

	Sicherheit von Maschinen Sicherheitsbezogene Teile von Steuerungen Teil 2: Validierung (ISO 13849-2:2003) Deutsche Fassung EN ISO 13849-2:2003	DIN EN ISO 13849-2
--	--	-------------------------------------

ICS 13.110

Safety of machinery —
 Safety-related parts of control systems —
 Part 2: Validation (ISO 13849-2:2003);
 German version EN ISO 13849-2:2003

Sécurité des machines —
 Parties des systèmes de commande relatives à la sécurité —
 Partie 2: Validation (ISO 13849-2:2003);
 Version allemande EN ISO 13849-2:2003

Die Europäische Norm EN ISO 13849-2:2003 hat den Status einer Deutschen Norm.

Beginn der Gültigkeit

EN ISO 13849-2:2003 wurde am 10. April 2003 angenommen.

Nationales Vorwort

Diese Norm enthält sicherheitstechnische Festlegungen im Sinne des Gerätesicherheitsgesetzes.

Diese Norm beinhaltet die Deutsche Fassung der von der Arbeitsgruppe 6 „Sichere Steuerungen“ des Technischen Komitees 114 „Sicherheit von Maschinen und Geräten“ des Europäischen Komitees für Normung (CEN) in Zusammenarbeit mit dem Technischen Komitee 44X „Sicherheit von Maschinen und Anlagen — Elektrotechnische Aspekte“ des Europäischen Komitees für Elektrotechnische Normung (CENELEC) und dem Technischen Komitee ISO/TC 199 „Sicherheit von Maschinen“ ausgearbeitete Norm EN ISO 13849-2:2003.

Die nationalen Interessen wurden dabei vom Gemeinschaftsausschuss GA 1.2 „Steuerungen“ des Normenausschusses Sicherheitstechnische Grundsätze (NASG) im DIN wahrgenommen.

Die in Abschnitt 2 zitierten Europäischen Normen wurden als DIN-EN-Normen mit gleicher Zählnummer veröffentlicht.

Fortsetzung 58 Seiten EN

Normenausschuss Sicherheitstechnische Grundsätze (NASG) im DIN Deutsches Institut für Normung e. V.
 Normenausschuss Maschinenbau (NAM) im DIN

— Leerseite —

Deutsche Fassung

Sicherheit von Maschinen
Sicherheitsbezogene Teile von Steuerungen
Teil 2: Validierung
(ISO 13849-2:2003)

Safety of machinery —
Safety-related parts of control systems —
Part 2: Validation (ISO 13849-2:2003)

Sécurité des machines —
Parties des systèmes de commande relatives à la sécurité —
Partie 2: Validation (ISO 13849-2:2003)

Diese Europäische Norm wurde vom CEN am 10. April 2003 angenommen.

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

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

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Portugal, Schweden, Schweiz, der Slowakei, Spanien, der Tschechischen Republik, Ungarn und dem Vereinigten Königreich.



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

Management-Zentrum: rue de Stassart, 36 B-1050 Brüssel

Inhalt

	Seite
Vorwort	3
Einleitung	4
1 Anwendungsbereich	4
2 Normative Verweisungen	4
3 Validierungsverfahren	5
3.1 Validierungsleitsätze	5
3.2 Allgemeine Fehlerlisten	6
3.3 Spezielle Fehlerlisten	7
3.4 Validierungsplan	7
3.5 Hinweise für die Validierung	8
3.6 Validierungsaufzeichnung	9
4 Validierung durch Analyse	9
4.1 Allgemeines	9
4.2 Analysentechniken	10
5 Validierung durch Prüfen	10
5.1 Allgemeines	10
5.2 Messunsicherheit	11
5.3 Höherwertige Festlegungen	11
5.4 Anzahl der Prüflinge	12
6 Validierung der Sicherheitsfunktionen	12
7 Validierung der Kategorien	12
7.1 Analyse und Prüfung der Kategorien	12
7.2 Validierung der Festlegungen für Kategorien	13
7.3 Validierung der Kombination von sicherheitsbezogenen Teilen	14
8 Validierung der Umgebungsanforderungen	14
9 Validierung der Instandhaltungsanforderungen	15
Anhang A (informativ) Möglichkeiten zur Validierung mechanischer Systeme	16
Anhang B (informativ) Möglichkeiten zur Validierung pneumatischer Systeme	21
Anhang C (informativ) Möglichkeiten zur Validierung hydraulischer Systeme	33
Anhang D (informativ) Möglichkeiten zur Validierung elektrischer Systeme	43
Anhang ZA (informativ) Zusammenhang dieses Dokuments mit EU-Richtlinien	56
Literaturhinweise	57

Vorwort

Dieses Dokument EN ISO 13849-2:2003 wurde vom Technischen Komitee CEN/TC 114 „Sicherheit von Maschinen“, dessen Sekretariat vom DIN gehalten wird, in Zusammenarbeit mit dem Technischen Komitee ISO/TC 199 „Sicherheit von Maschinen“ erarbeitet.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Februar 2004, und etwaige entgegenstehende nationale Normen müssen bis Februar 2004 zurückgezogen werden.

