shall not be replaced by a basic safety principle.

Example 5 When the application of the basic safety principle “Sequential switching for circuit of serial contacts of redundant signals” is not possible for technical reasons, then the well-tried safety principle “limitation of electrical parameters” (realized by overload protection of the contacts, e.g. by using a fuse) may be used as a substitute to avoid welding of both contacts.

The application of safety principles for subsystem elements can be validated in any of the following ways:

- The information for use (e.g. data sheet or application notes) of the subsystem element contains the confirmation that all applicable safety principles relevant for the design and manufacturing of the subsystem element are applied.
- The features specified in the information for use (e.g. data sheet or application notes) for the subsystem element indirectly confirm the application of some safety principles for the subsystem element.

NOTE 1 Normally there is no need to check the validity of these assured features during the integration of the subsystem element.

Example 6 The well-tried safety principle “over-dimensioning/safety factor” can be fulfilled by underrating the maximum load for an electrical output in relation to the specified maximum load. Over-dimensioning of environmental characteristics, e.g. temperature, is usually not required if the subsystem element is not constantly operated on the edge of the environmental characteristics.

When previously validated subsystems are integrated into SRP/CS there is no need to validate again the fulfilment of the internally applied safety principles. Only safety principles which affect the external integration shall be applied and validated.

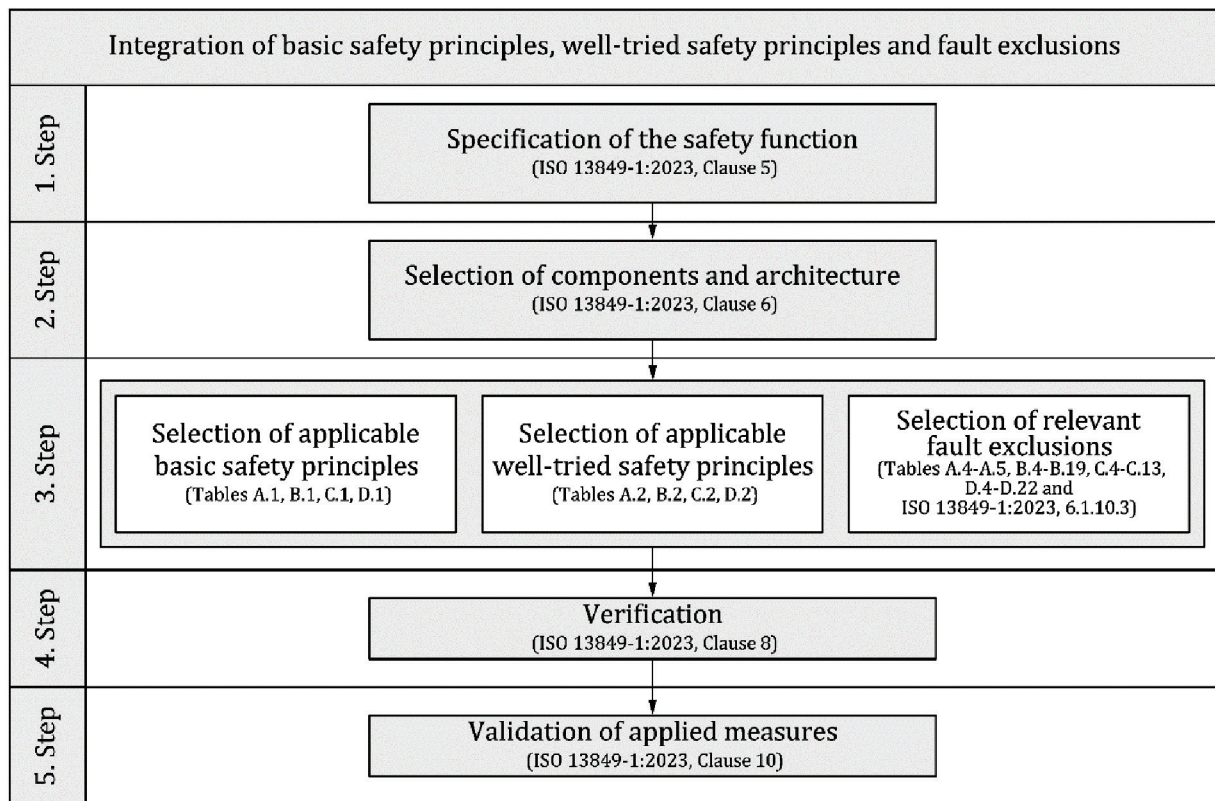
Example 7 The parametrization of inputs of a previously validated safety PLC is validated during the integration.

NOTE 2 A component complying with a type-B2 standard, e.g. ISO 14119:2024, *Safety of machinery - Interlocking devices associated with guards - Principles for design and selection*, usually supports the basic safety principles “use of suitable materials and adequate manufacturing” and “correct dimensioning and shaping”. But for the integration of this component into an SRP/CS several other applicable safety principles are additionally necessary, e.g. “use of de-energization”, “compatibility”, “withstanding environmental conditions” or “secure fixing of input devices”.

NOTE 3 Wording such as “robust”, “simple”, “significant”, “sufficient” and similar terms is intended to emphasize requirements or recommendations and is not quantified by factors or discrete values. Such information is found in product specific standards, e.g. type-C standards, and is not presented in this document. The term “good engineering practice” denotes a method to achieve a reliable SRP/CS through the systematic application of proven techniques, documented procedures, qualified personnel, risk assessment and mitigation, and thorough verification and validation activities.

**E DIN EN ISO 13849-2:2026-03
ISO/DIS 13849-2:2026(en)**

Figure 1 shows the process for integrating the basic and well-trying safety principles as well as the fault exclusions.



NOTE Well-trying safety principles are not mandatory for category B, see ISO 13849-1:2023, Table 10.

Figure 1 — Integration of basic safety principles, well tried safety principles and fault exclusions

Annex A (informative)

Validation tools for mechanical systems

Annex A applies to mechanical systems. It should also be considered when mechanical systems are used in conjunction with other technologies.

Table A.1 and Table A.2 list basic and well-tried safety principles.

The use of components designed according to a product standard can be helpful for the confirmation of some basic or well-tried safety principles (see Table 2, NOTE 2).

The fulfilment of principles can depend on multiple contributors involved in SRP/CS design (see 4.1, Table 2, implemented in column 3 of Table A.1 and Table A.2).

The status of “well-tried” is mainly application specific. Components can be described as “well-tried” if they are in accordance with ISO 13849-1:2023, 6.1.11. A well-tried component for some applications could be inappropriate for other applications. The status of being well-tried does not mean that all faults can be excluded for a well-tried component.

Table A.4 and Table A.5 list fault exclusions and their rationale.

**E DIN EN ISO 13849-2:2026-03
ISO/DIS 13849-2:2026(en)**

Table A.1 — Basic safety principles

Basic safety principle	Remarks	Relevant for (see Table 2)
Use of suitable materials and adequate manufacturing	Selection of material, manufacturing methods and treatment in relation to, e.g. stress, durability, elasticity, friction, wear, corrosion, temperature.	M, D
Correct dimensioning and shaping	Consider, e.g. stress, strain, fatigue, surface roughness, tolerances, sticking, manufacturing.	M, D
Correct selection, combination, arrangements, assembly and installation of components or systems related to the application	Apply the installation and operation instructions provided by the manufacturer, e.g. catalogue sheets, installation instructions, specifications, and use of good engineering practice in similar components or systems.	M, D, U
Use of de-energization principle This principle is not applicable when loss of energy creates a hazard, e.g. release of workpiece caused by loss of clamping or holding force.	The safe state is obtained by a release of energy. See primary action for stopping in ISO 12100:2010, 6.2.11.3. Energy is supplied for starting the movement of a mechanism. See primary action for starting in ISO 12100:2010, 6.2.11.3. Consider different modes, e.g. operation mode, maintenance mode. Time-delay functions may be necessary to achieve a system safe state (see e.g. IEC 60204-1:2016 + AMD1:2021, 9.2.2).	M, D
Correct fastening	For screw locking apply the manufacturer's installation and operation instructions. Fastening in the correct orientation and fastening to the correct torque is considered. Overloading can be avoided and adequate resistance to release can be achieved by applying adequate torque loading technology.	M, D, U
Withstanding environmental conditions (see ISO 13849-1:2023, Clause 10, and follow manufacturer's installation and operation instructions)	Design the equipment so that it can work within the environmental limits of the intended use and in any reasonably foreseeable adverse conditions, e.g. temperature, humidity, vibration, pollution.	M, D, U
Prevention of the ingress of solid foreign objects and fluids	Apply appropriate protection against ingress of solid foreign objects and fluids.	M, D, U
Temperature range	External and internal temperature effects are considered throughout the whole system.	M, D, U
Limitation of speed, acceleration and jerk (to avoid or limit mechanical stress)	Consider, e.g. spring, damping device.	M, D
Reduction of response time	Minimize delay in de-energizing of switching components. Consider, e.g. spring fatigue, friction, lubrication, temperature, inertia during acceleration and deceleration, combination of tolerances.	M, D
Abbreviations M – Design and manufacturing of components D – Design of subsystems U – Use of the machine		

Table A.1 (continued)

Basic safety principle	Remarks	Relevant for (see Table 2)
Protection against unexpected start-up (see ISO 12100:2010, 6.2.11.4, ISO 14118:2017)	Consider unexpected start-up caused by stored energy and after power supply restoration for different modes e.g. operation mode, maintenance mode.	M, D
	Special equipment for release of stored energy can be necessary. Special applications, e.g. to keep energy for clamping devices or ensure a position, need to be considered separately.	M, D, U
Simplification	Avoid unnecessary components in the safety-related system.	M, D
Separation	Separation of safety-related functions from other functions.	M, D
Limitation of the generation and/or transmission of force, torque (e.g. to prevent wear) This principle is not applicable when the continued integrity of components is essential to maintain the necessary level of control.	Examples are break pin, break plate and torque-limiting clutch.	M, D
Lubrication	Consider the need for lubrication devices, information on lubricants and lubrication intervals.	M, D, U
Abbreviations M – Design and manufacturing of components D – Design of subsystems U – Use of the machine		

Table A.2 — Well-trying safety principles

Well-trying safety principle	Remarks	Relevant for (see Table 2)
Use of carefully selected materials and manufacturing	Selection of suitable material, adequate manufacturing methods and treatments related to the application.	M, D
Use of components with oriented failure mode (see ISO 12100:2010, 6.2.12.3)	Use oriented failure mode components or systems wherever practicable. A safe state is directly or indirectly (e.g. through fault detection) obtained by the predominant failure mode.	M, D
Over-dimensioning	De-rate components when used in safety circuits. Safety factors are as given in standards or by good engineering practice in safety-related applications.	M, D
Safe position	The moving part of the component is held in one of the possible positions by mechanical means. Force is needed to change the position, especially to leave a safe position. If the realization is based on the principle of frictional engagement, the frictional force is always greater than the disturbing forces for the entire mission time.	M, D
Increased OFF force	A safe position or state is obtained by an increased OFF force in relation to the ON force.	M, D
Abbreviations M – Design and manufacturing of components D – Design of subsystems U – Use of the machine		

Table A.2 (continued)

Well-tried safety principle	Remarks	Relevant for (see Table 2)
Careful selection of fastening related to the application	Avoid relying only on friction, use e.g. form-fitting connections like positive-locking fastening, material-related connections like glueing/welding/soldering/vulcanizing, locking nuts.	M, D
Positive mechanical action (see ISO 12100:2010, 6.2.5.)	To achieve positive (or direct) mechanical action, mechanical components needed for the safety function are moved either by direct contact or via rigid elements, e.g. a cam directly opens the contacts of an electrical switch rather than relying on a spring.	M, D
Multiple parts	Reducing the effect of faults by providing multiple parts acting in parallel, e.g. where a failure of one of several springs does not lead to a dangerous condition.	M, D
Use of well-tried spring	See Table A.3	M, D
Limited range of force and similar parameters This principle is not applicable when the continued integrity of components is essential to maintaining the necessary level of control.	Determination of the necessary limitation in relation to the experience and application. Examples are break pin, break plate, and torque-limiting clutch.	M, D
Limited range of speed and similar parameters	Determination of the necessary limitation in relation to the experience and application. Examples are centrifugal governor, safe monitoring of speed, and limited displacement.	M, D, U
Limited range of environmental parameters See ISO 13849-1:2023, 10.7	Determination of the necessary limitations. Examples are temperature, humidity, pollution at the installation. Follow manufacturer's installation and operation instructions.	M, D, U
Limited range of reaction time, limited hysteresis	Determination of the necessary limitations. For example, spring fatigue, friction, lubrication, temperature, inertia during acceleration and deceleration, combination of tolerances.	M, D
Abbreviations M – Design and manufacturing of components D – Design of subsystems U – Use of the machine		

Table A.3 — Well-tried components

Well-tried component	Conditions for “well-tried”	Standard or specification
Screw	All factors influencing the screw connection and the application are to be considered. See Table A.2.	Mechanical jointing such as screws, nuts, washers, rivets, pins, bolts, etc. is standardized.
Spring	Well-tried springs are characterized by — use of carefully selected materials, manufacturing methods (e.g. pre-setting and cycling before use) and treatments (e.g. rolling and shot-peening); — sufficient guidance of the spring; and — sufficient safety factor for fatigue stress (i.e. with a high probability that a fracture will not occur, which can be demonstrated by an endurance test of e.g. a valve with the built-in spring or using other ways).	Technical specifications for spring steels and other special applications are given in EN 13906-1:2013.
	Well-tried compression coil springs can also be designed by — use of carefully selected materials, manufacturing methods (e.g. pre-setting and cycling before use) and treatments (e.g. rolling and shot-peening); — sufficient guidance of the spring; — clearance between the turns less than the wire diameter when unloaded; and — sufficient force after a fracture(s) is maintained (i.e. a fracture(s) will not lead to a dangerous condition). NOTE Compression springs are preferred.	
Cam	All factors influencing the cam arrangement (e.g. part of an interlocking device) are to be considered. See Table A.2.	See ISO 14119:2024
Break-pin Rupture disc, Shear pin	All factors influencing the application are to be considered. See Table A.2.	See ISO 4126-2:2018
Plunger	Guiding of the plunger in such a way that clamping/sticking can be excluded. The plunger is dimensioned in such a way that the forces can be transmitted reliably.	

