

Sicherheit von Maschinen
Sicherheitsbezogene Teile von Steuerungen
 Teil 1: Allgemeine Gestaltungsgrundsätze
 Deutsche Fassung EN 954-1 : 1996

DIN
EN 954-1

ICS 13.110

Deskriptoren: Sicherheitstechnik, Maschine, Steuerung, Gestaltung, Leitsatz

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

Part 1: General principles for design;

German version EN 954-1 : 1996

Sécurité des machines – Parties des systèmes de commande relatives à la sécurité –

Partie 1: Principes généraux de conception;

Version allemande EN 954-1 : 1996

Die Europäische Norm EN 954-1 : 1996 hat den Status einer Deutschen Norm.

Beginn der Gültigkeit

EN 954-1 : 1996 wurde am 1996-07-11 angenommen.

Nationales Vorwort

Diese Norm enthält sicherheitstechnische Festlegungen im Sinne des Gerätesicherheitsgesetzes.

Diese Norm beinhaltet die Deutsche Fassung der von der gemeinsamen Arbeitsgruppe 6 "Sichere Steuerungen" des Technischen Komitees 114 "Sicherheit von Maschinen, Geräten und Anlagen" des Europäischen Komitees für Normung (CEN) und des Technischen Komitees 44X "Sicherheit von Maschinen und Anlagen; Elektrotechnische Aspekte" des Europäischen Komitees für Elektrotechnische Normung (CENELEC) ausgearbeiteten Norm EN 954-1 : 1996.

Die Deutsche Fassung wurde vom Gemeinschaftsausschuß 2 "Steuerungen" des Normenausschusses Sicherheitstechnische Grundsätze (NASG) im DIN erstellt.

Für die im Abschnitt 2 zitierten Europäischen und Internationalen Normen wird, soweit die Norm-Nummer geändert ist, im folgenden auf die entsprechenden Deutschen Normen hingewiesen:

EN 60529 siehe DIN VDE 0470-1 (VDE 0470 Teil 1)

IEC 50(191) siehe IEC Kapitel 191

IEC 68 siehe Normen der Reihe DIN IEC 68

IEC 801-1 siehe DIN VDE 0843-1 (VDE 0843 Teil 1)

Nationaler Anhang NA (informativ)

Literaturhinweise

Normen der Reihe

DIN IEC 68

Grundlegende Prüfverfahren

DIN VDE 0470-1 (VDE 0470 Teil 1)

Schutzarten durch Gehäuse (IP Code); [IEC 529 (1989). 2. Ausgabe]; Deutsche Fassung EN 60529 : 1991

DIN VDE 0843-1 (VDE 0843 Teil 1)

Elektromagnetische Verträglichkeit von Meß-, Steuer- und Regeleinrichtungen in der industriellen Prozeßtechnik – Allgemeine Einführung; Identisch mit IEC 801-1, Ausgabe 1984

IEV Kapitel 191

Internationales Elektrotechnisches Wörterbuch – Kapitel 191: Zuverlässigkeit und Dienstgüte; Identisch mit IEC 50(191) : 1990

Fortsetzung 21 Seiten EN

Normenausschuß Sicherheitstechnische Grundsätze (NASG) im DIN Deutsches Institut für Normung e. V.

Normenausschuß Maschinenbau (NAM) im DIN

Deutsche Elektrotechnische Kommission im DIN und VDE (DKE)

ICS 13.110

Deskriptoren: Sicherheit von Maschinen, Stellorgan, Ausführung, Zwischenfläche, Gefährdung, Grundsätzlich, Fehler, Qualitätsnachweis

Deutsche Fassung

Sicherheit von Maschinen

Sicherheitsbezogene Teile von Steuerungen

Teil 1: Allgemeine Gestaltungsleitsätze

Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design

Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1: Principes généraux de conception

Diese Europäische Norm wurde von CEN am 1996-07-11 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 Zentralsekretariat 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 Zentralsekretariat 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, Niederlande, Norwegen, Österreich, Portugal, Schweden, Schweiz, Spanien und dem Vereinigten Königreich.