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

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

Die Anhänge A bis D sind informativer Art und strukturiert wie in Tabelle 1 angegeben.

Tabelle 1 — Aufbau der Abschnitte der Anhänge A bis D

Anhang	Technologie	Liste der grundlegenden Sicherheitsprinzipien	Liste der bewährten Sicherheitsprinzipien	Liste der bewährten Bauteile	Fehlerlisten und Fehlerausschlüsse
		Abschnitt			
A	Mechanik	A.2	A.3	A.4	A.5
B	Pneumatik	B.2	B.3	B.4	B.5
C	Hydraulik	C.2	C.3	C.4	C.5
D	Elektrik (einschließlich Elektronik)	D.2	D.3	D.4	D.5

Dieses Dokument enthält Literaturhinweise.

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

- Teil 1: Allgemeine Gestaltungsgrundsätze;
- Teil 2: Validierung;
- Teil 100: Leitfaden für Benutzung und Anwendung der EN ISO 13849-1.

Entsprechend der CEN/CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Portugal, Schweden, Schweiz, Slowakei, Spanien, Tschechische Republik, Ungarn und Vereinigtes Königreich.

Einleitung

Für die Benutzung in der Europäischen Union hat dieser Teil der EN ISO 13849 den Status einer allgemeinen Sicherheitsnorm (Typ B 1).

Diese Europäische Norm legt das Validierungsverfahren, einschließlich der beiden Verfahren Analyse und Prüfung, für die Sicherheitsfunktionen und Kategorien von sicherheitsbezogenen Teilen von Steuerungen fest. Beschreibungen der Sicherheitsfunktionen und die Anforderungen für die Kategorien sind in EN 954-1 (ISO 13849-1) gegeben, die sich mit den allgemeinen Leitsätzen für die Gestaltung befasst. Einige Anforderungen für die Validierung sind allgemeiner und einige spezifischer Art entsprechend der angewendeten Technologie. ISO 13849-2 legt auch die Bedingungen fest, unter welchen die Validierung beim Testen der sicherheitsbezogenen Teile von Steuerungen durchgeführt werden sollte.

EN 954-1 (ISO 13849-1) legt die Sicherheitsanforderungen fest und gibt Anleitung für die Leitsätze bei der Gestaltung [siehe EN 292-1:1991 (ISO/TR 12100:1992), 3.11] der sicherheitsbezogenen Teile von Steuerungen. Sie legt für diese Teile die Kategorie fest und beschreibt die speziellen Eigenschaften ihrer Sicherheitsfunktionen unabhängig von der verwendeten Energieart. Zusätzliche Hinweise zu EN 954-1 (ISO 13849-1) sind in CR 954-100 (ISO/TR 13849-100) enthalten.

Das Erreichen der Anforderungen kann durch alle möglichen Kombinationen der Analyse (siehe Abschnitt 4) und der Prüfung (siehe Abschnitt 5) validiert werden. Mit der Analyse sollte so früh wie möglich und gleichzeitig im Gestaltungsprozess begonnen werden.

1 Anwendungsbereich

Diese Europäische Norm legt die Vorgehensweisen und Bedingungen in Übereinstimmung mit EN 954-1 (ISO 13849-1) fest, die bei der Validierung durch Analyse und Prüfung zu befolgen sind, für

- die vorgesehenen Sicherheitsfunktionen und
- die ausgeführten Kategorien

der sicherheitsbezogenen Teile von Steuerungen, bei Anwendung der durch den Konstrukteur vorgesehenen sinnvollen Gestaltung.

Diese Europäische Norm gibt keine vollständigen Validierungsanforderungen für programmierbare elektronische Systeme und kann deshalb die Anwendung anderer Normen erfordern.

ANMERKUNG CEN/TC 114/WG 6 schlägt vor, sich eingehender mit der Validierung von programmierbaren elektronischen Systemen bei der Erarbeitung der Änderung der EN 954-1 (ISO 13849-1) zu befassen. Eine Anwendungsnorm für Maschinen (Entwurf IEC 62061), der die IEC 61508 zu Grunde liegt, wird zurzeit erarbeitet. Die Anforderungen für programmierbare elektronische Systeme, einschließlich der damit verbundenen Software, sind in IEC 61508 enthalten.

2 Normative Verweisungen

Diese Europäische Norm enthält durch datierte oder undatierte Verweisungen Festlegungen aus anderen Publikationen. Diese normativen Verweisungen sind an den jeweiligen Stellen im Text zitiert, und die Publikationen sind nachstehend aufgeführt. Bei datierten Verweisungen gehören spätere Änderungen oder Überarbeitungen dieser Publikationen nur zu dieser Europäischen Norm, falls sie durch Änderung oder Überarbeitung eingearbeitet sind. Bei undatierten Verweisungen gilt die letzte Ausgabe der in Bezug genommenen Publikation (einschließlich Änderungen).