Table A.4 — Faults and fault exclusions — Mechanical devices, components and elements (e.g. cam, follower, chain, clutch, brake, shaft, screw, pin, guide, bearing)

Fault considered	Fault exclusion	Remarks
Wear/corrosion	Yes, in the case of carefully selected material, (over)dimensioning, manufacturing process, treatment and proper lubrication, according to the specified lifetime (see also Table A.2).	See ISO 13849-1:2023, 6.1.10
Untightening/ loosening	Yes, in the case of carefully selected material, manufacturing process, locking means and treatment, according to the specified lifetime (see also Table A.2).	
Fracture	Yes, in the case of carefully selected material, (over)dimensioning, manufacturing process, treatment and proper lubrication, according to the specified lifetime (see also Table A.2).	
Deformation by over-stressing	Yes, in the case of carefully selected material, (over)dimensioning, treatment and manufacturing process, according to specified lifetime (see also Table A.2).	
Stiffness/sticking	Yes, in the case of carefully selected material, (over)dimensioning, manufacturing process, treatment and proper lubrication, according to specified lifetime (see also Table A.2).	

Table A.5 — Faults and fault exclusions — Pressure-coil springs

Fault considered	Fault exclusion	Remarks
Wear/corrosion	Yes, in case of use of well-tried springs and carefully selected fastenings (see Table A.3).	See ISO 13849-1:2023, 6.1.10
Force reduction by setting and fracture		
Fracture		
Stiffness/sticking		
Loosening		
Deformation by overstressing		

Annex B (informative)

Validation tools for pneumatic systems

Annex B applies to pneumatic systems. It should also be considered when pneumatic systems are used in conjunction with other technologies. Where pneumatic components are electrically connected/controlled, the appropriate fault lists in Annex D should be considered.

NOTE Additional requirements can exist in national legislation.

Table B.1 and Table B.2 list basic and well-trying safety principles.

The use of components designed according to a product standard can be helpful for the confirmation of some basic or well-trying safety principles (see Table 2, Note 2).

The fulfilment of principles can depend on multiple contributors (see 4.1, Table 2, implemented in column 3 of Table B.1 and Table B.2).

The status of “well-trying” is mainly application-specific. Components can be described as “well-trying” if they are in accordance with ISO 13849-1:2023, 6.1.11 and ISO 4414:2010, Clause 5 to Clause 7. A well-trying component for some applications could be inappropriate for other applications. The status of being well-trying does not mean that all faults can be excluded for a well-trying component

Table B.4 to Table B.19 list fault exclusions and their rationale.

Table B.1 — Basic safety principles

Basic safety principle	Remarks	Relevant for (see Table 2)
Use of suitable materials and adequate manufacturing	Selection of material, manufacturing methods and treatment in relation to, e.g. stress, durability, elasticity, friction, wear, corrosion, temperature characteristics of compressed air.	M, D
Correct dimensioning and shaping	Consider, e.g. stress, strain, fatigue, surface roughness, tolerances, sticking, manufacturing.	M, D
Correct selection, combination, arrangements, assembly and installation of components or systems related to the application	Apply the installation and operation instructions provided by the manufacturer, e.g. catalogue sheets, installation instructions, specifications, and use of good engineering practice in similar components or systems.	M, D, U
Use of de-energization principle This principle is not applicable when loss of energy creates a hazard, e.g. release of work-piece caused by loss of clamping or holding force.	The safe state is obtained by release of energy to all relevant devices. See primary action for stopping in ISO 12100:2010, 6.2.11.3. Energy is supplied for starting the movement of a mechanism. See primary action for starting in ISO 12100:2010, 6.2.11.3. Consider different modes, e.g. operation mode, maintenance mode. Time-delay functions may be necessary to achieve a system safe state (see e.g. IEC 60204-1:2016 + AMD1:2021, 9.2.2).	M, D
Correct fastening	For fasteners (e.g. screw locking, fittings, gluing or clamp ring) apply the manufacturer's installation and operation instructions. Fastening in the correct orientation and fastening to the correct torque is considered. Overloading can be avoided by applying adequate torque loading technology.	M, D, U
Withstanding environmental conditions (see ISO 13849-1:2023, Clause 10, and follow manufacturer's installation and operation instructions)	Design the equipment so that it can work within the environmental limits of the intended use and in any reasonably foreseeable adverse conditions, e.g. temperature, humidity, vibration, pollution, electromagnetic interference (EMI).	M, D, U
Prevention of the ingress of solid foreign objects and fluids	Apply appropriate protection against ingress of solid foreign objects and fluids.	M, D, U
Temperature range	External and internal temperature effects are considered throughout the whole system. (see ISO 4414:2010)	M, D, U
Limitation of speed, acceleration and jerk (to avoid or limit mechanical stress)	An example is the speed limitation placed on a piston by a flow valve or throttle.	M, D
Reduction of response time	Minimize delay in de-energizing of switching components. Suitable range of switching time, e.g. length of pipework, pressure, exhaust capacity, force, spring fatigue, friction, lubrication, temperature, inertia during acceleration and deceleration, frequencies, shock waves, combination of tolerances.	M, D
Simplification	Avoid unnecessary components in the safety-related system.	M, D
Abbreviations M – Design and manufacturing of components D – Design of subsystems U – Use of the machine		

Table B.1 (continued)

Basic safety principle	Remarks	Relevant for (see Table 2)
Protection against unexpected start-up (see ISO 12100:2010, 6.2.11.4, ISO 14118:2017)	Consider unexpected start-up caused by stored energy and after power supply restoration for different modes, e.g. operation mode, maintenance mode.	M, D
	Special equipment for the release of stored energy can be necessary. Special applications, e.g. to maintain energy for clamping devices or ensure a position, need to be considered separately.	M, D, U
Separation	Separation of the safety-related functions from other functions.	M, D
Pressure limitation (e.g. to prevent wear)	Examples are pressure-relief valve, pressure-reducing/control valve.	M, D
Basic measures against contamination of the fluid	Consider filtration and separation of solid particles and water in the fluid. Prevent contamination of fluid by external sources during installation and handling of components. Consider an indicator for when the filter needs service.	M, D, U
Correct use of pre-lubricated/self-lubricating/life-time lubrication valves	Use prepared oil-free air according to the manufacturer's installation and operation instructions, to prevent dissipation of the grease.	D, U
Abbreviations M – Design and manufacturing of components D – Design of subsystems U – Use of the machine		

Table B.2 — Well-trying safety principles

Well-trying safety principle	Remarks	Relevant for (see Table 2)
Use of components with oriented failure mode (see ISO 12100:2010, 6.2.12.3)	Use oriented failure mode components or systems wherever practicable. A safe state is directly or indirectly (e.g. through fault detection) obtained by the predominant failure mode.	M, D
Over-dimensioning	De-rate components when used in safety circuits, e.g. with respect to pressure level, temperature level, switching frequency. Safety factors are as given in standards or by good engineering practice in safety-related applications.	M, D
Safe position	The moving part of the component is held in one of the possible positions by mechanical means. Force is needed to change the position. If the realization is based on the principle of frictional engagement, the frictional force is always greater than the disturbing forces for the entire mission time.	M, D
Increased OFF force	A safe position or safe state is obtained by an increased OFF force in relation to the ON force. One solution can be that the area ratio for moving a valve spool to the safe position (OFF position) is significantly larger than for moving the spool to ON position.	M, D
Valve closed by load pressure	These are generally, but not exclusively, seat valves, e.g. poppet valves, ball valves. Consider how to apply the load pressure to keep the valve closed even if, e.g. the spring closing the valve breaks. NOTE High closing speeds can cause valve bounce.	M, D
Positive mechanical action (see ISO 12100:2010, 6.2.5.)	The positive mechanical action is used for moving parts inside pneumatic components. To achieve positive (or direct) mechanical action, mechanical components needed for the safety function are moved either by direct contact or via rigid elements.	M, D
Use of well-trying spring	See Table A.3.	M
Limited range of force and similar parameters to avoid or limit mechanical stress This principle is not applicable when the continued integrity of components is essential to maintaining the necessary level of control.	Determination of the necessary limitation in relation to the experience and application. This can be achieved by a well-trying pressure relief valve which is, e.g. equipped with a well-trying spring, correctly dimensioned and selected.	M, D
Limited range of speed and similar parameters	Determination of the necessary limitation in relation to the experience and application. Examples are fixed orifices and fixed throttles to reduce the speed by resistance to a defined fluidic flow.	M, D, U
Limited range of environmental parameters See ISO 13849-1:2023, 10.7	Determination of the necessary limitations. Examples are temperature, humidity, pollution at the installation. Follow manufacturer's installation and operation instructions.	M, D, U
Limited range of reaction time, limited hysteresis	Determination of the necessary limitations. For example, increased friction will increase the hysteresis. A combination of tolerances will also influence the hysteresis.	M, D
Abbreviations M – Design and manufacturing of components D – Design of subsystems U – Use of the machine		

Table B.2 (continued)

Well-tried safety principle	Remarks	Relevant for (see Table 2)
Appropriate range of working conditions	The limitation of working conditions, e.g. pressure range, flow rate and temperature range, is considered.	M, D, U
Enhanced measures against contamination of the fluid	Consideration of the need for a finer filtration and separation of solid particles and water in the fluid.	M, D, U
Sufficient positive overlap in spool valves or piston valves	The positive overlap ensures the stopping function and prevents dangerous movements.	M
Sufficient underlap in spool valves	Exhaust applications in redundant systems.	M
Periodic evaluation of the fluid condition	Apply a high degree of filtration or separation of solid particles, water and contaminants in the fluid and an indication of the need for a filter service. Evaluate the physical conditions of the fluid.	M, D, U
Abbreviations M – Design and manufacturing of components D – Design of subsystems U – Use of the machine		

Table B.3 — Well-tried components

Well-tried component	Conditions for “well-tried”	Standard or specification
Rupture disc	All factors influencing the application are to be considered. See Table B.1 and Table B.2	Technical specifications for bursting disk/flat bursting disk and other special applications are given in ISO 4126-2:2018.
Directional Valve (electrically or remotely actuated or piloted)	Only well-tried if a) the component fulfils the basic and well-tried safety principles with regard to the intended application, including use of the component according to the specification of the manufacturer; b) proven to be widely used in the past with documented successful results in similar applications or made, verified and validated using principles which demonstrate its suitability and reliability for safety-related applications according to relevant product and application standards; c) either no electronics on-board or on-board electronics, if available, does not participate in executing the safety function (see NOTE 3); d) the behavior of the component under all conditions is well defined and can be completely determined; and e) the following construction characteristics are fulfilled: — simple, robust design; — positive connection; — sufficient protection against loosening with detachable connection; — sufficiently robust in relation to the use (application) and the ambient conditions (e.g. pressure fluctuations, vibration); — return force provided by a spring to a safe position; — use of well-tried springs (see Table A.3); and — sufficient tightness in locking direction.	ISO 13849-1:2023, 6.1.3.2.3, 6.1.11
NOTE 1 The confirmation of basic and well-tried safety principles, as well as proof of wide use in the past with documented successful results in similar applications, can be done by the component manufacturer or by the designer of the subsystem. NOTE 2 Examples of directional valves can be valve types with discrete (specific) positions: stop (shut-off) valve, gate valve, AND-valve, shuttle valve, non-return (check) valve, blocking valve, exhaust valve, pressure relief valve. NOTE 3 Digital communication units for valve manifolds or pressure switches are complex and do not fulfil the conditions to be well-tried. If shutting-off the power supply puts the valves into a safe state and if a fault exclusion for cross-circuit connections between the power supply and the control bus (see Annex D) can be made and if for the installed valves the conditions for “well-tried” are fulfilled, the manifold can be considered a well-tried component.		

Table B.3 (continued)

Well-tried component	Conditions for “well-tried”	Standard or specification
Pressure switches	Only well-tried if a) the component fulfils the basic and well-tried safety principles with regard to the intended application, including use of the component according to the specification of the manufacturer; b) proven to be widely used in the past with documented successful results in similar applications or made, verified and validated using principles which demonstrate its suitability and reliability for safety-related applications according to relevant product and application standards; c) either no electronics on-board or on-board electronics, if available, does not participate in executing the safety function; d) the behavior of the component under all conditions is well defined and can be completely determined; and e) the following construction characteristics are fulfilled: — simple, robust design; — positive connection; — sufficient protection against loosening with detachable connection; — sufficiently robust in relation to the use (application) and the ambient conditions (e.g. pressure fluctuations, vibration); and — sufficient dimensioning of the spring.	ISO 13849-1:2023, 6.1.3.2.3, 6.1.11 For the electrical part, see IEC 6094751:2024
NOTE 1 The confirmation of basic and well-tried safety principles, as well as proof of wide use in the past with documented successful results in similar applications, can be done by the component manufacturer or by the designer of the subsystem. NOTE 2 Examples of directional valves can be valve types with discrete (specific) positions: stop (shut-off) valve, gate valve, AND-valve, shuttle valve, non-return (check) valve, blocking valve, exhaust valve, pressure relief valve. NOTE 3 Digital communication units for valve manifolds or pressure switches are complex and do not fulfil the conditions to be well-tried. If shutting-off the power supply puts the valves into a safe state and if a fault exclusion for cross-circuit connections between the power supply and the control bus (see Annex D) can be made and if for the installed valves the conditions for “well-tried” are fulfilled, the manifold can be considered a well-tried component.		

Table B.4 — Faults and fault exclusions — Directional control valves

Fault considered	Fault exclusion	Remarks
Change of switching times	Yes, in the case of positive mechanical action (see Table A.2) of the moving components, as long as the actuating force is sufficiently large.	—
Non-switching (sticking at the end or zero position) or incomplete switching (sticking at a random intermediate position)	Yes, in the case of positive mechanical action (see Table A.2) of the moving components, as long as the actuating force is sufficiently large.	
Spontaneous change of the initial switching position (without an input signal)	Yes, in the case of positive mechanical action (see Table A.2) of the moving components, as long as the holding force is sufficiently large, or if well-tried springs are used (see Table A.3) and normal installation and operating conditions apply (see remark), or in the case of spool valves with elastic sealing and if normal installation and operating conditions apply (see remark).	Normal installation and operating conditions apply when — the conditions laid down by the manufacturer have been considered; — there are no inertia forces acting adversely on moving components (e.g. direction of valve component motion considers magnitude and direction of inertia forces); and — the vibration and shock stresses are smaller than permissible, and no extreme vibration and shock stresses occur.
Leakage	Yes, in the case of spool-type valves with elastic seal, in so far as a sufficient positive overlap is present [see remark 1)], normal conditions of operation apply, and an adequate treatment and filtration of the compressed air is provided; or, in the case of seat valves, if normal conditions of operation apply [see remark 2)], and adequate treatment and filtration of the compressed air is provided.	1) In the case of spool-type valves with elastic seal, the effects due to leakage can usually be excluded. However, a small amount of leakage can occur over a long period of time. 2) Normal conditions of operation apply when the conditions laid down by the manufacturer are considered.
Change in the leakage flow rate over a long period of use	None.	—
Bursting of the valve housing or breakage of the moving component(s) as well as breakage/fracture of the mounting or housing screws	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	
For servo and proportional valves: pneumatic faults which cause uncontrolled behavior	Yes, in the case of servo and proportional directional valves, if these can be assessed in terms of technical safety as conventional directional control valves, owing to their design and construction.	—
NOTE If the control functions are realized by a number of single-function valves, then a fault analysis should be carried out for each valve. The same procedure should be carried out in the case of piloted valves.		