CEN

EUROPÄISCHES KOMITEE FÜR NORMUNG

European Committee for Standardization

Comité Européen de Normalisation

Zentralsekretariat: rue de Stassart 36, B-1050 Brüssel

Inhalt

	Seite		Seite
Vorwort	2	8 Validieren	15
0 Einleitung	3	8.1 Allgemeines	15
1 Anwendungsbereich	3	8.2 Validierungsplan	15
2 Normative Verweisungen	3	8.3 Validieren durch Analyse	16
3 Definitionen	4	8.4 Validieren durch Prüfung	16
4 Allgemeine Betrachtungen	4	8.5 Validierungsbericht	16
4.1 Sicherheitstechnische Ziele bei der Gestaltung	4	9 Instandhaltung	16
4.2 Allgemeine Vorgehensweise bei der Gestaltung	4	10 Benutzerinformation	16
4.3 Prozeß für die Auswahl und Gestaltung von Sicherheitsmaßnahmen	5	Anhang A (informativ) Fragebogen zum Gestaltungsprozeß	17
4.4 Leitsätze für ergonomische Gestaltung	6	Anhang B (informativ) Hinweise zur Auswahl der Kategorien	18
5 Charakteristische Eigenschaften von Sicherheitsfunktionen	6	Anhang C (informativ) Liste einiger wichtiger Fehler und Ausfälle bei verschiedenen Technologien	20
6 Kategorien	12	Anhang D (informativ) Zusammenhang zwischen Sicherheit, Zuverlässigkeit und Verfügbarkeit von Maschinen	20
6.1 Allgemeines	12	Anhang E (informativ) Literaturhinweise	21
6.2 Festlegungen für Kategorien	12	Anhang ZA (informativ) Abschnitte in dieser Europäischen Norm, die grundlegende oder andere Vorgaben von EU-Richtlinien betreffen	21
6.3 Auswahl und Kombination von sicherheitsbezogenen Teilen verschiedener Kategorien	15		
7 Fehlerbetrachtung	15		
7.1 Allgemeines	15		
7.2 Fehlerausschluß	15		

Vorwort

Diese Europäische Norm wurde vom Technischen Komitee CEN/TC 114 "Sicherheit von Maschinen und Geräten" erarbeitet, dessen Sekretariat vom DIN gehalten wird.

Diese Europäische Norm muß den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Juni 1997, und etwaige entgegenstehende nationale Normen müssen bis Juni 1997 zurückgezogen werden.

Diese Norm hat den Status einer Anwendungsnorm (Typ B1) und stellt einen Leitfaden dar, der bei der Gestaltung und Beurteilung von Steuerungen sowie durch Technische Komitees zu verwenden ist, die Typ B2- oder Typ C-Normen erstellen, bei denen die Vermutung gegeben ist, daß sie mit den in Angang I der Richtlinie des Rates 89/392/EWG und Änderungs-Richtlinien 91/368/EWG und 93/44/EWG (siehe Anhang A der EN 292-2 : 1991/A1 : 1995) festgelegten grundlegenden sicherheitstechnischen Anforderungen übereinstimmen. Diese Norm gibt keine besondere Anleitung zur Übereinstimmung mit anderen EU-Richtlinien.

Zur Zeit der Vorlage dieses Teiles 1 in CEN ist ein Entwurf für einen Teil 2 mit folgendem vorläufigen Titel in Vorbereitung: "Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung" (siehe auch Abschnitte 7 und 8 dieses Teiles 1).

ANMERKUNG: Bei der Erarbeitung von Teil 2 sollen die in Bezug zur Maschinensicherheit stehenden Anforderungen der IEC 1508 ¹⁾ "Funktionssicherheit: sicherheitsbezogene Systeme" berücksichtigt werden.

Diese Europäische Norm wurde im Rahmen eines Mandates, das dem CEN von der Europäischen Kommission und der Europäischen Freihandelszone erteilt wurde, erarbeitet und unterstützt grundlegende Anforderungen der EU-Richtlinie(n).

Zusammenhang mit EU-Richtlinien siehe informativen Anhang ZA, der Bestandteil dieser Norm ist.

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, Niederlande, Norwegen, Österreich, Portugal, Schweden, Schweiz, Spanien und das Vereinigte Königreich.

¹⁾ Norm in Vorbereitung

0 Einleitung

Teilen von Maschinensteuerungen werden häufig Sicherheitsaufgaben übertragen: diese werden sicherheitsbezogene Teile genannt. Diese Teile können aus Hardware und Software bestehen, und sie übernehmen die Sicherheitsfunktionen von Steuerungen. Sie können getrennt ausgeführt oder integrierte Teile der Steuerung sein.