EN 292-1:1991 (ISO/TR 12100:1992), *Sicherheit von Maschinen — Grundbegriffe, allgemeine Gestaltungsleitsätze — Teil 1: Grundsätzliche Terminologie, Methodologie.*

EN 954-1:1996 (ISO 13849-1:1999), *Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen — Teil 1: Allgemeine Gestaltungsleitsätze.*

3 Validierungsverfahren

3.1 Validierungsleitsätze

Der Zweck des Validierungsverfahrens ist, die Spezifikation und die Konformität der Gestaltung der sicherheitsbezogenen Teile der Steuerung innerhalb der Gesamtspezifikationen für die Sicherheitsanforderungen an der Maschine zu bestätigen.

Die Validierung muss aufzeigen, dass jedes sicherheitsbezogene Teil die Anforderungen von EN 954-1 (ISO 13849-1) erfüllt, insbesondere bei

- den festgelegten Sicherheitseigenschaften der Sicherheitsfunktionen für diesen Teil, wie in der sinnvollen Gestaltung realisiert, und
- den Anforderungen für die festgelegte Kategorie [siehe EN 954-1:1996 (ISO 13849-1:1999), Abschnitt 6].

Die Validierung sollte von Personen ausgeführt werden, die von der Gestaltung der sicherheitsbezogenen Teile unabhängig sind.

ANMERKUNG Unabhängige Person bedeutet nicht notwendigerweise, dass eine Prüfung durch eine dritte Partei erforderlich ist.

Der Grad der Unabhängigkeit sollte die sicherheitstechnische Leistungsfähigkeit des sicherheitsbezogenen Teiles widerspiegeln.

Die Validierung besteht aus der Durchführung der Analyse (siehe Abschnitt 4) und, soweit notwendig, aus der Durchführung von Prüfungen (siehe Abschnitt 5) in Übereinstimmung mit dem Validierungsplan. Bild 1 gibt einen Überblick über das Validierungsverfahren. Die Abwägung zwischen Analyse und/oder Prüfung hängt von der Technologie ab.

Mit der Analyse sollte so früh wie möglich und gleichzeitig mit dem Gestaltungsprozess begonnen werden, so dass Probleme frühzeitig korrigiert werden können, in einem Stadium, in dem sie relativ leicht korrigierbar sind, d. h. im Rahmen der Schritte 3 und 4 der EN 954-1:1996 (ISO 13849-1:1999), 4.3. Für einige Analysen kann es notwendig sein, sie solange hinauszuschieben, bis die Gestaltung gut entwickelt ist.