**Table B.5 — Faults and fault exclusions — Stop (shut-off) valves/non-return (check) valves/
quick-action venting valves/shuttle valves, etc.**

Fault considered	Fault exclusion	Remarks
Change of switching times	None.	—
Non-opening, incomplete opening, non-closure or incomplete closure (sticking at an end position or at an arbitrary intermediate position)	Yes, if the guidance system for the moving component(s) is designed in a manner similar to that for a non-controlled ball seat valve without a damping system (see remark) and if well-tried springs are used (see Table A.3).	For a non-controlled ball seat valve without a damping system, the guidance system is generally designed such that any sticking of the moving component is unlikely.
Spontaneous change of the initial switching position (without an input signal)	Yes, for normal installation and operating conditions (see remark) and if there is sufficient closing force on the basis of the pressures and areas provided.	Normal installation and operating conditions are met when — the conditions laid down by the manufacturer are being followed; — no special inertial forces affect the moving components, e.g. direction of motion considers the orientation of the moving machine parts; and — the vibration and shock stresses are smaller than permissible, and no extreme vibration or shock stresses occur.
For shuttle valves: simultaneous closing of both input connections	Yes, if simultaneous closing is unlikely, based on the construction and design of the moving component.	—
Leakage	Yes, if normal conditions of operation apply (see remark) and there is adequate treatment and filtration of the compressed air.	Normal conditions of operation apply when the conditions laid down by the manufacturer are considered.
Change in the leakage flow rate over a long period of use	None.	—
Bursting of the valve housing or breakage of the moving component(s) as well as breakage/fracture of the mounting or housing screws	Yes, if construction, dimensioning and installation are in accordance with good engineering practice and following the valve manufacturer's specifications.	

Table B.6 — Faults and fault exclusions — Flow valves

Fault considered	Fault exclusion	Remarks
Change in flow rate without any change in setting device	Yes, for flow control valves containing components of metal without moving parts [see remark 1)], e.g. throttle valves, if normal operating conditions apply [see remark 2)], and adequate treatment and filtration of the compressed air is provided.	1) The setting device is not considered to be a moving part. Changes in flow rate due to changes in pressure differences are physically limited in this type of valve and are not covered by this assumed fault. 2) Normal operating conditions apply when the conditions laid down by the manufacturer are considered.
Change in the flow rate in the case of non-adjustable, circular orifices and nozzles	Yes, if the diameter is $\geq 0,8$ mm, normal operating conditions apply [see remark 2)], and if adequate treatment and filtration of the compressed air is provided.	
For proportional flow valves: change in the flow rate due to an unintended change in the set value	None.	—
Spontaneous change in the setting device	Yes, where there is an effective protection of the setting device adapted to the particular case, based upon technical safety specification(s).	
Unintended loosening (unscrewing) of the operating element(s) of the setting device	Yes, if an effective positive locking device against loosening (unscrewing) is provided.	
Bursting of the valve housing or breakage of the moving component(s) as well as the breakage/fracture of the mounting or housing screws	Yes, if construction, dimensioning and installation are in accordance with good engineering practice and following the valve manufacturer's specifications.	

Table B.7 — Faults and fault exclusions — Pressure valves

Fault considered	Fault exclusion	Remarks
Non-opening or insufficient opening when exceeding the set pressure (sticking or sluggish movement of the moving component) [see remark 1)]	Yes, if — the guidance system for the moving component(s) is similar to the case of a non-controlled ball seat or membrane valve [see remark 2)], e.g. for a pressure-reducing valve with secondary pressure relief; and — the installed springs are well-tried springs (see Table A.3).	1) This fault applies only when the pressure valve(s) is used for forced actions, e.g. clamping. This fault does not apply to its normal function in the pneumatic systems, e.g. pressure limitation, pressure decrease. 2) For a non-controlled ball seat valve or for a membrane valve, the guidance system is generally designed such that any sticking of the moving component is unlikely.
Non-closing or insufficient closing if pressure drops below the set value (sticking or sluggish movement of the moving component) [see remark 1)]		
Change of the pressure control behavior without changing the setting device [see remark 1)]	Yes, for directly actuated pressure-limiting valves and pressure-switching valves if the installed spring(s) are well-tried (see Table A.3).	
For proportional pressure valves: change in the pressure control behavior due to unintended change in the set value [see remark 1)]	None.	
Spontaneous change in the setting device	Yes, where there is effective protection of the setting device within the requirements of the application, e.g. lead seals.	—

Table B.7 (continued)

Fault considered	Fault exclusion	Remarks
Unintended unscrewing of the operating element of the setting device	Yes, if an effective positive locking device against unscrewing is provided.	
Leakage	Yes, for seat valves, membrane valves and spool valves with elastic sealing in normal operating conditions (see remark) and if adequate treatment and filtration of the compressed air is provided.	Normal operating conditions are met when the conditions laid down by the manufacturer are followed.
Change of the leakage flow rate, over a long period of use	None.	—
Bursting of the valve housing or breakage of the moving component(s) as well as breakage/fracture of the mounting or housing screws	Yes, if construction, dimensioning and installation are in accordance with good engineering practice and following the valve manufacturer's specifications.	

Table B.8 — Faults and fault exclusions — Piping

Fault considered	Fault exclusion	Remarks
Bursting and leakage	Yes, if the dimensioning, choice of materials and fixing are in accordance with good engineering practice (see remark) e.g. installation avoiding accumulation of water, regular draining.	When using plastic pipes, it is necessary to consider the manufacturer's data, in particular with respect to operational environmental influences, e.g. thermal influences, chemical influences or influences due to radiation. When using steel pipes that have not been treated with a corrosion-resistant medium, it is particularly important to provide sufficient drying of the compressed air. Consideration of the environmental dew point is also essential.
Failure at the connector (e.g. tearing off, leakage)	Yes, if using bite-type fittings or threaded pipes (i.e. steel fittings, steel pipes) and if dimensioning, choice of materials, manufacture, configuration and fixing are in accordance with good engineering practice.	—
Clogging (blockage)	Yes, for pipework in the power circuit. Yes, for the control and measurement pipework if the nominal diameter is ≥ 2 mm.	
Kinking of plastic pipes with a small nominal diameter	Yes, if properly protected and installed, considering the relevant manufacturer's data, e.g. minimum bending radius.	

**E DIN EN ISO 13849-2:2026-03
ISO/DIS 13849-2:2026(en)**

Table B.9 — Faults and fault exclusions — Hose assemblies

Fault considered	Fault exclusion	Remarks
Bursting, tearing off at the fitting attachment and leakage	Yes, if hose assemblies use hoses manufactured in accordance with ISO 4079:2020, ISO 2398:2024, ISO 5774:2023 or similar hoses (see remark) with the corresponding hose fittings. NOTE: ISO 4414:2010 does not include criteria regarding the manufacturing specifications of rubber hoses and hose assemblies.	Fault exclusion is not considered when — the intended lifetime is expired; — fatigue behavior of reinforcement can occur; or — external damage is unavoidable.
Clogging (blockage)	Yes, for hose assemblies in the power circuit, and, in the case of the control and measurement hose assemblies, if the nominal diameter is ≥ 2 mm.	—

Table B.10 — Faults and fault exclusions — Connectors

Fault considered	Fault exclusion	Remarks
Bursting, breaking of screws or stripping of threads	Yes, if dimensioning, choice of material, manufacture, configuration and connection to the piping and/or to the pipe/hose fittings are in accordance with good engineering practice.	—
Leakage (loss of airtightness)	None.	Due to wear, ageing, deterioration of elasticity, etc. it is not possible to exclude faults over a long period.
Leakage (sudden major change of airtightness)	Yes, if measures to reduce the risk of leakage are applied that could lead to the loss of the intended component function. Measures can include but are not limited to: — robust connection methods, i.e. compression fittings or appropriately rated push-lock fittings (see remarks 1 to 3); — robust hoses, tubing and fittings; — robust materials that are appropriate for the intended environment.	1) If leakage (sudden major change of airtightness) can lead to a dangerous movement, particularly on gravity-loaded (e.g. vertical) axes, a fault exclusion is not recommended. A fault exclusion on this type of application is only possible with risk estimation and additional measures. 2) Tubing push-to-connect fittings, also known as push-in fittings or push-fit fittings, are considered as appropriately rated push-lock fittings if over-dimensioning and installation and operation instructions provided by the manufacturer are adhered to, notably the push-to-connect fitting matches the tube type being used. 3) Hose push-lock fittings, e.g. featuring a barbed-end that is inserted into the hose, are considered as appropriately rated push-lock fittings only if high-pressure hose clamps are used.
Clogging (blockage)	Yes, for applications in the power circuit and, in the case of control and measurement connectors, if the nominal diameter is ≥ 2 mm.	—

Table B.11 — Faults and fault exclusions — Pressure transmitters and pressure medium transducers

Fault considered	Fault exclusion	Remarks
Loss or change of air/oil-tightness of pressure chambers	None.	—
Bursting of the pressure chambers as well as fracture of the attachment or cover screws	Yes, if dimensioning, choice of material, configuration and attachment are in accordance with good engineering practice.	
Too high output pressure caused by too high inlet pressure	Yes, if an internal pressure relief valve in the inlet circuit is used.	
Change of the ratio inlet pressure to output pressure	Yes, if the pressure ratio is fixed, e.g. by the design of the piston active areas and other internal measures.	
NOTE Pressure transmitters and pressure medium transducers are devices to e.g. limit the output pressure or achieve a fixed ratio of inlet pressure to output pressure.		

Table B.12 — Faults and fault exclusions — Compressed air treatment — Filters

Fault considered	Fault exclusion	Remarks
Blockage of the filter element	None.	—
Rupture or partial rupture of the filter element	Yes, if the filter element is sufficiently resistant to pressure.	
Failure of the filter condition indicator or monitor	None.	
Bursting of the filter housing or fracture of the cover or connecting elements	Yes, if dimensioning, choice of material, arrangement in the system and fixing are in accordance with good engineering practice.	

Table B.13 — Faults and fault exclusions — Compressed-air treatment — Oilers

Fault considered	Fault exclusion	Remarks
Change in the set value (oil volume per unit time) without change to the setting device	None.	—
Spontaneous change in the setting device	Yes, if effective protection of the setting device is provided, adapted to the particular case.	
Unintended unscrewing of the operating element of the setting device	Yes, if an effective positive locking device against unscrewing is provided.	
Bursting of the housing or fracture of the cover, fixing or connecting elements.	Yes, if the dimensioning, choice of materials, arrangement in the system and fixing are in accordance with good engineering practice.	

Table B.14 — Faults and fault exclusions — Compressed air treatment — Silencers

Fault considered	Fault exclusion	Remarks
Blockage (clogging) of the silencer	Yes, if the design and construction of the silencer element fulfils the remark.	Clogging of the silencer element and/or an increase in the exhaust air back-pressure above a certain critical value is unlikely if the silencer has a suitably large diameter and is designed to meet the operating conditions.

Table B.15 — Faults and fault exclusions — Accumulators and pressure vessels

Fault considered	Fault exclusion	Remarks
Fracture/bursting of the accumulator/pressure vessel or connectors or stripping of the threads of the fixing screws	Yes, if construction, choice of equipment, choice of materials and arrangement in the system are in accordance with good engineering practice.	—

**E DIN EN ISO 13849-2:2026-03
ISO/DIS 13849-2:2026(en)**

Table B.16 — Faults and fault exclusions — Sensors

Fault considered	Fault exclusion	Remarks
Faulty sensor (see remark)	None.	—
Change of the detection or output characteristics	None.	
NOTE Sensors in this table are devices for signal capture, processing and output, in particular for, e.g. pressure, flow, temperature.		

Table B.17 — Faults and fault exclusions — Information processing — Logical elements

Fault considered	Fault exclusion	Remarks
Faulty logical element (e.g. AND element, OR element, logic-storage-element) due to, e.g. change in the switching time, failing to switch or incomplete switching	For corresponding fault assumptions and fault exclusions, see Tables B.4, B.5 and B.6 and the relevant related components.	—

Table B.18 — Faults and fault exclusions — Information processing — Time-delay devices

Fault considered	Fault exclusion	Remarks
Faulty time-delay device, e.g. pneumatic and pneumatic/mechanical time and counting elements	Yes, for time-delay devices without moving components, e.g. fixed resistance, if normal operating conditions apply and adequate treatment and filtration of the compressed air is provided.	—
Change of detection or output characteristics		
Bursting of the housing or fracture of the cover or fixing elements	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	—

Table B.19 — Faults and fault exclusions — Information processing — Converters

Fault considered	Fault exclusion	Remarks
Faulty converter (see remark)	Yes, for converters without moving components, e.g. reflex nozzle, if normal operating conditions apply and adequate treatment and filtration of the compressed air is provided.	—
Change of the detection or output characteristics		
Bursting of the housing or fracture of the cover or fixing elements	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	
NOTE Converters in this table are devices to e.g. detect that a position is reached or switch between binary states (position reached/not reached, pressure on/off). They are also used to amplify pneumatic signals.		

Annex C (informative)

Validation tools for hydraulic systems

Annex C applies to hydraulic systems. It should also be considered when hydraulic systems are used in conjunction with other technologies. Where hydraulic components are electrically connected/controlled, the appropriate fault lists in Annex D should be considered.

NOTE Additional requirements can exist in national legislation.

Table C.1 and Table C.2 list basic and well-trying safety principles.

The use of components designed according to a product standard can be helpful for the confirmation of some basic or well-trying safety principles (see Table 2, Note 2). The fulfilment of principles can depend on multiple contributors (see 4.1, Table 2, implemented in column 3 of Table C.1 and Table C.2).

The status of “well-trying” is mainly application-specific. Components can be described as “well-trying” if they are in accordance with ISO 13849-1:2023, 6.1.11 and ISO 4413:2010, Clause 5 to Clause 7. A well-trying component for some applications could be inappropriate for other applications. The status of being well-trying does not mean that all faults can be excluded for a well-trying component

Table C.4 to Table C.13 list fault exclusions and their rationale.