Die Leistungsfähigkeit eines sicherheitsbezogenen Teiles einer Steuerung beim Auftreten von Fehlern wird in dieser Norm in fünf Kategorien unterteilt (B, 1, 2, 3, 4), die als Bezugspunkte angewendet werden sollten. Diese Kategorien (siehe 6.2) sind nicht dazu bestimmt, in irgendeiner gegebenen Reihenfolge oder hierarchischen Anordnung in bezug auf die sicherheitstechnischen Anforderungen angewendet zu werden.

Die Kategorien können angewendet werden für:

- Steuerungen aller Maschinenarten, von einfachen Maschinen, z. B. kleinen Küchenmaschinen, bis zu komplexen Fertigungsanlagen, z. B. Verpackungsmaschinen, Druckmaschinen, Pressen;
- Steuerungen von Schutzeinrichtungen, z. B. Zweihandschaltungen, Verriegelungseinrichtungen, berührungslos wirkende Schutzeinrichtungen (z. B. Lichtschranken) und Schalmatten.

Die ausgewählte Kategorie ist abhängig von der Maschine und von dem Ausmaß, in dem Steuerungsmittel für die Schutzmaßnahmen eingesetzt werden.

Bei der Auswahl einer Kategorie und der Gestaltung eines sicherheitsbezogenen Teiles einer Steuerung ist es notwendig, daß der Konstrukteur mindestens folgende Information über das sicherheitsbezogene Teil angibt:

- die ausgewählte(n) Kategorie(n);
- die Funktionseigenschaften;
- die genaue Aufgabe, die es in bezug auf die Schutzmaßnahme(n) an Maschinen erfüllt;
- die genauen Grenzen (siehe 3.1);
- alle betrachteten sicherheitsbezogenen Fehler;
- solche sicherheitstechnisch zutreffenden, nicht durch Fehlerausschluß berücksichtigte Fehler sowie die angewendeten Maßnahmen, die ihren Ausschluß erlauben;
- die für die Zuverlässigkeit zutreffenden Parameter, wie Umgebungsbedingungen;
- die angewendete(n) Technologie(n).

Die Anwendung der Kategorien als Bezugspunkte und diese Angaben zur sinnvollen Vorgehensweise bei der Gestaltung sind dazu bestimmt, eine flexible Anwendung dieser Norm zu ermöglichen. Es ist beabsichtigt, eine klare Grundlage zur Beurteilung, z. B. durch Dritte, interne oder unabhängige Prüfstellen, sowohl der Gestaltung als auch der Leistungsfähigkeit des sicherheitsbezogenen Teiles einer Steuerung (und der Maschine) in einer beliebigen Anwendung zu schaffen.

1 Anwendungsbereich

Diese Europäische Norm enthält sicherheitstechnische Anforderungen und Hinweise auf Gestaltungsleitsätze (siehe 3.11 der EN 292-1 : 1991) von sicherheitsbezogenen Teilen von Steuerungen. Für diese Teile legt sie Kategorien fest und beschreibt Eigenschaften ihrer Sicherheitsfunktionen. Dies schließt programmierbare Systeme für alle Maschinen und darauf bezogene Schutzeinrichtungen ein. Sie gilt für alle sicherheitsbezogenen Teile von Steuerungen, unabhängig von der verwendeten Energieart, z. B. elektrisch, hydraulisch, pneumatisch, mechanisch. Sie legt nicht fest, welche Sicherheitsfunktionen und welche Kategorien im Einzelfall angewendet werden müssen.

Sie gilt für alle Maschinen im gewerblichen und nichtgewerblichen Bereich. Wo dies angebracht ist, kann diese Norm auch auf sicherheitsbezogene Teile von Steuerungen angewendet werden, die zu anderen technischen Zwecken verwendet werden.

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.