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

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

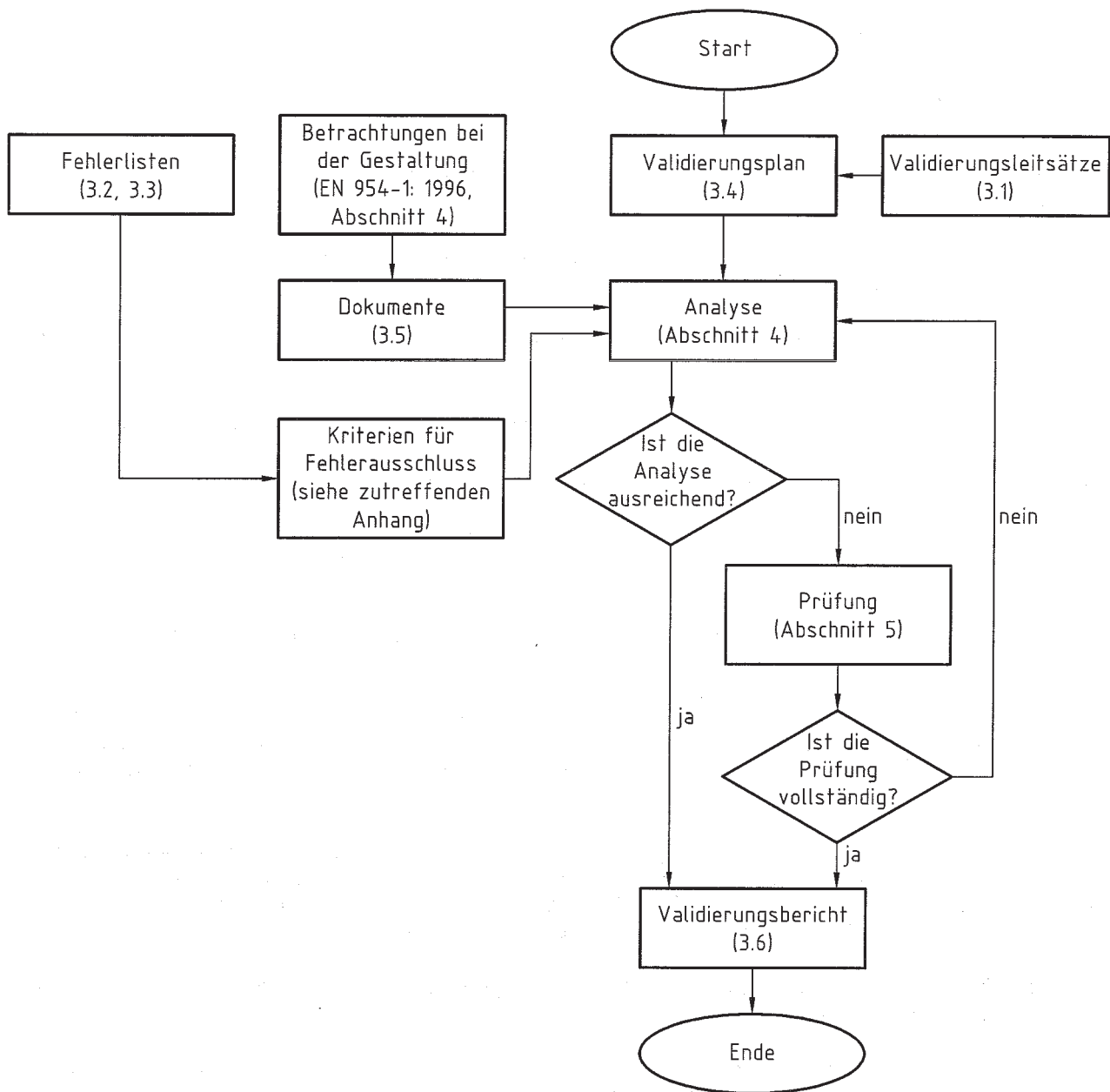


Bild 1 — Übersicht über das Validierungsverfahren

3.2 Allgemeine Fehlerlisten

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

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

Nur permanente Fehler sind berücksichtigt.

3.3 Spezielle Fehlerlisten

Eine spezielle auf das Produkt bezogene Fehlerliste muss als Bezugsdokument für das Validierungsverfahren für die sicherheitsbezogenen Teile erstellt werden. Dieser Liste müssen die entsprechenden allgemeinen Listen in den Anhängen zu Grunde liegen.

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

- die aus den allgemeinen Listen einbezogenen Fehler;
 - alle anderen relevanten einbezogenen Fehler, die nicht in der allgemeinen Liste aufgeführt sind (z. B. Fehler gemeinsamer Ursache);
 - die aus der allgemeinen Liste entnommenen Fehler, die ausgeschlossen werden dürfen und schließlich die Kriterien befriedigen können, die in den allgemeinen Listen enthalten sind [siehe EN 954-1:1996 (ISO 13849-1:1999), 7.2],
- und, ausnahmsweise
- alle anderen relevanten Fehler aus der allgemeinen Liste, für die die allgemeine Liste jedoch einen Ausschluss nicht zulässt, zusammen mit einer Begründung und sinnvollen Erklärung für ihren Ausschluss [siehe EN 954-1:1996 (ISO 13849-1:1999), 7.2].

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

3.4 Validierungsplan

Der Validierungsplan muss die Anforderungen für die Durchführung des Validierungsverfahrens für die festgelegten Sicherheitsfunktionen und ihrer Kategorien identifizieren und beschreiben.

Der Validierungsplan muss auch die Mittel identifizieren, die zu benutzen sind, um die festgelegten Sicherheitsfunktionen und Kategorien zu validieren. Wo es angemessen ist, muss er darlegen:

- a) die Identität der Dokumente für die Festlegungen;
- b) die Betriebs- und Umgebungsbedingungen;
- c) die grundlegenden Sicherheitsprinzipien (siehe A.2, B.2, C.2 und D.2);
- d) die bewährten Sicherheitsprinzipien (siehe A.3, B.3, C.3 und D.3);
- e) die bewährten Bauteile (siehe A.4 und D.4);
- f) die Fehlerannahmen und Fehlerausschlüsse, die z. B. aus den informativen Fehlerlisten in A.5, B.5, C.5 und D.5 zu berücksichtigen sind;
- g) die Analysen und Prüfungen, die angewandt wurden.