Table C.1 — Basic safety principles

Basic safety principle	Remarks	Relevant for (see Table 2)
Use of suitable materials and adequate manufacturing	Selection of material, manufacturing methods and treatment in relation to e.g. stress, durability, elasticity, friction, wear, corrosion, temperature, characteristics of hydraulic fluid.	M, D
Correct dimensioning and shaping	Consider, e.g. stress, strain, fatigue, surface roughness, tolerances, manufacturing.	M, D
Correct selection, combination, arrangements, assembly and installation of components or systems related to the application	Apply the installation and operation instructions provided by the manufacturer, e.g. catalogue sheets, installation instructions, specifications, and use of good engineering practice in similar components or systems.	M, D, U
Use of de-energization principle This principle is not applicable when loss of energy creates a hazard, e.g. release of workpiece caused by loss of clamping or holding force.	The safe state is obtained by release of energy to all relevant devices. See primary action for stopping in ISO 12100:2010, 6.2.11.3. Energy is supplied for starting the movement of a mechanism. See primary action for starting in ISO 12100:2010, 6.2.11.3. Consider different modes, e.g. operation mode, maintenance mode. Time-delay functions may be necessary to achieve a system safe state (see e.g. IEC 60204-1:2016 + AMD1:2021, 9.2.2).	M, D
Correct fastening	For fasteners (e.g. screw locking, fittings, gluing, clamp ring) apply the manufacturer's installation and operation instructions. Fastening in the correct orientation and fastening to the correct torque is considered. Overloading can be avoided by applying adequate torque loading technology.	M, D, U
Withstanding environmental conditions (see ISO 13849-1:2023, Clause 10, and follow manufacturer's installation and operation instructions)	Design the equipment so that it can work within the environmental limits of the intended use and in any reasonably foreseeable adverse conditions, e.g. temperature, humidity, vibration, pollution, electromagnetic interference (EMI).	M, D, U
Prevention of the ingress of solid foreign objects and fluids	Apply appropriate protection against ingress of solid foreign objects and fluids.	M, D, U
Temperature range	External and internal temperature effects are considered throughout the whole system. (See ISO 4413:2010)	M, D, U
Limitation of speed, acceleration and jerk (to avoid or limit mechanical stress)	An example is the speed limitation of a piston by a flow valve or a throttle.	M, D
Reduction of response time	Minimize delay in de-energizing of switching components. Suitable range of switching time, e.g. length of pipework, pressure, evacuation relief capacity, spring fatigue, friction, lubrication, temperature, viscosity, inertia during acceleration and deceleration, frequencies, shock waves, combination of tolerances.	M, D
Protection against unexpected start-up (see ISO 12100:2010, 6.2.11.4, ISO 14118:2017)	Consider unexpected start-up caused by stored energy and after power supply restoration for different modes, e.g. operation mode, maintenance mode.	M, D
	Special equipment for release of stored energy can be necessary. Special applications, e.g. to maintain energy for clamping devices or ensure a position, need to be considered separately.	M, D, U
Abbreviations M – Design and manufacturing of components D – Design of subsystems U – Use of the machine		

Table C.1 (continued)

Basic safety principle	Remarks	Relevant for (see Table 2)
Simplification	Avoid unnecessary components in the safety-related system.	M, D
Separation	Separation of safety-related functions from other functions.	M, D
Pressure limitation (e.g. to prevent wear)	Examples are pressure-relief valve, pressure-reducing/control valve.	M, D
Basic measures against contamination of the fluid	Consider filtration of solid particles and separation of water and gas from the fluid. Prevent contamination of fluid by external sources during installation and handling of components. Consider an indicator for when the filter needs service.	M, D, U
Correct fluid handling	Air bubbles and restrictions in the hydraulic fluid are avoided because they can create cavitation which can cause additional hazards, e.g. unintended movements.	M, D, U
Abbreviations M – Design and manufacturing of components D – Design of subsystems U – Use of the machine		

Table C.2 — Well-trying safety principles

Well-trying safety principle	Remarks	Relevant for (see Table 2)
Use of components with oriented failure mode (see ISO 12100:2010, 6.2.12.3)	Use oriented failure mode components or systems wherever practicable. A safe state is directly or indirectly (e.g. through fault detection) obtained by the predominant failure mode.	M, D
Over-dimensioning	De-rate components when used in safety circuits. Safety factors are as given in standards or by good engineering practice in safety-related applications.	M, D
Safe position	The moving part of the component is held in one of the possible positions by mechanical means. Force is needed to change the position, especially to leave a safe position.	M, D
Increased OFF force	A safe position or safe state is obtained by an increased OFF force in relation to the ON force. One solution can be that the area ratio for moving a valve spool to the safe position (OFF position) is significantly larger than for moving the spool to the ON position (a safety factor).	M, D
Valve closed by load pressure	Examples are seat and cartridge valves. Consider how to apply the load pressure to keep the valve closed even if, e.g. the spring closing the valve breaks.	M, D
Positive mechanical action (See ISO 12100:2010, 6.2.5.)	The positive mechanical action is used for moving parts inside hydraulic components. To achieve positive (or direct) mechanical action, mechanical components needed for the safety function are moved either by direct contact or via rigid elements.	M, D
Use of well-trying spring	See Table A.3.	M
Abbreviations M – Design and manufacturing of components D – Design of subsystems U – Use of the machine		

Table C.2 (continued)

Well-tried safety principle	Remarks	Relevant for (see Table 2)
Limited range of force and similar parameters to avoid or limit mechanical stress This principle is not applicable when the continued integrity of components is essential to maintaining the necessary level of control.	Determination of the necessary limitation in relation to the experience and application. This can be achieved by a well-tried pressure-relief valve which is, e.g. equipped with a well-tried spring, correctly dimensioned and selected.	M, D
Limited range of speed and similar parameters	Determination of the necessary limitation in relation to the experience and application. Examples are fixed orifices and fixed throttles to reduce the speed by resistance to a defined fluidic flow.	M, D, U
Limited range of environmental parameters See ISO 13849-1:2023, 10.7	Determination of the necessary limitations. Examples are temperature, humidity, pollution at the installation. Follow manufacturer's installation and operation instructions.	M, D, U
Limited range of reaction time, limited hysteresis	Determination of the necessary limitations. For example, increased friction will increase the hysteresis. A combination of tolerances will also influence the hysteresis.	M, D
Appropriate range of working conditions	The limitation of working conditions, e.g. pressure range, flow rate and temperature range, is considered.	M, D, U
Enhanced measures against contamination of the fluid	Consideration of the need for a finer filtration and separation of solid particles and water in the fluid.	M, D, U
Sufficient positive overlapping in spool valves or piston valves	The positive overlapping ensures the stopping function and prevents dangerous movements.	M
Periodic evaluation of the fluid condition	Apply a high degree of filtration or separation of solid particles, water and contaminants in the fluid and an indication of the need for a filter service. Evaluate the physical and chemical conditions of the fluid.	M, D, U
Abbreviations M – Design and manufacturing of components D – Design of subsystems U – Use of the machine		

Table C.3 — Well-tried components

Well-tried component	Conditions for “well-tried”	Standard or specification
Pressure relief valve (spring loaded)	All factors influencing the application are to be considered. See Table C.2.	Technical specifications for bursting disk/flat bursting disk and other special applications are given in ISO 4126-1:2013.
Directional Valve (electrically or remotely actuated or piloted)	Only well-tried if a) the component fulfils the basic and well-tried safety principles with regard to the intended application, including use of the component according to the specification of the manufacturer; b) proven to be widely used in the past with documented successful results in similar applications or made, verified and validated using principles which demonstrate its suitability and reliability for safety-related applications according to relevant product and application standards; c) either no electronics on-board or on-board electronics, if available, does not participate in executing the safety function (see NOTE 3); d) the behavior of the component under all conditions is well defined and can be completely determined; and e) the following construction characteristics are fulfilled: — simple, robust design; — positive connection; — sufficient protection against loosening with detachable connection; — sufficiently robust in relation to the use (application) and the ambient conditions (e.g. pressure fluctuations, vibration); — return force provided by a spring to a safe position; — use of well-tried springs, see Table A.3; and — sufficient tightness in locking direction.	ISO 13849-1:2023, 6.1.3.2.3, 6.1.11
NOTE 1 The confirmation of basic and well-tried safety principles as well as proof of wide use in the past with documented successful results in similar applications can be done by the component manufacturer or by the designer of the subsystem. NOTE 2 Examples of directional valves can be valve types with discrete (specific) positions: stop (shut-off) valve, gate valve, AND-valve, shuttle valve, non-return (check) valve, blocking valve, exhaust valve, pressure relief valve. NOTE 3 Digital communication units for valve manifolds or pressure switches are complex and do not fulfil the conditions to be well-tried. If shutting-off the energy supply puts the valves into a safe state and if a fault exclusion for cross-circuit connections between the power supply and the control bus (see Annex D) can be made and if for the installed valves the conditions for “well-tried” are fulfilled, the manifold can be considered a well-tried component.		

Table C.3 (continued)

Well-trying component	Conditions for “well-trying”	Standard or specification
Pressure switches	Only well-trying if a) the component fulfils the basic and well-trying safety principles with regard to the intended application, including use of the component according to the specification of the manufacturer; b) proven to be widely used in the past with documented successful results in similar applications or made, verified and validated using principles which demonstrate its suitability and reliability for safety-related applications according to relevant product and application standards; c) either no electronics on-board or on-board electronics, if available, does not participate in executing the safety function; d) the behavior of the component under all conditions is well defined and can be completely determined; and e) the following construction characteristics are fulfilled: — simple, robust design; — positive connection; — sufficient protection against loosening with detachable connection; — sufficiently robust in relation to the use (application) and the ambient conditions (e.g. pressure fluctuations, vibration); and — sufficient dimensioning of the spring.	ISO 13849-1:2023, 6.1.3.2.3, 6.1.11 For the electrical part, see IEC 6094751:2024
NOTE 1 The confirmation of basic and well-trying safety principles as well as proof of wide use in the past with documented successful results in similar applications can be done by the component manufacturer or by the designer of the subsystem. NOTE 2 Examples of directional valves can be valve types with discrete (specific) positions: stop (shut-off) valve, gate valve, AND-valve, shuttle valve, non-return (check) valve, blocking valve, exhaust valve, pressure relief valve. NOTE 3 Digital communication units for valve manifolds or pressure switches are complex and do not fulfil the conditions to be well-trying. If shutting-off the energy supply puts the valves into a safe state and if a fault exclusion for cross-circuit connections between the power supply and the control bus (see Annex D) can be made and if for the installed valves the conditions for “well-trying” are fulfilled, the manifold can be considered a well-trying component.		

Table C.4 — Faults and fault exclusions — Directional control valves

Fault considered	Fault exclusion	Remarks
Change of switching times	Yes, in the case of positive mechanical action (see Table A.2) of the moving components as long as the actuating force is sufficiently large; or, in respect of the non-opening of a special type of cartridge seat valve, when used with at least one other valve, to control the main flow of the fluid [see remark 1)].	1) A special type of cartridge seat valve is obtained if - the active area for initiating the safety-related switching movement is at least 90 % of the total area of the moving component (poppet); - the effective control pressure on the active area can be increased up to the maximum working pressure (in accordance with ISO 5598:2020, 3.2.429) in line with the behavior of the seat valve in question; - the effective control pressure on the area opposite the active area of the moving component is vented to a very low value compared with the maximum operating pressure, e.g. return pressure in case of pressure dump valves or supply pressure in case of suction/fill valves; - the moving component (poppet) is provided with peripheral balancing grooves; and - the pilot valve(s) to this seat valve is designed together in a manifold block (i.e. without hose assemblies and pipes for the connection of these valves).
Non-switching (sticking at an end or zero position) or incomplete switching (sticking at a random intermediate position)	Yes, in the case of positive mechanical action (see Table A.2) of the moving components if the actuating force is sufficiently large; or, in respect of the non-opening of a special type of cartridge seat valve, when used with at least one other valve, to control the main flow of the fluid [see remark 1)].	
Spontaneous change of the initial switching position (without an input signal)	Yes, in the case of positive mechanical action (see Table A.2) of the moving components as long as the holding force is sufficiently large; or if well-trying springs are used (see Table A.3) and normal installation and operating conditions apply [see remark 2)]; or, in respect of the non-opening of a special type of cartridge seat valve, when used with at least one other valve, to control the main flow of the fluid [see remark 1)] and if normal installation and operating conditions apply [see remark 2)].	2) Normal installation and operating conditions apply when - the conditions laid down by the manufacturer are taken into account; - the weight of the moving component does not act in an unfavorable sense in terms of safety, e.g. horizontal installation; - no special inertial forces affect the moving components, e.g. direction of motion considers the orientation of the moving machine parts; and - no extreme vibration and shock stresses occur.
Leakage	Yes, in the case of seat valves, if normal installation and operating conditions apply (see remark) and an adequate filtration system is provided.	Normal installation and operating conditions apply when the conditions laid down by the manufacturer are considered.
NOTE If the control functions are realized by several single-function valves, then a fault analysis should be carried out for each valve. The same procedure should be carried out in the case of piloted valves.		

Table C.4 (continued)

Fault considered	Fault exclusion	Remarks
Change in the leakage flow rate over a long period of use	None.	—
Bursting of the valve housing or breakage of the moving component(s) as well as breakage/fracture of the mounting or housing screws	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	
For servo and proportional valves: hydraulic faults which cause uncontrolled behavior	Yes, in the case of servo and proportional directional valves, if these can be assessed in terms of safety as conventional directional control valves, owing to their design and construction.	
NOTE If the control functions are realized by several single-function valves, then a fault analysis should be carried out for each valve. The same procedure should be carried out in the case of piloted valves.		

Table C.5 — Faults and fault exclusions — Stop (shut-off) valves/non-return (check) valves/shuttle valves, etc.