EN 292-1 : 1991

Sicherheit von Maschinen – Grundbegriffe, allgemeine Gestaltungsleitsätze – Teil 1: Grundsätzliche Terminologie, Methodologie

EN 292-2 : 1991/A1 : 1995

Sicherheit von Maschinen – Grundbegriffe, allgemeine Gestaltungsleitsätze – Teil 2: Technische Leitsätze und Spezifikationen

EN 418

Sicherheit von Maschinen – NOT-AUS-Einrichtung, funktionelle Aspekte – Gestaltungsleitsätze

EN 457

Sicherheit von Maschinen – Akustische Gefahrensignale – Allgemeine Anforderungen, Gestaltung und Prüfung (ISO 7731 : 1986 modifiziert)

EN 614-1

Sicherheit von Maschinen – Ergonomische Gestaltungsgrundsätze – Teil 1: Begriffe und allgemeine Leitsätze

EN 842

Sicherheit von Maschinen – Optische Gefahrensignale – Allgemeine Anforderungen, Gestaltung und Prüfung

EN 981

Sicherheit von Maschinen – System akustischer und optischer Gefahrensignale und Informationssignale

EN 982

Sicherheit von Maschinen – Sicherheitstechnische Anforderungen an fluidtechnische Anlagen und deren Bauteile – Hydraulik

EN 983

Sicherheit von Maschinen – Sicherheitstechnische Anforderungen an fluidtechnische Anlagen und deren Bauteile – Pneumatik

prEN 999 : 1995

Sicherheit von Maschinen – Anordnung von Schutzeinrichtungen im Hinblick auf die Annäherungsgeschwindigkeiten von Körperteilen

EN 1037

Sicherheit von Maschinen – Vermeidung von unerwartetem Anlauf

EN 1050 : 1996

Sicherheit von Maschinen – Leitsätze zur Risikobeurteilung

EN 60204-1 : 1992

Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen – Teil 1: Allgemeine Anforderungen (IEC 204-1 : 1992, modifiziert)

EN 60447 : 1993

Mensch-Maschine-Schnittstelle (MMI) – Bedienungsgrundsätze (IEC 447 : 1993)

EN 60529

Schutzarten durch Gehäuse (IP-Code) (IEC 529 : 1989)

EN 60721-3-0

Klassifizierung von Umweltbedingungen – Teil 3: Klassen von Umwelteinflußgrößen und deren Grenzwerte – Einführung und Hinweise für den Anwender (IEC 721-3-0 : 1984 + A1 : 1987)

IEC 50 (191) : 1990

Internationales elektrotechnisches Wörterbuch, Kapitel 191: Zuverlässigkeit und Dienstgüte

3 Definitionen

Für die Anwendung dieser Norm gelten die folgenden Definitionen zusätzlich zu den in EN 292-1 und IEC 50 (191) enthaltenen Definitionen:

3.1 Sicherheitsbezogenes Teil einer Steuerung: Teil oder ein untergeordneter Teil (untergeordnete Teile) einer Steuerung, der (die) auf Eingangssignale anspricht (ansprechen) und sicherheitsbezogene Ausgangssignale erzeugt (erzeugen). Die kombinierten sicherheitsbezogenen Teile einer Steuerung beginnen dort, wo die sicherheitsbezogenen Signale eingegeben werden und enden am Ausgang der Leistungssteuerungselemente (siehe auch Anhang A der EN 292-1 : 1991). Dies beinhaltet auch Überwachungssysteme.

3.2 Kategorie: Einteilung der sicherheitsbezogenen Teile einer Steuerung in bezug auf ihre Widerstandsfähigkeit gegen Fehler und ihr Verhalten im Fehlerfall, die aufgrund der strukturellen Anordnung der Teile und/oder deren Zuverlässigkeit erreicht wird.

3.3 Sicherheit von Steuerungen: Fähigkeit von sicherheitsbezogenen Teilen einer Steuerung, ihre Sicherheitsfunktion(en) für einen gegebenen Zeitraum entsprechend der für sie festgelegten Kategorie auszuführen.

3.4 Fehler: Der Zustand eines Gegenstandes, der durch die Unfähigkeit gekennzeichnet ist, eine geforderte Funktion auszuführen, ausgenommen die Unfähigkeit bei der Durchführung präventiver Instandhaltung oder anderer geplanter Handlungen oder aufgrund fehlender externer Betriebsmittel.

ANMERKUNG 1: Ein Fehler ist häufig das Ergebnis eines Ausfalls des Gegenstandes selbst, kann aber auch ohne vorherigen Ausfall vorhanden sein.

ANMERKUNG 2: Im Englischen sind die Benennung "fault" und seine Definition identisch mit der in IEC 50(191) der IEC 50(191) : 1990 enthalten. Im Bereich der Maschinen werden die französische Benennung "défaut" und die deutsche Benennung "Fehler" eher benutzt, als die Benennungen "panne" und "Fehlzustand", die diese Definition widerspiegeln.