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

3.5 Hinweise für die Validierung

Die Hinweise, die für die Validierung erforderlich sind, unterscheiden sich hinsichtlich der angewendeten Technologie, der Kategorie(n), die aufzuzeigen sind, der sinnvollen Gestaltung des Systems und hinsichtlich des Beitrages der sicherheitsbezogenen Teile der Steuerung für die Risikoverringerung. Dokumente, die in ausreichendem Maße die Hinweise aus unten stehender Liste beinhalten, müssen im Validierungsverfahren aufgenommen sein, um die erreichten Kategorie(n) und die Sicherheitsfunktion(en) der sicherheitsbezogenen Teile aufzuzeigen:

- a) Spezifikationen über die angenommene Leistungsfähigkeit der Sicherheitsfunktionen und Kategorien;
- b) Zeichnungen und Spezifikationen, z. B. für mechanische, hydraulische und pneumatische Teile, gedruckte Steuerkreisläne, Montagepläne, interne Verdrahtung, Gehäuse, Materialien, Aufstellung;
- c) Blockdiagramm(e) mit Funktionsbeschreibung der Blöcke;
- d) Steuerkreisdigramm(e) einschließlich ihrer Verknüpfungen/Verbindungen;
- e) Funktionsbeschreibung der Steuerkreisdigramme;
- f) Zeitfolgediagramm(e) für schaltende Bauteile, für Signale, die für die Sicherheit zuständig sind;
- g) Beschreibung der relevanten Eigenschaften von früher validierten Bauteilen;
- h) für andere sicherheitsbezogene Teile (ausgenommen der unter g) aufgelisteten) die Bauteillisten mit Stückbezeichnung, Nennwerten, Toleranzen, relevanten Betriebsbeanspruchungen, Typ-Bezeichnungen, Daten über Fehlerraten und Bauteilhersteller und alle anderen Daten, die für die Sicherheit maßgebend sind;
- i) Analyse aller relevanten Fehler (siehe auch 3.2), die in z. B. A.5, B.5, C.5 und D.5 aufgelistet sind, einschließlich der Begründung aller ausgeschlossenen Fehler;
- j) Analyse des Einflusses der im Verfahren verwendeten Materialien;
- k) spezielle Information für die Kategorie nach Tabelle 2;

Wo angebracht, muss die Software-Dokumentation beinhalten:

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

Tabelle 2 — Anforderungen an die Dokumentation für Kategorien

Anforderungen an die Dokumentation	Kategorie, für die eine Dokumentation erforderlich ist				
	B	1	2	3	4
grundlegende Sicherheitsprinzipien	x	x	x	x	x
zu erwartende Betriebsbeanspruchungen	x	x	x	x	x
Einfluss des zu verarbeitenden Materials	x	x	x	x	x
Leistungsfähigkeit während anderer relevanter externer Einflüsse	x	x	x	x	x
bewährte Bauteile	—	x	—	—	—
bewährte Sicherheitsprinzipien	—	x	x	x	x
das Testverfahren für die Sicherheitsfunktion(en)	—	—	x	—	—
Testintervalle, wenn festgelegt	—	—	x	—	—
bei der Gestaltung berücksichtigte vorhersehbare Einzelfehler und das angewendete Erkennungsverfahren	—	—	—	x	x
die identifizierten Fehler gemeinsamer Ursache und wie sie verhindert werden	—	—	—	x	x
die vorhersehbaren ausgeschlossenen Einzelfehler	—	—	—	x	x
Fehler, die zu erkennen sind	—	—	x	x	x
verschiedene Fehleranhäufungen, die bei der Gestaltung zu berücksichtigen sind	—	—	—	—	x
wie die Sicherheitsfunktion in jedem Fehlerfall aufrechterhalten bleibt	—	—	—	x	x
wie die Sicherheitsfunktion bei allen Fehlerkombinationen aufrechterhalten bleibt	—	—	—	—	x

ANMERKUNG Die in Tabelle 2 genannten Kategorien entsprechen denen, die in EN 954-1 (ISO 13849-1) angegeben sind.

3.6 Validierungsaufzeichnung

Die Validierung durch Analyse und Prüfung muss aufgezeichnet werden. Die Aufzeichnung muss das Validierungsverfahren aller sicherheitstechnischen Anforderungen ersichtlich machen. Es können Querverweise zu anderen Dokumenten gemacht werden, vorausgesetzt sie sind richtig identifiziert.

Für jedes sicherheitsbezogene Teil, das einen Teil des Validierungsverfahrens nicht bestanden hat, muss die Aufzeichnung den Teil (die Teile) beschreiben, die die Validierungsprüfungen und/oder -analysen nicht bestanden haben.

4 Validierung durch Analyse

4.1 Allgemeines

Die Validierung von sicherheitsbezogenen Teilen von Steuerungen muss durch eine Analyse erfolgen. In die Analyse gehen ein:

- die identifizierten Gefährdungen, die sich bei der Analyse an der Maschine ergeben [siehe EN 954-1:1996 (ISO 13849-1:1999), Bild 1];
- die Zuverlässigkeit [siehe EN 954-1:1996 (ISO 13849-1:1999), 4.2];
- die Systemstruktur [siehe EN 954-1:1996 (ISO 13849-1:1999), 4.2];
- die nicht quantifizierbaren qualitativen Aspekte, die Auswirkung auf das Systemverhalten haben [siehe EN 954-1:1996 (ISO 13849-1:1999), 4.2];
- deterministische Argumente.