Fault considered	Fault exclusion	Remarks
Change of switching times	None.	—
Non-opening, incomplete opening, non-closure or incomplete closure (sticking at an end position or at an arbitrary intermediate position)	Yes, if the guidance system for the moving component(s) is designed in a manner similar to that for a non-controlled ball seat valve without a damping system (see remark) and if well-tries springs are used (see Table A.3).	For a non-controlled ball seat valve without damping system, the guidance system is generally designed in such a manner that any sticking of the moving component is unlikely.
Spontaneous change of the initial switching position (without an input signal)	Yes, for normal installation and operating conditions (see remark) and if there is sufficient closing force based on the pressures and areas provided.	Normal installation and operating conditions are met when — the conditions laid down by the manufacturer are followed; — no special inertial forces affect the moving components, e.g. direction of motion considers the orientation of the moving machine parts; and — no extreme vibration or shock stresses occur.
For shuttle valves: simultaneous closing of both input connections	Yes, if this simultaneous closing is unlikely, based on the construction and design of the moving component.	—
Leakage	Yes, if normal conditions of operation apply (see remark) and an adequate filtration system is provided.	Normal conditions of operation apply when the conditions laid down by the manufacturer are considered.
Change in the leakage flow rate over a long period of use	None.	—
Bursting of the valve housing or breakage of the moving component(s) as well as breakage/fracture of the mounting or housing screws	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	

Table C.6 — Faults and fault exclusions — Flow valves

Fault considered	Fault exclusion	Remarks
Change in the flow rate without change in the setting device	Yes, in the case of flow valves without moving parts [see remark 1)], e.g. throttle valves, if normal operating conditions apply [see remark 2)] and an adequate filtration system is provided [see remark 3)].	1) The setting device is not considered to be a moving part. Changes in flow rate due to changes in the pressure differences and viscosity are physically limited in this type of valve and are not covered by this assumed fault.
Change in the flow rate in the case of non-adjustable, circular orifices and nozzles	Yes, if the diameter is $\geq 0,8$ mm, normal operating conditions apply [see remark 2)] and an adequate filtration system is provided.	2) Normal operating conditions are met when the conditions laid down by the manufacturer are followed. 3) Where a non-return valve is integrated into the flow valve, then, in addition, the fault assumptions for non-return valves have to be considered.
For proportional flow valves: change in the flow rate due to an unintended change in the set value	None.	—
Spontaneous change in the setting device	Yes, where there is an effective protection of the setting device adapted to the particular case, based upon technical safety specification(s).	
Unintended loosening (unscrewing) of the operating element(s) of the setting device	Yes, if an effective positive locking device against loosening (unscrewing) is provided.	
Bursting of the valve housing or breakage of the moving component(s) as well as the breakage/fracture of the mounting or housing screws	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	

Table C.7 — Faults and fault exclusions — Pressure valves

Fault considered	Fault exclusion	Remarks
Non-opening or insufficient opening (spatially and temporarily) when exceeding the set pressure (sticking or sluggish movement of the moving component) [see remark 1)]	Yes, in respect of the non-opening of a special type of cartridge seat valve, when used with at least one other valve, to control the main flow of the fluid [see remark 1) of Table C.4]; or if the guidance system for the moving component(s) is similar to the case of a non-controlled ball seat valve without a damping device [see remark 2)] and if the installed springs are well-ried (see Table A.3).	1) This fault applies only when the pressure valve(s) is (are) used for forced actions, e.g. clamping, and for the control of hazardous movement, e.g. suspension of loads. This fault does not apply to its normal function in hydraulic systems, e.g. pressure limitation, pressure decrease. 2) For a non-controlled ball seat valve without a damping device, the guidance system is generally designed in such a manner that any sticking of the moving component is unlikely.
Non-closing or insufficient closing (spatially and temporarily) if the pressure drops below the set value (sticking or sluggish movement of the moving component) [see remark 1)]		
Change of the pressure control behaviour without changing the setting device [see remark 1)]	Yes, in the case of directly actuated pressure-relief valves, if the installed spring(s) are well- tried (see Table A.3).	—
For proportional pressure valves: change in the pressure control behaviour due to unintended change in the set value [see remark 1)]	None.	
Spontaneous change in the setting device	Yes, where there is an effective protection of the setting device adapted to the particular case in relation to technical safety specifications (e.g. lead seals).	
Unintended unscrewing of the operating element of the setting device	Yes, if an effective positive locking device against unscrewing is provided.	Normal operating conditions apply when the conditions laid down by the manufacturer are considered.
Leakage	Yes, for seat valves if normal operating conditions apply (see remark) and if an adequate filtration system is provided.	
Change of the leakage flow rate over a long period of use	None.	
Bursting of the valve housing or breakage of the moving component(s) as well as breakage/fracture of the mounting or housing screws	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	—

Table C.8 — Faults and fault exclusions — Metal pipework

Fault considered	Fault exclusion	Remarks
Bursting and leakage	Yes, if the dimensioning, choice of materials and fixing are in accordance with good engineering practice.	Dimensioning, possible loads due to vibrations and pressure pulsations must be considered (e.g. due to gear pumps).
Failure at the connector (e.g. tearing off, leakage)	Yes, if welded fittings or welded flanges or flared fittings are used, and dimensioning, choice of materials, manufacture, configuration and fixing are in accordance with good engineering practice.	—
Clogging (blockage)	Yes, for pipework in the power circuit, and for control and measurement pipework if the nominal diameter is ≥ 3 mm.	

Table C.9 — Faults and fault exclusions — Hose assemblies

Fault considered	Fault exclusion	Remarks
Bursting, tearing off at the fitting attachment and leakage	None.	—
Clogging (blockage)	Yes, for hose assemblies in the power circuit, and for control and measurement hose assemblies if the nominal diameter is ≥ 3 mm.	

Table C.10 — Faults and fault exclusions — Connectors

Fault considered	Fault exclusion	Remarks
Bursting, breaking of screws or stripping of threads	Yes, if dimensioning, choice of material, manufacture, configuration and connection to the piping and/or to the fluid technology component are in accordance with good engineering practice.	—
Leakage (loss of the leak-tightness)	None (see remark).	Due to wear, ageing, deterioration of elasticity, etc., it is not possible to exclude faults over a long period. A sudden major failure of the leak-tightness is not assumed.
Clogging (blockage)	Yes, for applications in the power circuit, and for control and measurement connectors if the nominal diameter is ≥ 3 mm.	—

Table C.11 — Faults and fault exclusions — Filters

Fault considered	Fault exclusion	Remarks
Blockage of the filter element	None.	—
Rupture of the filter element	Yes, if the filter element is sufficiently resistant to pressure and an effective bypass valve or an effective monitoring of dirt is provided.	
Failure of the bypass valve	Yes, if the guidance system of the bypass valve is designed similarly to that for a non-controlled ball seat valve without a damping device (see Table C.5) and if well-tried springs are used (see Table A.3).	
Failure of the dirt indicator or dirt monitor	None.	
Bursting of the filter housing or fracture of the cover or connecting elements	Yes, if dimensioning, choice of material, arrangement in the system and fixing are in accordance with good engineering practice.	

Table C.12 — Faults and fault exclusions — Energy storage

Fault considered	Fault exclusion	Remarks
Fracture/bursting of the energy storage vessel or connectors or cover screws as well as stripping of the screw threads	Yes, if construction, choice of equipment, choice of materials and arrangement in the system are in accordance with good engineering practice.	—
Leakage at the separating element between the gas and the operating fluid	None.	
Failure/breakage of the separating element between the gas and the operating fluid	Yes, in the case of cylinder/piston storage (see remark).	A sudden major leakage is not to be considered.
Failure of the filling valve on the gas side	Yes, if the filling valve is installed in accordance with good engineering practice and if adequate protection against external influences is provided.	—

Table C.13 — Faults and fault exclusions — Sensors

Fault considered	Fault exclusion	Remarks
Faulty sensor (see remark)	None.	Types of sensors include signal capture, processing and output, in particular for pressure, flow rate and temperature.
Change of the detection or output characteristics	None.	—

Annex D (informative)

Validation tools for electrical systems

D.1 General

Annex D applies to electrical systems. It should also be considered when electric systems are used in conjunction with other technologies.

The environmental conditions of IEC 60204-1:2016 + AMD1:2021 apply to the validation process. If other environmental conditions are specified, they should also be considered.

Table D.1 and Table D.2 list basic and well-trying safety principles.

The fulfilment of principles can depend on multiple contributors (see 4.1, Table 2, implemented in column 3 of Table D.1 and Table D.2).

The use of components designed according to a product standard can be helpful for the confirmation of some basic or well-trying safety principles (see Table 2, Note 2).

NOTE 1 Examples of product standards are IEC 61131 (all parts) for programmable controller and their associated peripherals, IEC 61800 (all parts) for power drive systems and IEC 60947 (all parts) for low-voltage switchgear and control gear.

The components listed in Table D.3 are considered to be “well-trying” when they comply with the description given in ISO 13849-1:2023, 6.1.11. The standards listed in Table D.3 should be used to demonstrate their suitability and reliability for a particular application. A well-trying component for some applications can be inappropriate for other applications. The status of being well-trying does not mean that all faults can be excluded for a well-trying component.

NOTE 2 Complex electronic components, such as programmable logic controllers (PLCs), microprocessors and application-specific integrated circuits, cannot be considered equivalent to the “well-trying” components.

Table D.4 to Table D.22 list fault exclusions.

For validation, both permanent faults and transient disturbances should be considered.

Table D.1 — Basic safety principles

Basic safety principle	Remarks	Relevant for (see Table 2)
Use of suitable materials and adequate manufacturing	Selection of material, manufacturing methods and treatment in relation to e.g. stress, durability, elasticity, friction, wear, corrosion, temperature, conductivity, dielectric rigidity.	M, D
Correct dimensioning and shaping	Consider, e.g. stress, strain, fatigue, surface roughness, tolerances, manufacturing.	M, D
Correct selection, combination, arrangements, assembly and installation of components or systems related to the application	Apply the installation and operation instructions provided by the manufacturer, e.g. catalogue sheets, installation instructions, specifications, and use of good engineering practice in similar components or systems.	M, D, U
	Use components compatible with the voltages and currents used.	M, D
Use of de-energization This principle is not applicable when loss of energy creates a hazard, e.g. release of workpiece caused by loss of clamping or holding force.	The safe state is obtained by de-energizing all relevant devices, e.g. by use of normally closed (NC) contact for inputs (push-buttons and position switches) and normally open (NO) contact for relays (see also ISO 12100:2010, 6.2.11.3). Time-delay functions may be necessary to achieve a system safe state (see e.g. IEC 60204-1:2016 + AMD1:2021, 9.2.2).	M, D
Correct fastening	For fastening of electrical conductors, e.g. DC busbars in frequency converters, apply the manufacturer's installation and operation instructions. Fastening in the correct orientation and fastening to the correct torque is considered. Overloading can be avoided and adequate resistance to release can be achieved by applying adequate torque loading technology.	M, D, U
Withstanding environmental conditions (see ISO 13849-1:2023, Clause 10, and follow manufacturer's installation and operation instructions)	Design the equipment so that it can work within the environmental limits of the intended use and in any reasonably foreseeable adverse conditions, e.g. temperature, humidity, vibration and electromagnetic interference (EMI).	M, D, U
Prevention of the ingress of solid foreign objects and fluids	Apply an appropriate degree of protection against ingress of solid foreign objects and fluids. Consider IP rating (see IEC 60529:1989+AMD1:1999+AMD2:2013+Cor1:2019)	M, D, U
Limitation of speed, acceleration and jerk (to avoid or limit mechanical stress)	An example is the acceleration limitation of a motor by limitation of the motor current in a frequency converter.	M, D
Reduction of response time	Minimize delay in de-energizing of switching components. Suitable range of switching time, e.g. response time of devices and components (e.g. solenoids, contactors, relays) and the effects of EMI measures to these elements (e.g. surge suppression diodes on contactors).	M, D
Protection against unexpected start-up (see ISO 12100:2010, 6.2.11.4, ISO 14118:2017)	Consider unexpected start-up caused by stored energy and after power supply restoration for different modes, e.g. operation mode, maintenance mode. (See IEC 60204-1:2016 + AMD1:2021).	M, D
	Special equipment for release of stored energy can be necessary. Special applications, e.g. to keep energy for clamping devices or ensure a position, need to be considered separately.	M, D, U
Abbreviations M – Design and manufacturing of components D – Design of subsystems U – Use of the machine		

Table D.1 (continued)

Basic safety principle	Remarks	Relevant for (see Table 2)
Simplification	Avoid unnecessary components in the safety-related system.	M, D
Separation	Separation of safety-related functions from other functions.	M, D
Current limitation (e.g. to prevent wear)	Example is a resistor (series resistor).	M, D
Correct protective bonding	One side of the control circuit, one terminal of the operating coil of each electromagnetic operated device, or one terminal of another electrical device is connected to the protective bonding circuit. (See IEC 60204-1:2016 + AMD1:2021, 9.4.3.1)	M, D, U
Insulation monitoring	Use of an insulation monitoring device which either indicates an earth fault or interrupts the circuit automatically after an earth fault. (See IEC 60204-1:2016 + AMD1:2021, 6.3.3)	M, D, U
Transient suppression	Use of a suppression device (RC, diode, varistor) parallel to the load, but not parallel to the contacts. NOTE A diode increases the switch-off time.	M, D
Temperature range	External and internal temperature effects are considered throughout the whole system.	M, D, U
Secure fixing of input devices	Secure input devices, e.g. interlocking switches, position switches, limit switches, proximity switches, so that position, alignment and switching tolerance is maintained under all expected conditions, e.g. vibration, normal wear, ingress of foreign bodies, temperature. (See ISO 14119:2024, Clause 5)	M, D, U
Protection of the control circuit	Apply protection in accordance with IEC 60204-1:2016 + AMD1: 2021, 7.2 and 9.1.1.	M, D
Sequential switching for circuit of serial contacts of redundant signals	To avoid common mode failure by the welding of both contacts, switching on and off does not happen simultaneously, so that one contact always switches without load.	M, D
Abbreviations M – Design and manufacturing of components D – Design of subsystems U – Use of the machine		

Table D.2 — Well-trying safety principles

Well-trying safety principle	Remarks	Relevant for (see Table 2)
Use of components with oriented failure mode (see ISO 12100:2010, 6.2.12.3)	Use oriented failure mode components or systems wherever practicable. A safe state is directly or indirectly (e.g. through fault detection) obtained by the predominant failure mode.	M, D
Over-dimensioning	De-rate components when used in safety circuits, e.g. by the following means: — the current passed through switched contacts should be less than half their rated current; — the switching frequency of components should be less than half their rated value; — the total number of expected switching operations should be no more than 10 % of the device's electrical durability. NOTE De-rating can depend on the design rationale. Safety factors are as given in standards or by good engineering practice in safety-related applications.	M, D
Separation distance	Use of sufficient distance between position terminals, components and wiring to avoid unintended connections.	M, D
Minimizing possibility of faults	Separate safety-related functions from the other functions.	M, D
Positive mechanical action (see ISO 12100:2010, 6.2.5.)	Direct action is transmitted by the shape (and not the strength) with no elastic elements, e.g. spring between actuator and the contacts (see ISO 14119:2024, 5.1). To achieve positive (or direct) mechanical action, mechanical components needed for the safety function are moved either by direct contact or via rigid elements.	M, D
Multiple parts	Reducing the effect of faults by providing multiple parts acting in parallel, e.g. where a failure of one of several resistors does not lead to a dangerous condition.	M, D
Use of well-trying spring	See Table A.3	M
Limited range of force and similar parameters to avoid or limit mechanical stress This principle is not applicable when the continued integrity of components is essential to maintaining the necessary level of control.	Determination of the necessary limitation in relation to the experience and application.	M, D
Limited range of environmental parameters See ISO 13849-1:2023, 10.7	Determination of the necessary limitations. Examples are temperature, humidity, pollution at the installation. Follow manufacturer's installation and operation instructions.	M, D, U
Limited range of reaction time, limited hysteresis	Determination of the necessary limitations. For example, proper selection of protective devices.	M, D
Positively mechanically linked contacts	Use of positively mechanically linked contacts for, e.g. monitoring function in Category 2, 3, and 4 systems (IEC 61810-3:2015, IEC 60947-4-1:2023, Annex F, IEC 60947-5-1:2024, Annex L).	M, D
Abbreviations M – Design and manufacturing of components D – Design of subsystems U – Use of the machine		