3.5 Ausfall: Die Beendigung der Fähigkeit eines Gegenstandes, eine geforderte Funktion durchzuführen.

ANMERKUNG 1: Nach Ausfall hat der Gegenstand einen Fehler.

ANMERKUNG 2: "Ausfall" ist ein Ereignis, im Gegensatz zu "Fehler", der einen Zustand darstellt.

ANMERKUNG 3: Der hier definierte Begriff gilt nicht für Gegenstände, die nur aus Software bestehen.

[IEV 191-04-01 der IEC 50 (191) : 1990]

ANMERKUNG 4: In der Praxis werden die Benennungen Fehler und Ausfall häufig synonym verwendet.

3.6 Sicherheitsfunktionen von Steuerungen: Durch ein Eingangssignal ausgelöste und durch sicherheitsbezogene Teile von Steuerungen verarbeitete Funktion, die der

Maschine (als System) das Erreichen eines sicheren Zustandes ermöglicht.

3.7 Muting: Zeitbegrenztes automatisches Aufheben einer Sicherheitsfunktion(en) durch sicherheitsbezogene Teile der Steuerung.

3.8 Manuelle Rückstellung: Funktion innerhalb der sicherheitsbezogenen Teile der Steuerung, um gegebene Sicherheitsfunktionen vor erneutem Anlaufen der Maschine manuell wiederherzustellen.

4 Allgemeine Betrachtungen

4.1 Sicherheitstechnische Ziele bei der Gestaltung

Die sicherheitsbezogenen Teile einer Steuerung, die Sicherheitsfunktionen übernehmen, müssen so gestaltet und gebaut sein, daß die Grundsätze der EN 1050 in vollem Umfang berücksichtigt werden:

- bei bestimmungsgemäßer Verwendung und vorhersehbarem Mißbrauch;
- beim Auftreten von Fehlern;
- im Falle von vorhersehbaren menschlichen Fehlern bei bestimmungsgemäßer Verwendung der Maschine als Ganzes.

4.2 Allgemeine Vorgehensweise bei der Gestaltung

Ausgehend von der Risikobeurteilung (siehe EN 1050) an der Maschine muß der Konstrukteur über den Beitrag zur Risikoverringerung entscheiden, den jedes Teil der sicherheitsbezogenen Teile der Steuerung (siehe Anhang B) zu leisten hat. Dieser Beitrag deckt nicht das Gesamtrisiko der gesteuerten Maschinen ab, z. B. wird nicht das Gesamtrisiko einer mechanischen Presse oder einer Waschmaschine berücksichtigt, sondern der Teil des Risikos, der durch die Anwendung bestimmter Sicherheitsfunktionen reduziert wird. Beispiele für solche Funktionen sind die Stop-Funktion, die durch Verwendung einer berührungslos wirkenden Schutzeinrichtung an einer Presse oder durch die Funktion der Türverriegelung einer Waschmaschine ausgelöst wird.

Als Hauptziel muß der Konstrukteur sicherstellen, daß sicherheitsbezogene Teile einer Steuerung Ausgänge erzeugen, durch die sich die in EN 1050 festgelegten Ziele zur Risikoverringerung erreichen lassen. Dies läßt sich nicht immer erreichen, und in solchen Fällen muß der Konstrukteur andere Sicherheitsmaßnahmen durchführen. Die Hierarchie bei der Vorgehensweise zur Risikoverringerung ist in Abschnitt 5 der EN 292-1 : 1991 gegeben.

Die Kategorie und andere Merkmale, z. B. physikalische Anordnung der Teile, Isolierung, die der Konstrukteur für die sicherheitsbezogenen Teile auswählt, sind abhängig vom Beitrag, den diese Teile zur Risikoverringerung leisten, von der Gestaltung sowie von der Technologie (siehe Abschnitt 0). Der Konstrukteur muß angeben:

- welche Kategorie(n) bei der Gestaltung als Bezugspunkt genommen worden ist;
- die genauen Punkte, wo der sicherheitsbezogene Teil(e) beginnt und wo genau dieser endet;
- die sinnvolle Vorgehensweise, z. B. die berücksichtigten Fehler, die ausgeschlossen Fehler, bei der Gestaltung, um diese Kategorie(n) zu erreichen.