Bei der Validierung der Sicherheitsfunktionen durch Analyse ist weit mehr als bei der Prüfung die Festlegung von deterministischen Argumenten erforderlich. Deterministische Argumente unterscheiden sich von anderen Beweisführungen dadurch, dass sie zeigen, dass die geforderten Eigenschaften des Systems einem Systemmodell logisch folgen. Solche Argumente können auf der Grundlage einfacher, gut verständlicher Begriffe entwickelt werden, wie z. B. die Genauigkeit einer mechanischen Verriegelung.

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

4.2 Analystechniken

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

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

Weitere Informationen zu Analysemethoden enthält EN 1050:1996 (ISO 14121:1999), Anhang B.

5 Validierung durch Prüfen

5.1 Allgemeines

Wenn die Validierung durch Analyse nicht ausreichend das Erreichen der festgelegten Sicherheitsfunktionen und Kategorien zeigt, müssen Prüfungen durchgeführt werden, um die Validierung zu vervollständigen. Eine Prüfung ist immer zusätzlich zur Analyse durchzuführen und ist oft notwendig.

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

- a) Vor Beginn der Prüfungen muss ein Prüfplan ausgearbeitet werden, der Folgendes beinhalten muss:
 - 1) die Prüfspezifikationen;
 - 2) die zu erwartenden Ergebnisse der Prüfungen;
 - 3) die Reihenfolge der Prüfungen.
- b) Prüfaufzeichnungen müssen erstellt werden, die Folgendes beinhalten:
 - 1) den Namen des Prüfers;
 - 2) die Umgebungsbedingungen (siehe Abschnitt 8);
 - 3) die Vorgehensweisen bei der Prüfung und die benutzten Ausrüstungen;
 - 4) die Ergebnisse der Prüfungen.
- c) Die Prüfaufzeichnungen müssen mit dem Prüfplan verglichen werden, um Gewissheit zu erhalten, dass die festgelegten Funktions- und Leistungsziele erreicht sind.

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

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

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

Es wird empfohlen, dass die Kombination dieser Eingangssignale systematisch der Steuerung und der Maschine anzupassen ist. Ein Beispiel für diese Logik ist: Energie einschalten, starten, Arbeitsablauf, Richtungsumkehr, Wiederanlauf. Wo notwendig, muss eine erweiterte Anzahl Eingangsdaten eingegeben werden, um anormale oder ungewöhnliche Situationen zu berücksichtigen, und um zu sehen, wie die sicherheitsbezogenen Teile der Steuerung reagieren. Solche Kombinationen von Eingangsdaten müssen vorhersehbare inkorrekte Abläufe berücksichtigen.

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

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

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

5.2 Messunsicherheit

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

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

Abweichungen von diesen Messunsicherheiten müssen begründet werden.

5.3 Höherwertige Festlegungen

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

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

5.4 Anzahl der Prüflinge

Soweit nicht anderweitig festgelegt, müssen die Prüfungen an einem einzelnen Muster der sicherheitsbezogenen Teile durchgeführt werden, das allen relevanten Prüfungen standhalten sollte.

Sicherheitsbezogene Teile, die sich in der Prüfung befinden, dürfen während des Prüfablaufes nicht verändert werden.

Einige Prüfungen können dauerhaft die Leistungsfähigkeit einiger Bauteile verändern. Wo die dauerhafte Veränderung in den Bauteilen der Grund dafür ist, dass die sicherheitsbezogenen Teile außerhalb der Gestaltungsspezifikationen liegen, müssen weitere Muster für nachfolgende Prüfungen benutzt werden.

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

6 Validierung der Sicherheitsfunktionen

Ein wichtiger Schritt ist die Validierung der Sicherheitsfunktionen auf vollständige Übereinstimmung der vorgesehenen Teile der Steuerung mit ihren spezifischen Eigenschaften. Im Validierungsprozess ist es wichtig, Fehler und insbesondere Auslassungen in der formulierten Spezifikation, die in einer sinnvollen Konstruktion anzunehmen sind, zu überprüfen.

Das Ziel der Validierung von Sicherheitsfunktionen ist sicherzustellen, dass sicherheitsbezogene Ausgangssignale abhängig von den Eingangssignalen entsprechend den Festlegungen korrekt und logisch sind. Die Validierung sollte alle normalen und vorhersehbaren abnormalen Bedingungen durch statische und dynamische Simulation abdecken.

Die festgelegten Sicherheitsfunktionen [nach EN 954-1:1996 (ISO 13849-1:1999), Abschnitt 5] müssen in allen Betriebsarten der Maschine validiert werden. Das heißt: die Validierung muss durchgeführt werden, um die korrekte Funktion

- bei verschiedenen Konfigurationen zu demonstrieren und um ausreichend sicherzustellen, dass alle sicherheitsbezogenen Ausgangssignale über ihren gesamten Bereich umgesetzt sind. Prüfungen (z. B. Überlastprüfungen) können notwendig sein, um die festgelegten Sicherheitsfunktionen zu validieren;
- durch Reaktion auf vorhersehbare abnormale Signale von irgendeiner Eingangsquelle unter Einbeziehung der Energieunterbrechung und –wiederkehr zu demonstrieren.