Table D.2 (continued)

Well-tried safety principle	Remarks	Relevant for (see Table 2)
Fault avoidance or detection in cables	To avoid or detect short circuits between two adjacent conductors, — use cable with shielding connected to the protective bonding circuit on each separate conductor; — in flat cables, use one earthed conductor between each signal conductor; or — use cross-circuit monitoring, e.g. by test pulses.	M, D
Energy limitation	Use of a capacitor for supplying a finite amount of energy, e.g. in a timer application.	M, D
Limitation of electrical parameters	Limiting voltage, current, energy or frequency to restrict movement, e.g. torque limitation, hold-to-run with displacement/time limited, reduced speed, to avoid an unsafe state.	M, D
No undefined states	Avoid undefined states in the control system. Design and construct the control system so that, during normal operation and all expected operating conditions, its state, e.g. its output(s), can be predicted.	M, D
Failure mode orientation	Wherever possible, the device/circuit should fail to the safe state or condition.	M, D
Balance complexity and simplicity	Balance between complexity to reach better control and simplification to have better reliability.	M, D
Abbreviations M – Design and manufacturing of components D – Design of subsystems U – Use of the machine		

Table D.3 — Well-tried components

Well-tried component	Additional conditions for “well-tried”	Standard or specification
Switch with positive mode actuation (direct opening action), e.g.: — push-button; — position switch; — cam-operated selector switch, e.g. for mode of operation	—	IEC 60947-5-1:2024, Annex K
Emergency stop device	—	ISO 13850:2015 IEC 60947-5-5:1997+AMD1:2005+AMD2:2016
Fuse	—	IEC 60269-1:2024
Circuit-breaker	—	IEC 60947-2:2024
Switches, disconnectors	—	IEC 60947-3:2025
Differential circuit-breaker or RCD (residual current device)	—	IEC 60947-2:2024

Table D.3 (continued)

Well-trying component	Additional conditions for “well-trying”	Standard or specification
Main contactor	Only well-trying if a) other influences are considered, e.g. vibration; b) failure is avoided by appropriate methods, e.g. over-dimensioning (see Table D.2); c) the short-circuit current to the load is limited by a protection device, e.g. thermal fuse; and d) the circuits are protected by a protection device against overload.	IEC 60947-4-1:2023
Control and protective switching device or equipment (CPS)	—	IEC 60947-6-2:2020
Force Guided Relays (e.g. Auxiliary contactor, contactor relay)	Only well-trying if a) other influences are considered, e.g. vibration; b) there is positive opening; c) failure is avoided by appropriate methods, e.g. over-dimensioning (see Table D.2); d) the current in the contacts is limited by a fuse or circuit-breaker to avoid the welding of the contacts; and e) contacts are positively mechanically guided when used for monitoring.	IEC 61810-1:2015/AMD1: 2019 IEC 61810-2:2017 IEC 61810-3:2015 IEC 60947-5-1:2024 IEC 60947-4-1:2023, Annex F
Relay	Only well-trying if a) other influences are considered, e.g. vibration; b) positive opening action; c) failure avoided by appropriate methods, e.g. over-dimensioning (see Table D.2); and d) the current in the contacts is limited by fuse or circuit-breaker to avoid the welding of the contacts.	IEC 61810-1:2015+AMD1: 2019 IEC 61810-2:2017 IEC 61810-3:2015
Transformer	—	IEC 61558 (all parts)
Cable	Protection of cabling external to enclosure against mechanical damage (including, e.g. vibration or bending) is considered.	IEC 60204-1:2016 + AMD1: 2021, Clause 12
Plug and socket	—	According to an electrical standard relevant for the intended application. For interlocking, see also ISO 14119:2024.

Table D.3 (continued)

Well-tried component	Additional conditions for “well-tried”	Standard or specification
Temperature switch	Only well-tried if a) the component fulfils the basic and well-tried safety principles regarding the intended application (see NOTE), including use of the component according to the specification of the manufacturer; b) proven to be widely used in the past with documented successful results in similar applications or made, verified and validated using principles which demonstrate its suitability and reliability for safety-related applications according to relevant product and application standards; c) either no electronics on-board or on-board electronics, if available, does not participate in executing the safety function; d) the behavior of the component under all conditions is well defined and can be completely determined; and e) the following construction characteristics are fulfilled: — simple, robust design; — positive connection; — sufficient protection against loosening with detachable connection; and — sufficiently robust in relation to the use (application) and the ambient conditions (e.g. humidity, vibration).	ISO 13849-1:2023, 6.1.11 For the electrical part, see IEC 607301:2022
NOTE The confirmation of basic and well-tried safety principles as well as proof of wide use in the past with documented successful results in similar applications can be done by the component manufacturer or by the designer of the subsystem.		

D.2 Fault exclusion

D.2.1 General

A fault exclusion is valid only if the parts operate within their specified ratings.

D.2.2 “Tin whiskers”

If lead-free processes and products are applied, electrical short circuits due to the growth of “tin whiskers” can occur. This possibility should be evaluated and considered when applying the fault exclusion “short circuit ...” of any component. For example, if the risk of tin whisker growth is considered high, the fault exclusion “short circuit of a resistor” is useless, since a short between the contacts of this component has to be considered.

NOTE 1 Tin whisker growth is a phenomenon related mainly to pure bright tin finishes. The needle-like protrusions can grow to several hundred micrometers in length and can cause electrical short circuits. The prevailing theory is that the whiskers are caused by compressive stress build-up in tin plating.

NOTE 2 References [47] and [48] can be helpful for evaluation of the phenomenon.

**E DIN EN ISO 13849-2:2026-03
ISO/DIS 13849-2:2026(en)**

NOTE 3 Whiskers on printed circuit boards have not so far been reported. Tracks usually consist of copper without tin coating. Pads can be coated with tin alloy, but the production process seems not to stimulate the susceptibility to whisker growing.

D.2.3 Short circuits on PCB-mounted parts

Short circuits for parts which are mounted on a printed circuit board (PCB) can only be excluded if the fault exclusion “short circuit between two adjacent tracks/pads”, described in Table D.5, is made.

D.2.4 Fault exclusions and integrated circuits

As it is not possible to exclude faults that can cause the malfunction of an integrated circuit (see Table D.20 and Table D.21), a single fault can lead to loss of a safety function (including its check/test) implemented in a single integrated circuit. Consequently, it is highly unlikely that either the multi-channel functionality necessary for the fault tolerance or detection requirements of category 2, 3 or 4, or both, can be achieved using a single integrated circuit, unless it satisfies the special architecture requirements of IEC 61508-2:2010, Annex E.

Table D.4 — Faults and fault exclusions — Conductors/cables

Fault considered	Fault exclusion	Remarks
Short circuit between any two conductors	Short circuits between conductors which are — permanently connected (fixed) and protected against external damage, e.g. by cable ducting, armoring; — separate multicore cables; — within an electrical enclosure (see remark); or — individually shielded with earth connection.	Provided both the conductors and enclosure meet the appropriate requirements (see IEC 60204-1:2016 + AMD1:2021).
Short circuit of any conductor to an exposed conductive part or to earth or to the protective bonding conductor	Short circuits between conductor and any exposed conductive part within an electrical enclosure (see remark).	
Open circuit of any conductor	None.	—

Table D.5 — Faults and fault exclusions — Printed circuit boards/assemblies

Fault considered	Fault exclusion	Remarks
Short circuit between two adjacent tracks/pads	Short circuits between adjacent conductors in accordance with remarks.	As base material, EP GC according to IEC 60893-1:2004 is used as a minimum. The clearances and creepage distances are dimensioned to at least IEC 60664-1:2025, for pollution degree 2/overvoltage category III. If both tracks are powered by a SELV/PELV power supply, pollution degree 2/overvoltage category II applies, with a minimum clearance of 0,1 mm. The assembled board is mounted in an enclosure giving protection against conductive contamination, e.g. an enclosure with a protection of at least IP54, and the printed side(s) is (are) coated with an ageing-resistant varnish or protective layer covering all conductor paths. NOTE 1 Experience has shown that solder masks are satisfactory as a protective layer. NOTE 2 A further protective layer covering according to IEC 60664-3:2016 can reduce the creepage distances and clearances dimensions.
Open circuit of any track	None.	—

**E DIN EN ISO 13849-2:2026-03
ISO/DIS 13849-2:2026(en)**

Table D.6 — Faults and fault exclusions — Terminal block

Fault considered	Fault exclusion	Remarks
Short circuit between adjacent terminals	Short circuit between adjacent terminals in accordance with remarks 1) or 2).	1) The terminals and connections used are in accordance with IEC 60947-7-1:2025 or IEC 60947-7-2:2009 and the requirements of IEC 60204-1:2016 + AMD1:2021, 13.1.1, are satisfied. 2) The design in itself ensures that a short circuit is avoided, e.g. by shaping shrink-down plastic tubing over connection point.
Open circuit of individual terminals	None.	—

Table D.7 — Faults and fault exclusions — Multi-pin connector

Fault considered	Fault exclusion	Remarks
Short circuit between any two adjacent pins	Short circuit between adjacent pins in accordance with remark. If the connector is mounted on a PCB, the fault exclusion considerations of Table D.5 apply.	By using ferrules or other suitable means for multi-stranded wires. Creepage distances and clearances and all gaps should be dimensioned to at least IEC 60664-1:2025 with overvoltage category III.
Interchanged or incorrectly inserted connector when not prevented by mechanical means	None.	—
Short circuit of any conductor (see remark) to earth or a conductive part or to the protective conductor	None.	The core of the cable is considered a part of the multi-pin connector.
Open circuit of individual connector pins	None.	—

Table D.8 — Faults and fault exclusions — Switches — Electromechanical position switches, manually operated switches (e.g. push-button, reset actuator, DIP switch, magnetically operated contacts, reed switch, pressure switch, temperature switch)

Fault considered	Fault exclusion	Remarks
Contact will not close	None.	—
Contact will not open	Contacts in accordance with IEC 60947-5-1:2024, Annex K, are expected to open.	—
Short circuit between adjacent contacts insulated from each other	Short circuit can be excluded for switches in accordance with IEC 60947-5-1:2024 (see remark).	Conductive parts which become loose should not be able to bridge the insulation between contacts.
Simultaneous short circuit between three terminals of change-over contacts	Simultaneous short circuits can be excluded for switches in accordance with IEC 60947-5-1:2024 (see remark).	
NOTE 1 For PL e, a fault exclusion for mechanical (e.g. the mechanical link between an actuator and a contact element) and electrical aspects is not allowed. In this case redundancy is necessary. For emergency stop devices in accordance with IEC 60947-5-5:1997+AMD1:2005+AMD2:2016, a fault exclusion for mechanical aspects is allowed if a maximum number of operations is considered.		
NOTE 2 The fault lists for the mechanical aspects are considered in Annex A.		

Table D.9 — Faults and fault exclusions — Switches — Electromechanical devices (e.g. relays, contactors and valve switches)

Fault considered	Fault exclusion	Remarks
All contacts remain in the energized position when the coil is de-energized (e.g. due to mechanical fault)	None.	—
All contacts remain in the de-energized position when power is applied (e.g. due to mechanical fault, open circuit of coil)	None.	
Contact will not open	None.	
Contact will not close	None.	
Simultaneous short circuit between the three terminals of a change-over contact	Simultaneous short circuit can be excluded if remarks are considered.	The creepage and clearance distances are dimensioned to at least IEC 60664-1:2025 with at least pollution degree 2/overvoltage category III. Conductive parts which become loose cannot bridge the insulation between contacts and the coil.
Short circuit between two pairs of contacts and/or between contacts and coil terminal	Short circuit can be excluded if remarks are considered.	
Simultaneous closing of normally open and normally closed contacts	Simultaneous closing of contacts can be excluded if remark is considered.	Positively driven (or mechanically linked) contacts are used (see IEC 60947-5-1:2024, Annex L).

Table D.10 — Faults and fault exclusions — Switches — Proximity switches

Fault considered	Fault exclusion	Remarks
Permanently low resistance at output	None (see remark).	See IEC 60947-5-3:2013.
Permanently high resistance at output	None (see remark).	Fault prevention measures should be described.
Interruption in power supply	None.	—
No operation of switch due to mechanical failure	No operation due to mechanical failure when remark is considered.	All parts of the switch should be sufficiently well fixed. For mechanical aspects, see Annex A.
Short circuit between the three connections of a change-over switch	None.	—

Table D.11 — Faults and fault exclusions — Switches — Solenoid valves

Fault considered	Fault exclusion	Remarks
Does not energize	None.	—
Does not de-energize	None.	
NOTE The fault lists for the mechanical aspects of pneumatic and hydraulic valves are considered in Annexes B and C respectively.		

**E DIN EN ISO 13849-2:2026-03
ISO/DIS 13849-2:2026(en)**

Table D.12 — Faults and fault exclusions — Discrete electrical components — Transformers

Fault considered	Fault exclusion	Remarks
Open circuit of individual winding	None.	—
Short circuit between different windings	Short circuit between different windings can be excluded if remarks 1) and 2) are considered.	1) The requirements of the relevant parts of IEC 61558 (all parts) should be met. 2) Between different windings, doubled or reinforced insulation or a protective screen applies. Testing according to e.g. IEC 61558-1:2017, Clause 18, applies. Appropriate test voltages are given in IEC 61558-1:2017, Table 8 a) or other appropriate product standards. Short circuits in coils and windings need to be avoided by taking appropriate steps; e.g. — impregnating the coils so as to fill all the cavities between individual coils and the body of the coil and the core; — using winding conductors well within their insulation and high-temperature ratings. 3) In the event of a secondary short circuit, heating above a specified operating temperature should not occur.
Short circuit in one winding	A short circuit in one winding can be excluded if remark 1) is considered.	
Change in effective turns ratio	Change in effective turns ratio can be excluded if remark 1) is considered. See also remark 3).	