Je mehr die Risikoverringerung von den sicherheitsbezogenen Teilen von Steuerungen abhängig ist, desto höher muß die erforderliche Widerstandsfähigkeit dieser Teile gegen Fehler sein. Diese Fähigkeit – im Sinne, daß die erforderliche Funktion ausgeführt wird – kann zum Teil durch Zuverlässigkeitswerte und durch eine fehlerwiderstandsfähige Struktur quantitativ erfaßt werden. Sowohl die Zuverlässigkeit als

auch die Struktur tragen zur Widerstandsfähigkeit der sicherheitsbezogenen Teile gegen Fehler bei. Eine vorgegebene Widerstandsfähigkeit gegen Fehler kann durch Festlegung des Zuverlässigkeitsgrades der Bauteile und/oder durch verbesserte Strukturen für die sicherheitsbezogenen Teile erreicht werden. Der Beitrag, den Zuverlässigkeit und Struktur leisten, kann je nach verwendeter Technologie unterschiedlich sein. So ist beispielsweise bei Verwendung eines einzelnen Kanals sicherheitsbezogener Teile mit hoher Zuverlässigkeit in der einen Technologie die gleiche oder höhere Widerstandsfähigkeit gegen Fehler möglich, als bei einer fehlertoleranten Struktur geringerer Zuverlässigkeit in einer anderen Technologie.

ANMERKUNG: Je höher die Widerstandsfähigkeit der sicherheitsbezogenen Teile gegen Fehler, desto geringer die Wahrscheinlichkeit, daß die sicherheitsbezogenen Teile bei der Ausführung der geforderten Funktionen versagen.

Zuverlässigkeit und Sicherheit bedeuten nicht dasselbe (siehe Anhang D). Zum Beispiel ist die Sicherheit eines Systems, das aus verhältnismäßig unzuverlässigen Bauteilen besteht, innerhalb einer redundanten Struktur möglicherweise höher als die Sicherheit eines Systems mit einfacher Struktur, jedoch mit zuverlässigeren Bauteilen. Dieser Gedanke ist wichtig, weil die Sicherheit in einigen Anwendungen höchste Priorität erfordert ungeachtet der erreichten Zuverlässigkeit, z. B. wenn die Folgen eines Ausfalls immer schwer und üblicherweise irreversibel sind. Bei Anwendungen dieser Art muß in Übereinstimmung mit der Risikobeurteilung eine Struktur der Fehlererkennung (Fehlertoleranz in einem Arbeitszyklus) vorgesehen werden, die die geforderte Sicherheitsfunktion nach dem Auftreten von einem, zwei oder mehr Fehlern erfüllt.

Diese Norm erfordert keine Berechnung von Zuverlässigkeitswerten für komplexe Strukturen, wenn die Sicherheit überwiegend durch die Strukturverbesserung der sicherheitsbezogenen Teile erreicht wird. Im Falle von weniger komplexen Strukturen, bei denen die Zuverlässigkeit von Bauteilen für die Sicherheit wichtig ist, ist die Berechnung von Zuverlässigkeitswerten ein nützlicher Hinweis für den Beitrag, den die sicherheitsbezogenen Teile zur Risikoverringung insgesamt erbringen.

Im Falle von Anwendungen mit niedrigerem Risiko können Maßnahmen zur Vermeidung von Fehlern angemessen sein; für Anwendungen mit höherem Risiko können durch Verbesserung der Struktur der sicherheitsbezogenen Teile einer Steuerung Maßnahmen zur Vermeidung, Erkennung oder Tolerierung von Fehlern erreicht werden. Praktische Maßnahmen schließen Redundanz, Diversität, Überwachung ein (siehe auch Abschnitt 3 der EN 292-2 : 1991, Anhang A der EN 292-2 : 1991/A1 : 1995 und 9.4 der EN 60204-1 : 1992).

Das erreichte Verhalten in bezug auf die Widerstandsfähigkeit der sicherheitsbezogenen Teile der Steuerung gegen Fehler ist eine Funktion von zahlreichen Parametern, z. B.:

- die Zuverlässigkeit im Hinblick auf die Ausführung der Sicherheitsfunktionen;
- die Struktur (oder Architektur) der Steuerung;
- die Qualität der sicherheitsbezogenen Dokumentation;
- die Vollständigkeit der Spezifikation;
- die Gestaltung, Herstellung und Instandhaltung;
- die Qualität und Richtigkeit der Software;
- das Ausmaß an Funktionsprüfungen;
- die betriebstechnischen Eigenschaften der gesteuerten Maschine oder des gesteuerten Teiles der Maschine.