ANMERKUNG Wo es angebracht ist, sollten Kombinationen von verschiedenen Konfigurationen berücksichtigt werden.

7 Validierung der Kategorien

7.1 Analyse und Prüfung der Kategorien

Die Validierung der Kategorien muss zeigen, dass ihre Anforderungen erfüllt sind. Grundsätzlich sind die folgenden Verfahren anwendbar:

- eine Analyse der Steuerkreisdigramme (siehe Abschnitt 4);
- Prüfungen bei den tatsächlich vorhandenen Steuerkreisen und Fehlersimulation an den tatsächlich vorhandenen Bauteilen, besonders in zweifelhaften Bereichen, hinsichtlich der bei der Analyse festgestellten Leistungsfähigkeit (siehe Abschnitt 5);
- eine Simulation des Verhaltens der Steuerung, z. B. mit Mitteln von Hardware- und/oder Softwaremodellen.

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

Bei der Durchführung der Validierung durch Prüfung, können die Prüfungen, sofern angemessen, beinhalten:

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

Der genaue Zeitpunkt, bei dem ein Fehler in ein System eingegeben wird, kann kritisch sein. Der „worst case effect“ bei einer Fehlereingabe sollte anhand einer Analyse bestimmt werden und der Fehler sollte entsprechend dieser Analyse bei der angemessenen kritischen Zeit eingegeben werden.

7.2 Validierung der Festlegungen für Kategorien

7.2.1 Kategorie B

Die sicherheitsbezogenen Teile von Steuerungen der Kategorie B müssen in Übereinstimmung mit den grundlegenden Sicherheitsprinzipien validiert werden (siehe A.2, B.2, C.2 und D.2) durch Aufzeigen, dass die Spezifikation, die Gestaltung, Konstruktion und Wahl der Bauteile mit EN 954-1:1996 (ISO 13849-2:1999), 6.2.1 übereinstimmen. Dies muss durch Prüfung so erreicht werden, dass die sicherheitsbezogenen Teile der Steuerung, so wie in den Dokumenten für die Validierung vorgesehen, in Übereinstimmung mit ihren Spezifikationen sind (siehe 3.5). Für die Validierung der Umgebungsbedingungen siehe 5.1.

7.2.2 Kategorie 1

Die sicherheitsbezogenen Teile von Steuerungen der Kategorie 1 müssen validiert werden, um aufzuzeigen, dass:

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

Zutreffende Bauteilnormen können benutzt werden, um die Übereinstimmung mit diesem Unterabschnitt aufzuzeigen (siehe A.4 bis D.4).

7.2.3 Kategorie 2

Sicherheitsbezogene Teile von Steuerungen der Kategorie 2 müssen validiert werden, um aufzuzeigen, dass:

- a) sie die Anforderungen der Kategorie B erfüllen;
- b) die angewandten bewährten Sicherheitsprinzipien (sofern anwendbar) die Anforderungen von 7.2.2 c) erfüllen;

- c) die Testeinrichtung alle relevanten Fehler erkennt, die nacheinander während des Testablaufs berücksichtigt werden, und eine angemessene Reaktion der Steuerung bewirkt, die:
 - 1) einen sicheren Zustand einleitet, oder wenn das nicht möglich ist,
 - 2) eine Warnung vor der Gefährdung vorsieht;
- d) die mit der Testeinrichtung durchgeführten Prüfungen nicht in einen unsicheren Zustand führen;
- e) die Einleitung des Tests durchgeführt wird:
 - 1) beim Anlauf der Maschine und vor der Einleitung einer gefährlichen Situation, und
 - 2) periodisch während des Betriebs, wenn die Risikobeurteilung und die Art des Betriebs zeigen, dass dies notwendig ist.

7.2.4 Kategorie 3

Die sicherheitsbezogenen Teile von Steuerungen der Kategorie 3 müssen validiert werden, um aufzuzeigen, dass:

- a) sie die Anforderungen der Kategorie B erfüllen;
- b) die bewährten Sicherheitsprinzipien (wenn anwendbar) die Anforderungen von 7.2.2 c) erfüllen;
- c) ein Einzelfehler nicht zum Verlust der Sicherheitsfunktion führt;
- d) Einzelfehler (einschließlich Fehler gemeinsamer Ursache) in Übereinstimmung mit der sinnvollen Gestaltung erkannt werden.