Table D.13 — Faults and fault exclusions — Discrete electrical components — Inductances

Fault considered	Fault exclusion	Remarks
Open circuit	None.	—
Short circuit	Short circuit can be excluded if remark 1) is considered.	Coil is single-layered, enamelled or potted, with axial wire connections and axial-mounted.
Random change of value $0,5 L_N < L < L_N$ + tolerance, where L_N is the nominal value of the inductors	None.	Depending upon the type of construction, other ranges can be considered.

Table D.14 — Faults and fault exclusions — Discrete electrical components — Resistors

Fault considered	Fault exclusion	Remarks
Open circuit	None.	—
Short circuit	Short circuit can be excluded if remark 1) or 2) is considered.	1) The resistor is of the film type, or wire-wound single-layer type with protection to prevent unwinding of wire in the event of breakage, with axial wire connections, axial-mounted and varnished. 2) Resistors in surface-mount technology must be of the thin film metal type in package types MELF, mini MELF or μ MELF. 3) For example, if the risk of tin-whisker growth is considered high, the fault exclusion “short circuit of a resistor” is useless, since a short between the contacts of this component has to be considered.
Random change of value $0,5 R_N < R < 2 R_N$, where R_N is the nominal value of resistance	None.	

Table D.15 — Faults and fault exclusions — Discrete electrical components — Resistor networks

Fault considered	Fault exclusion	Remarks
Open circuit	None.	—
Short circuit between any two connections	None.	
Short circuit between any connections	None.	
Random change of value $0,5 R_N < R < 2 R_N$, where R_N is the nominal value of resistance	None.	Depending upon the type of construction, other ranges can be considered.

Table D.16 — Faults and fault exclusions — Discrete electrical components — Potentiometers

Fault considered	Fault exclusion	Remarks
Open circuit of individual connection	None.	—
Short circuit between all connections	None.	
Short circuit between any two connections	None.	
Random change of value $0,5 R_p < R < 2 R_p$, where R_p is the nominal value of resistance	None.	Depending upon the type of construction, other ranges can be considered.

Table D.17 — Faults and fault exclusions — Discrete electrical components — Capacitors

Fault considered	Fault exclusion	Remarks
Open circuit	None.	—
Short circuit	None.	
Random change of value $0,5 C_N < C < C_N + \text{tolerance}$, where C_N is the nominal value of capacitance	None.	Depending upon the type of construction, other ranges can be considered.
Changing value $\tan \delta$	None.	—

Table D.18 — Faults and fault exclusions — Electronic components — Discrete semiconductors (e.g. diodes, Zener diodes, transistors, triacs, thyristors, voltage regulators, quartz crystal, phototransistors, light-emitting diodes [LEDs])

Fault considered	Fault exclusion	Remarks
Open circuit of any connection	None.	—
Short circuit between any two connections	None.	
Short circuit between all connections	None.	
Change in characteristics	None.	

**E DIN EN ISO 13849-2:2026-03
ISO/DIS 13849-2:2026(en)**

Table D.19 — Faults and fault exclusions — Electronic components — Couplers for galvanic isolation (e.g. optocouplers, capacitive couplers)

Fault considered	Fault exclusion	Remarks
Open circuit of individual connection	None.	—
Short circuit between any two input connections	None.	
Short circuit between any two output connections	None.	
Short circuit between any two connections of input and output	Short circuit between input and output can be excluded if the remarks are considered.	The coupler is built in accordance with overvoltage category III according to IEC 60664-1:2025. If a SELV/PELV power supply is used, pollution degree 2/overvoltage category II applies. NOTE See Table D.5. Measures are taken to ensure that an internal failure of the coupler for galvanic isolation cannot result in excessive temperature of its insulating material.

Table D.20 — Faults and fault exclusions — Electronic components — Non-programmable and non-complex integrated circuits

Fault considered	Fault exclusions	Remarks
Open circuit of each individual connection	None.	—
Short circuit between any two connections	None.	—
Stuck-at-fault (i.e. short circuit to 1 and 0 with isolated input or disconnected output). Static “0” and “1” signal at all inputs and outputs, either individually or simultaneously	None.	—
Parasitic oscillation of outputs	None.	—
Changing values (e.g. input/output voltage of analogue devices or change of information due to soft error if shown to be relevant)	None.	See Annex D.3.
NOTE In this document, ICs with either less than 1 000 gates or less than 24 pins, or both; operational amplifiers; shift registers and hybrid modules are considered non-complex. This definition is arbitrary.		

Table D.21 — Faults and fault exclusions — Electronic components — Programmable or complex integrated circuits

Fault considered	Fault exclusions	Remarks
Faults in all or part of the function including software faults	None.	—
Open circuit of each individual connection	None.	—
Short circuit between any two connections	None.	—
Stuck-at-fault (i.e. short circuit to 1 and 0 with isolated input or disconnected output). Static “0” and “1” signal at all inputs and outputs, either individually or simultaneously	None.	—
Parasitic oscillation of outputs	None.	—
NOTE 1 The analysis should identify additional faults, which should be considered if they influence the operation of the safety function.		
NOTE 2 In this document, an IC is considered complex if it consists of either more than 1 000 gates or more than 24 pins, or both. This definition is arbitrary.		

Table D.21 (continued)

Fault considered	Fault exclusions	Remarks
Changing value, e.g. - input/output voltage of analogue devices - change of information due to soft error if shown to be relevant, e.g. for RAM, FPGA	None.	See Annex D.3
Undetected faults in the hardware which go unnoticed because of the complexity of the integrated circuit	None.	—
NOTE 1 The analysis should identify additional faults, which should be considered if they influence the operation of the safety function.		
NOTE 2 In this document, an IC is considered complex if it consists of either more than 1 000 gates or more than 24 pins, or both. This definition is arbitrary.		

Table D.22 — Faults and fault exclusions – Transmission errors in digital data communication

Fault considered	Fault exclusion	Remarks
Communication errors (corruption, unintended repetition, incorrect sequence, loss, unacceptable delay, insertion, masquerade, addressing)	None	Measures to control the effects of errors and other effects arising from any data communication, including transmission errors (such as corruption, unintended repetition, incorrect sequence, loss, unacceptable delay, insertion, masquerade, addressing) should be applied. NOTE 1 Further information can be found in IEC 61784-3:2021+AMD1:2024, 5.3, Table 1 and IEC 61508-2:2010, 7.4.11.2. NOTE 2 The term ‘masquerade’ means that the true contents of a message are not correctly identified. For example, a message from a non-safety component is incorrectly identified as a message from a safety component.

D.3 Soft errors

D.3.1 General

Soft errors are relevant for hardware containing semiconductors with volatile memories and sequential logic.

Components can be used without consideration of soft error rates if mitigation measures (see D.3.4.3), implemented in hardware, SRESW or SRASW, are integrated. The contribution of soft errors to the PFH is typically considered at subsystem level in the following three steps: analysis, avoidance, and control. Soft errors are normally considered up to the subsystem level. In the design phase of integration of subsystems to SRP/CS, normally there is no need to consider soft errors.

For further information on soft errors see also IEC 61508-2-1 Ed 1 (under development) as well as IEC 61508-4:2010.

D.3.2 Introduction to soft errors

Soft errors

- are non-permanent unintended hardware states, e.g. reverse or flip the data state of a semiconductor memory cell, latch, or flip flop, which can persist as a latent fault;
- are types of errors where a signal or data value is corrupted, but there is no permanent damage to the hardware;
- are mainly caused by charge disturbance due to radiation events (alpha particles from package decay and cosmic rays creating energetic neutrons);

- are random hardware faults that can be quantified with a probabilistic method supported by measured data;
- mainly affect volatile memories and sequential logic;
- can be classified as single event upset (SEU) or multiple bit upset (MBU).

D.3.3 Relevance of soft errors for functional safety

This document states in Annex D.1 (General) that for validation, both permanent faults and transient disturbances should be considered.

Especially digital circuits, e. g. RAM, FPGA, microcontrollers, show a high susceptibility to soft errors. Flash memories are non-volatile and therefore they usually show lower susceptibility.

Soft error rates can dominate compared with rates of permanent random hardware faults for certain technologies. This depends on the amount and density of memory cells in RAM memories.

Diagnostic measures effective for hard errors will possibly not be effective for soft errors. The effect of soft errors can be mastered by adequate safety measures at runtime. RAM tests, such as walk-path, galpat, etc. are not effective, whereas monitoring techniques such as parity and error correcting code (ECC) with recurring read of the memory cells are.

Soft errors are expected to remain relevant also in the future. This is due to device scaling, continuous decreasing of the technology node size and of the integrated circuit supply voltage.

For further information see IEC 61508-7:2010, A.5.

D.3.4 Avoidance and control of soft errors during subsystem design

D.3.4.1 Analysis

Each integrated circuit, containing e. g. flip flops, latches, volatile memory elements or analogue devices should be investigated for potential susceptibility to soft errors.

Diagnostic measures implemented in integrated circuits such as ECC can reduce the probability that a soft error will result in a dangerous failure in the safety function.

Offline CPU self-tests or RAM tests are not effective for soft errors. The effect of soft errors can only be mastered by safety measures at runtime. Scrubbing of memories is a means to reduce build-up of multibit errors.

D.3.4.2 Avoidance and reduction of soft errors

The probability of soft errors can be reduced by avoidance of electronic components with high soft error susceptibility or substitution of them by components with low susceptibility. Suitable components with low soft error rates should be selected according to their data sheets or manufacturer's information.

NOTE Depending on the application it is sometimes not possible to avoid soft errors completely if complex electronic components are used (containing memory elements).

Depending on the application design measures at subsystem or SRP/CS level, e. g. shielding against cosmic rays can reduce the probability of soft errors. Shielding is not effective against radioactive contaminants in the chip-housing or in the semiconductor material itself.

D.3.4.3 Control of soft errors

To improve the control of soft errors additional measures, like e.g. radiation hardened design or software measures (e.g. on-chip ECC or redundant data storage), can be applied.

For single channel architectures such as Categories B and 2, software mitigation measures e. g. based on informational redundancy (for example by adding extra information to the data by means of error correcting codes), or temporal redundancy (e.g. by executing the same program two times in sequence; SEU are detected by comparison) are effective against dangerous failures due to soft errors.

NOTE For information on soft errors mitigation solutions see [50].

Redundant functional channels with fault detection by comparison are very effective against dangerous failures due to soft errors. Since soft errors have local causes even homogeneous redundancy shows high efficiency. This is different from common cause failures (CCF) where homogeneous redundancy in some cases is less effective.

Soft errors are more critical to single channel architectures such as category B and 1, but category B is limited to PL b. Furthermore, in category 1 complex components as mentioned in D.3.2 are not considered as equivalent to well-tries.

Soft errors can significantly affect single channel architectures such as category 2 with low diagnostic coverage. In this case the PL is limited to c or in rare cases d.

Soft errors are less critical to single channel architectures such as category 2 with at least medium diagnostic coverage or architectures with redundant channels as category 3 and 4.

D.3.4.4 Determination of soft error rates to estimate PFH

For the determination of PFH, relevant soft error rates can be considered in the same way as hardware failure rates.

Soft errors are not expected to affect both channels in a category 2, 3 or 4 system in the same way. For this reason, the soft error rate typically does not have to be considered in the CCF part of the PFH calculation.

Generally, the portion of the soft error rate induced by cosmic radiation depends on the altitude above sea level. For cases of applications intended to be operated at higher altitudes, see [49] for further information.

D.3.4.5 Priority for the determination of soft error rates

The primary source for soft error rates is the data provided by the semiconductor manufacturer, e. g. data sheets and white papers.

NOTE 1 It is preferable that the semiconductor manufacturer makes the base failure rate caused by alpha particles and neutrons available to the subsystem manufacturer for example in the safety manual^[49]. is considered as the main reference for the testing and calculation of the soft error rate by semiconductor manufacturers. On the semiconductor level logical and electrical masking is possible. In addition, process measures, layout measures or design techniques can prevent or reduce soft errors.

If the semiconductor manufacturer does not provide soft error rates, as an alternative, estimated values can be used. The documents maintained by the International Roadmap for Devices and Systems (IRDS) such as the International Technology Roadmap for Semiconductors (ITRS) provide projected values for the soft error rate for each chip generation.

As a last option, SN 29500-2:2010 (soft error rate 1 000 FIT/Mbit for SRAM devices) or other generic sources can be used as a rough estimation.

NOTE 2 SN 29500-1:2016, Clause 3 specifies the failure rates in FIT (failure in time), i.e., the number of failures in 10^9 component hours. Therefore $\lambda = 1$ FIT is equal to $\lambda = 10^{-9} \text{ h}^{-1}$ ($\lambda = 1/\text{MTTF}$, therefore $\lambda = 1$ FIT is equivalent to $\text{MTTF} = 114\,155 \text{ a}$).

D.3.4.6 Non-accessible hardware

Non-accessible hardware in the context of soft errors means, e.g. components without safety rating by the manufacturer, are used as “black box” components in the design of subsystems. The contribution of soft error rates to the PFH value of a subsystem typically cannot be determined because the necessary detailed internal hardware information (e.g. type, number, failure rate and size of programmable logic

involved and the fraction of memory bits that are safety relevant for the proper execution of the safety function) is not available to the integrator or designer of the subsystem. These components can be used without consideration of soft error rates if software mitigation measures (see D.3.4.3), implemented in hardware, SRESW or SRASW, are integrated in the non-accessible hardware. If no information is available regarding the implementation of software mitigation measures or if it is not possible to implement software mitigation measures in hardware, SRESW or SRASW, as a last alternative, these components can be used with consideration of soft error rates estimated as a 10 % reduction of the calculated $MTTF_D$ for random hardware failures.

NOTE 1 The 10 % estimate is based on the assumption that typically only a small amount of the volatile memory is safety-relevant and can lead to a dangerous failure. Additionally, most modern memory technologies internally use some soft error correcting mechanism.

See also 7.3.2 of ISO 13849-1:2023 if the non-accessible hardware incorporates non-accessible embedded software.

NOTE 2 Soft errors typically do not contribute to the PFH portion due to CCF, which is typically the main PFH contribution in categories 3 and 4 (see D.3.4.4).

NOTE 3 For components without a safety rating from the manufacturer, the reliability value available from the component manufacturer is usually only a rough estimate.

D.3.5 Example demonstrating the contribution of soft errors to estimate PFH

The example in Figure D.1 of a category 2 SRP/CS is intended to demonstrate the contribution of soft errors to the estimation of PFH according to the procedure laid down in D.3.4. The description of any details not relevant for soft errors is omitted.