Diese Parameter können drei Haupteigenschaften zugeordnet werden:

- Zuverlässigkeit der Hardware – der Zuverlässigkeitsgrad der Bauteile zur Vermeidung von Fehlern;
- Struktur des Systems – die Anordnung der Bauteile im sicherheitsbezogenen Teil einer Steuerung zur Vermeidung, Tolerierung oder Erkennung von Fehlern;
- die nicht-quantifizierbaren, qualitativen Gesichtspunkte, die das Verhalten des sicherheitsbezogenen Teiles einer Steuerung beeinflussen.

4.3 Prozeß für die Auswahl und Gestaltung von Sicherheitsmaßnahmen

In diesem Unterabschnitt wird ein Prozeß zur Auswahl der zu treffenden Sicherheitsmaßnahmen und danach zur Gestaltung der sicherheitsbezogenen Teile der Steuerung dargestellt. Hierbei ist es wichtig, die Schnittstellen zwischen den sicherheitsbezogenen Teilen der Steuerung und den nicht sicherheitsbezogenen Teilen der Steuerung und allen anderen Teilen der Maschine festzulegen. Somit kann der Beitrag der sicherheitsbezogenen Teile zur Risikoverringung in Übereinstimmung mit der Risikobeurteilung der Maschine nach EN 1050 festgelegt werden.

Da es zahlreiche Möglichkeiten gibt, um das Risiko an einer Maschine zu verringern und es ebenso viele Möglichkeiten gibt, um die sicherheitsbezogenen Teile der Steuerungen zu gestalten, handelt es sich hierbei um einen iterativen Prozeß. Entscheidungen und/oder Annahmen, die bei jedem Verfahrensschritt getroffen werden, können die bei einem früheren Schritt gemachten Entscheidungen und/oder Annahmen beeinflussen. Dieser Gesichtspunkt läßt sich prüfen, indem man bei jedem Schritt das Verfahren noch einmal durchläuft. Bei der Validierung ist diese Art der Prüfung von grundlegender Bedeutung, um sicherzustellen, daß die erreichte sicherheitstechnische Leistungsfähigkeit mit der in der Spezifikation festgelegten übereinstimmt.

Das Verfahren ist in Bild 1 dargestellt. Wichtige Gesichtspunkte, die beim Gestaltungsprozeß berücksichtigt werden sollten, sind in Anhang A in Form von Fragen als Denkanstoß für den Konstrukteur gegeben. Diese Fragen geben die Philosophie wieder, die bei der Gestaltung von sicherheitsbezogenen Teilen befolgt werden sollte. Nicht alle Fragen gelten für alle Anwendungsmöglichkeiten. Einige Anwendungsmöglichkeiten erfordern zusätzliche Fragen.

Schritt 1: Gefährdungsanalyse und Risikobeurteilung

- Feststellen der Gefährdungen an einer Maschine bei allen Betriebsarten und in jeder Phase der Lebensdauer der Maschine entsprechend den Hinweisen in EN 292-1 und EN 1050,
- Beurteilen des durch diese Gefährdungen auftretenden Risikos und Entscheiden über die angemessene Risikoverringung für diese Anwendung nach EN 292-1 und EN 1050.

Schritt 2: Entscheiden über Maßnahmen zur Risikoverringung durch Steuerungsmittel

- Entscheiden über gestaltungstechnische Maßnahmen an der Maschine selbst und/oder das Vorsehen von Schutzeinrichtungen, um die Risikoverringung zu bewirken. Diese Teile der Steuerung, die als integraler Bestandteil der gestaltungstechnischen Maßnahmen und/oder bei der Steuerung der Schutzeinrichtungen dazu einen Beitrag erbringen, müssen als sicherheitsbezogene Teile betrachtet werden.

Schritt 3: Festlegen der sicherheitstechnischen Anforderungen für die sicherheitsbezogenen Teile der Steuerung

- Festlegen der Sicherheitsfunktionen (siehe Abschnitt 5 und andere in Bezug genomme Dokumente), die in der Steuerung vorzusehen sind. In Tabelle 1 sind die Quellenangaben der üblicheren Sicherheitsfunktionen und die Eigenschaften aufgeführt, die bei