7.2.5 Kategorie 4

Sicherheitsbezogene Teile von Steuerungen der Kategorie 4 müssen validiert werden, um aufzuzeigen, dass:

- a) sie die Anforderungen der Kategorie B erfüllen;
- b) die bewährten Sicherheitsprinzipien (wenn anwendbar) die Anforderungen von 7.2.2 c) erfüllen;
- c) ein Einzelfehler (einschließlich Fehler gemeinsamer Ursache) nicht zum Verlust der Sicherheitsfunktion führt;
- d) die Einzelfehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt werden;
- e) wenn d) nicht möglich ist, eine Anhäufung von Fehlern nicht zum Verlust der Sicherheitsfunktion(en) führt. Der in Betracht gezogene Umfang der Anhäufung von Fehlern muss in Übereinstimmung mit der sinnvollen Gestaltung sein.

7.3 Validierung der Kombination von sicherheitsbezogenen Teilen

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

8 Validierung der Umgebungsanforderungen

Die bei der Gestaltung festgelegte Leistungsfähigkeit von sicherheitsbezogenen Teilen der Steuerung muss unter Berücksichtigung der festgelegten Umgebungsbedingungen für die Steuerung validiert werden.

Die Validierung muss durch Analyse durchgeführt werden und wenn nötig durch Prüfung. Der Umfang der Analyse und Prüfung hängt ab von den sicherheitsbezogenen Teilen, dem System, in dem sie eingebaut sind, der angewandten Technologie und den Umgebungsbedingungen, die validiert werden. Die Anwendung von

Betriebszuverlässigkeitsdaten des Systems oder seiner Bauteile, oder die Bestätigung der Übereinstimmung mit den entsprechenden Umgebungsnormen (z. B. für die Wasserdichtigkeit, Vibrationsschutz) können den Validierungsprozess unterstützen.

Wo anwendbar, muss sich die Validierung beziehen auf:

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

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

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

9 Validierung der Instandhaltungsanforderungen

Das Validierungsverfahren muss aufzeigen, dass die Instandhaltungsanforderungen, wie sie in EN 954-1:1996 (ISO 13849-2:1999), Abschnitt 9, Absatz 2, festgelegt sind, einbezogen wurden.

Anhang A (informativ)

Möglichkeiten zur Validierung mechanischer Systeme

Inhalt

	Seite
Anhang A (informativ) Möglichkeiten zur Validierung mechanischer Systeme	16
A.1 Einleitung	16
A.2 Liste der grundlegenden Sicherheitsprinzipien	16
A.3 Liste der bewährten Sicherheitsprinzipien	18
A.4 Liste der bewährten Bauteile	19
A.5 Fehlerlisten und Fehlerausschlüsse	20
A.5.1 Einleitung	20
A.5.2 Verschiedene mechanische Geräte, Bauteile, Elemente	20
A.5.3 Schraubendruckfedern	20

A.1 Einleitung

Bei Anwendung mechanischer Systeme in Verbindung mit anderen Technologien sollten auch die zutreffenden Tabellen für grundlegende und bewährte Sicherheitsprinzipien berücksichtigt werden. Für weitere Fehlerausschlüsse siehe 3.3.

A.2 Liste der grundlegenden Sicherheitsprinzipien

Tabelle A.1 — Grundlegende Sicherheitsprinzipien

Grundlegende Sicherheitsprinzipien	Bemerkungen
Anwendung geeigneter Werkstoffe und Herstellungsverfahren	Auswahl des Werkstoffs, der Herstellungs- und Behandlungsverfahren unter Berücksichtigung von z. B. Spannungen, Haltbarkeit, Elastizität, Reibung, Verschleiß, Korrosion, Temperatur.
richtige Dimensionierung und Formgebung	Berücksichtigen z. B. von Spannung, Dehnung, Ermüdung, Oberflächenrauheit, Toleranzen, Hängenbleiben, Herstellungsverfahren.
geeignete Auswahl, Kombination, Anordnungen, Zusammenbau und Einbau der Bauteile/des Systems	Berücksichtigen von Anwendungshinweisen des Herstellers, z. B. Katalogblätter, Einbauanweisungen, Spezifikationen, sowie von Erfahrungen mit ähnlichen Bauteilen/Systemen.
Anwendung des Prinzips der Energietrennung	Der sichere Zustand wird durch Abtrennung von der Energiequelle erreicht. Siehe Primärmaßnahme zum Anhalten in EN 292-2:1991 (ISO/TR 12100-2:1992), 3.7.1. Zum Starten der Bewegung eines Mechanismus wird Energie benötigt. Siehe Primärmaßnahme zum Starten in EN 292-2:1991 (ISO/TR 12100-2:1992), 3.7.1. Berücksichtigen von unterschiedlichen Betriebsarten, z. B. Betriebsmodus, Instandhaltungsmodus. Dieses Prinzip darf bei speziellen Anwendungen nicht benutzt werden, z. B., wenn die Energie für Spanneinrichtungen aufrechtzuhalten ist.