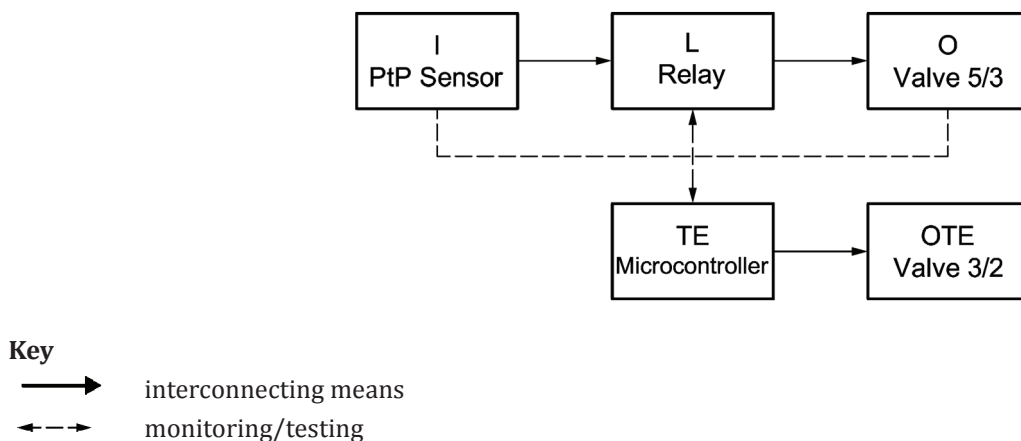


Figure D.1 — Safety-related block diagram for a category 2 SRP/CS

An analysis of the relevance of soft errors in this example shows that only the microcontroller (TE) is susceptible to soft errors.

For this example, a 64-bit microcontroller with ARM architecture was chosen, which is used in many control designs. Referring to the manufacturer's data sheet, it has 2 GByte of working memory (DRAM), 4 GByte of internal physical solid-state memory (eMMC) as well as 128 kByte of internal remanent solid-state memory (NVRAM).

Only the volatile memory (DRAM) contributes to the soft error rate since the solid-state memories (eMMC and NVRAM) are not affected by soft errors.

Errors in the data transmission of the PtP sensor (a sensor communicating by point-to-point-protocol) to the microcontroller due to soft errors are successfully controlled by error detecting measures in the data transmission protocol using cyclic redundancy checks (CRC) and other typical measures. The interconnection between the PtP sensor and the relay is based on a 24 V DC signal which is not susceptible to soft errors. The same applies for the interconnections to the valves.

E DIN EN ISO 13849-2:2026-03
ISO/DIS 13849-2:2026(en)

Avoidance and reduction of soft errors has been considered in this example by choosing a microcontroller suitable for this application which shows a low susceptibility to soft errors (low soft error rate). By separation of the safety-related embedded software (SRESW) from the non-safety-related software it can be estimated by analysis of the machine code that only about 1 MByte of the total 2 GByte DRAM contains SRESW.

The manufacturer of the microcontroller specifies a soft error rate of 100 FIT/MByte for its included volatile memory in the data sheet. Using a worst-case estimation of 50 % dangerous failures, this results in a dangerous failure rate due to soft errors $\lambda_D = 50$ FIT (or $MTTF_D = 2\,283$ a, see D.3.4.5, NOTE 2). Because soft errors events and permanent random hardware faults are statistically independent, both related failure rates have to be added to get the overall dangerous failure rate of TE.

This additional soft error contribution is not considered for the PFH portion due to CCF.

NOTE 1 The simplified procedure for estimating the PL for subsystems (see ISO 13849-1:2023, 6.1.8) is not capable of handling a separate dangerous failure rate for the PFH portion due to CCF. The alternative method which will be outlined in ISO/TR 13849-3 (currently being developed) allows for separate handling.

NOTE 2 The supplement of 2 283 years, due to soft errors, to the $MTTF_D$ of the block TE is very low compared to the contribution of permanent random hardware failures.

Annex ZAA (informative)

Relationship between this European Standard and the essential requirements of Directive 2006/42/EC aimed to be covered

This European Standard has been prepared under a Commission's standardization request "M/396 Mandate to CEN and CENELEC for Standardisation in the field of machinery" to provide one voluntary means of conforming to essential requirements of Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast).

Once this standard is cited in the Official Journal of the European Union under that Directive, compliance with the normative clauses of this standard given in Table ZAA.1 confers, within the limits of the scope of this standard, a presumption of conformity with the corresponding essential requirements of that Directive, and associated EFTA regulations.

Table ZAA.1 — Correspondence between this European Standard and Annex I of Directive 2006/42/EC

The relevant Essential Requirements of Directive 2006/42/EC	Clause(s)/sub-clause(s) of this EN	Remarks/Notes
1.2.1. Safety and reliability of control systems	4	

Table ZAA.2 — Applicable Standards to confer presumption of conformity as described in this Annex ZAA

Reference in Clause 2	International Standard Edition	Title	Corresponding European Standard Edition
ISO 12100:2010	ISO 12100:2010	<i>Safety of machinery — General principles for design — Risk assessment and risk reduction</i>	EN ISO 12100:2010
ISO 13849-1:2023	ISO 13849-1:2023	<i>Safety of machinery — Safety-related parts of control systems Part 1: General principles for design</i>	EN ISO 13849-1:2023

The documents listed in the Column 1 of Table ZAA.2, in whole or in part, are normatively referenced in this document, i.e. are indispensable for its application. The achievement of the presumption of conformity is subject to the application of the edition of Standards as listed in Column 4 or, if no European Standard Edition exists, the International Standard Edition given in Column 2 of Table ZAA.2.

WARNING 1 Presumption of conformity stays valid only as long as a reference to this European Standard is maintained in the list published in the Official Journal of the European Union. Users of this standard should consult frequently the latest list published in the Official Journal of the European Union.

WARNING 2 Other Union legislation may be applicable to the product(s) falling within the scope of this standard.

Annex ZAB (informative)

Relationship between this European Standard and the essential requirements of Regulation (EU) 2023/1230 aimed to be covered

This European Standard has been prepared under a Commission's standardization request C(2025)121 final Commission Implementing Decision of 20 January 2025 to the European Committee for Standardization and to the European Committee for Electrotechnical Standardization as regards machinery in support of Regulation (EU) 2023/1230 of the European Parliament and of the Council (M/605) to provide one voluntary means of conforming to essential requirements of Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery (OJ L 165, 29.6.2023).

Once this standard is cited in the Official Journal of the European Union under that Regulation, compliance with the normative clauses of this standard given in Table ZAB.1 confers, within the limits of the scope of this standard, a presumption of conformity with the corresponding essential requirements of that Regulation, and associated EFTA regulations.

Table ZAB.1 — Correspondence between this European Standard and Annex III of Regulation (EU) 2023/1230

The relevant Essential Requirements of Regulation (EU) 2023/1230	Clause(s)/sub-clause(s) of this EN	Remarks/Notes
1.2.1. Safety and reliability of control systems	4	Exclusions: 2. Paragraph: (a) second part: "... and intended and unintended external influences, including reasonably foreseeable malicious attempts from third parties leading to a hazardous situation", (d), (f) 3. Paragraph: (a), (b), (c) 4. Paragraph: (c)

Table ZAB.2 — Applicable Standards to confer presumption of conformity as described in this Annex ZAB

Reference in Clause 2	International Standard Edition	Title	Corresponding European Standard Edition
ISO 12100:2010	ISO 12100:2010	<i>Safety of machinery — General principles for design — Risk assessment and risk reduction</i>	EN ISO 12100:2010
ISO 13849-1:2023	ISO 13849-1:2023	<i>Safety of machinery — Safety-related parts of control systems Part 1: General principles for design</i>	EN ISO 13849-1:2023

The documents listed in the Column 1 of Table ZAB.2, in whole or in part, are normatively referenced in this document, i.e. are indispensable for its application. The achievement of the presumption of conformity is subject to the application of the edition of Standards as listed in Column 4 or, if no European Standard Edition exists, the International Standard Edition given in Column 2 of Table ZAB.2.

WARNING 1 Presumption of conformity stays valid only as long as a reference to this European Standard is maintained in the list published in the Official Journal of the European Union. Users of this standard should consult frequently the latest list published in the Official Journal of the European Union.

WARNING 2 Other Union legislation may be applicable to the product(s) falling within the scope of this standard.

Bibliography

- [1] IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*
- [2] IEC 60204-1:2016, + AMD1:2021, *Safety of machinery — Electrical equipment of machines — Part 1: General requirements*
- [3] ISO 14118:2017, *Safety of machinery — Prevention of unexpected start-up*
- [4] EN 13906-1:2013, *Cylindrical helical springs made from round wire and bar — Calculation and design — Part 1: Compression springs*
- [5] ISO 14119:2024, *Safety of machinery — Interlocking devices associated with guards — Principles for design and selection*
- [6] ISO 4126-2:2018, *Safety devices for protection against excessive pressure — Part 2: Bursting disc safety devices*
- [7] ISO 4414:2010, *Pneumatic fluid power — General rules and safety requirements for systems and their components*
- [8] IEC 60947-5-1:2024, *Low-voltage switchgear and controlgear — Part 5-1: Control circuit devices and switching elements — Electromechanical control circuit devices*
- [9] ISO 4079:2020, *Rubber hoses and hose assemblies — Textile-reinforced hydraulic types for oil-based or water-based fluids — Specification*
- [10] ISO 2398:2024, *Rubber hoses, textile-reinforced, for compressed air — Specification*
- [11] ISO 5774:2023, *Plastics hoses — Textile-reinforced types for compressed-air applications — Specification*
- [12] ISO 4413:2010, *Hydraulic fluid power — General rules and safety requirements for systems and their components*
- [13] ISO 4126-1:2013, *Safety devices for protection against excessive pressure — Part 1: Safety valves*
- [14] ISO 5598:2020, *Fluid power systems and components — Vocabulary*
- [15] IEC 60947 (all parts), *Low-voltage switchgear and controlgear*
- [16] IEC 61131 (all parts), *Programmable controllers*
- [17] IEC 61800 (all parts), *Adjustable speed electrical power drive systems*
- [18] IEC 60529:1989+AMD1:1999+AMD2:2013+Cor1:2019, *Degrees of protection provided by enclosures (IP Codes)*
- [19] IEC 61810-3:2015, *Electromechanical elementary relays — Part 3: Relays with forcibly guided (mechanically linked)*
- [20] IEC 60947-4-1:2023, *Low-voltage switchgear and controlgear — Part 4-1: Contactors and motor-starters — Electromechanical contactors and motor-starters*
- [21] IEC 60947-5-1:2024, *Low-voltage switchgear and controlgear — Part 5: Control circuit devices and switching elements — Section one: Electromechanical control circuit devices*
- [22] ISO 13850:2015, *Safety of machinery — Emergency stop function — Principles for design*
- [23] IEC 60947-5-5:1997+AMD1:2005+AMD2:2016, *Low-voltage switchgear and controlgear — Part 5-5: Control circuit devices and switching elements — Electrical emergency stop device with mechanical latching function*

E DIN EN ISO 13849-2:2026-03
ISO/DIS 13849-2:2026(en)

- [24] IEC 60269-1:2024, *Low-voltage fuses — Part 1: General requirements*
- [25] IEC 60947-2:2024, *Low-voltage switchgear and controlgear — Part 2: Circuit-breakers*
- [26] IEC 60947-3:2025, *Low-voltage switchgear and controlgear — Part 3: Switches, disconnectors, switch-disconnectors and fuse-combination units*
- [27] IEC 60947-6-2:2020, *Low-voltage switchgear and controlgear — Part 6-2: Multiple function equipment — Control and protective switching devices (or equipment) (CPS)*
- [28] IEC 60947-4-1:2023, *Low-voltage switchgear and controlgear — Part 4-1: Contactors and motor-starters — Electromechanical contactors and motor-starters*
- [29] IEC 61810-1:2025+AMD1:2019, *Electromechanical elementary relays — Part 1: General and safety requirements*
- [30] IEC 61810-3:2015, *Electromechanical elementary relays — Part 3: Relays with forcibly guided (mechanically linked) contacts*
- [31] IEC 61810-4:2020, *Electromechanical elementary relays — Part 4: General and safety requirements for reed relays*
- [32] IEC 61558 (all parts), *Safety of power transformers, power supply units and similar devices*
- [33] IEC 607301:2022, *Automatic electrical controls for household and similar use — Part 1: General requirements*
- [34] IEC 60893-1:2004, *Insulating materials - Industrial rigid laminated sheets based on thermosetting resins for electrical purposes — Part 1: Definitions, designations and general requirements*
- [35] IEC 60664-1:2025, *Insulation coordination for equipment within low-voltage systems — Part 1: Principles, requirements and tests*
- [36] IEC 60947-7-1:2025, *Low-voltage switchgear and controlgear — Part 7-1: Ancillary equipment — Terminal blocks for copper conductors*
- [37] IEC 60947-7-2:2009, *Low-voltage switchgear and controlgear — Part 7-2: Ancillary equipment — Protective conductor terminal blocks for copper conductors*
- [38] IEC 60947-5-3:2013, *Low-voltage switchgear and controlgear — Part 5-3: Control circuit devices and switching elements — Requirements for proximity devices with defined behaviour under fault conditions*
- [39] IEC 61558-1:2017, *Safety of power transformers, power supply units and similar — Part 1: General requirements and tests*
- [40] IEC 61784-3:2021+AMD1:2024, *Industrial communication networks — Profiles — Part 3: Functional safety fieldbuses - General rules and profile definitions*
- [41] IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*
- [42] IEC 61508-2-1, (ED1 under development), *Functional safety of electrical/electronic/ programmable electronic safety-related systems — Part 2-1: Requirements for complex semiconductors*
- [43] IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations*
- [44] IEC 61508-7:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures*
- [45] SN 29500-1:2016, *Failure rates of components, Part 1: Expected values, general*
- [46] SN 29500-2:2010, *Failure rates of components, Part 2: Expected values for integrated circuits*

- [47] JESD22A121.01, *Test Method for Measuring Whisker Growth on Tin and Alloy Surfaces Finishes*
- [48] JESD201, *Environmental Acceptance Requirements for Tin Whisker Susceptibility of Tin and Alloy Surface Finishes*
- [49] JEDEC JESD89A, *Measurement and Reporting of Alpha Particle and Terrestrial Cosmic Ray-Induced Soft Errors in Semiconductor Devices. Arlington, VA 22201-2107. 2012-01*
- [50] Michael Nicolaidis - *Soft Errors in Modern Electronic Systems*, Springer 2011