

Sonderdruck

Sicherheitsgerechtes Gestalten technischer Erzeugnisse

Auszüge aus DIN 31000 (VDE 1000) u. a.

– Nur zu Ausbildungszwecken –

Sicherheitsfragen für Produkte werden in steigendem Maß im internationalen weltweiten oder europäischen Rahmen behandelt. Zum Beispiel verlangt die Europäische Richtlinie über die Allgemeine Produktsicherheit vom 1. Dezember 2001 in Artikel 1 (1), dass die in Verkehr gebrachten Produkte sicher sind. Was darunter zu verstehen ist, legt Artikel 3 fest. Ziel ist eine sicherheitstechnische Harmonisierung des europäischen Binnenmarkts ohne nationale Abweichungen.

Für Maschinen fordert die europäische Maschinenrichtlinie vom 17. Mai 2006 nach den in ihrem Anhang I aufgeführten „Allgemeinen Grundsätzen“, dass eine Risikobeurteilung für die Integration der Sicherheit nach Absatz 1.1.2 der Richtlinie durchgeführt wird.

Der ISO/IEC Guide 51 weist an, wie Sicherheitsaspekte, die sich auf Menschen, Güter oder die Umwelt beziehen, in Normen aufzunehmen sind. DIN 820-120 setzt diesen internationalen Leitfaden wortgetreu für das deutsche Normenwerk um.

Zweck dieses Sonderdrucks ist, dem Auszubildenden und Studierenden einen Einstieg in Grundlagen des sicherheitsgerechten Gestaltens technischer Erzeugnisse zu geben. **Für die Arbeit im Betrieb ist das Studium der Originaltexte der Normen in der jeweils gültigen Fassung unerlässlich.**

Je nach Arbeitsgebiet bietet der VDE VERLAG gezielt zusammengestellten VDE-Auswahlreihen als wichtige Grundaustattungen, z. B.:

- VDE-Auswahl für den Elektromaschinenbau,
- VDE-Auswahl zur funktionalen Sicherheit,

die jeweils als Papiersammlung, auf DVD und als PDF-Dateien im Rahmen des VDE-Online-Abonnements bei der VDE VERLAG GmbH, Bismarckstr. 33, 10625 Berlin, www.vde-verlag.de zu beziehen sind. Dort sind auch jederzeit aktuelle Verzeichnisse der in den VDE-Auswahlen enthaltenen Normen abrufbar.

Die DVD ist die beste, komfortabelste, effektivste und dennoch preisgünstigste Art der Nutzung der elektrotechnischen Sicherheitsnormen: Die Verweise elektronisch verlinkt und so ergänzt, dass mitgeltende Anforderungen und separat veröffentlichte Änderungen nicht übersehen werden.

Ausgabe 2008

Herausgegeben durch DKE, Stresemannallee 15; 60596 Frankfurt am Main; Telefon: +49 69 6308-0; Fax: +49 69 6312925
E-Mail: dke@vde.com, Internet: www.dke.de

© DIN Deutsches Institut für Normung e. V. und VDE Verband der Elektrotechnik Elektronik Informationstechnik e. V.
Jede Art der Vervielfältigung, auch auszugsweise, nur mit besonderer Genehmigung des DIN, Berlin, und des VDE, Frankfurt am Main.

Einzelverkauf und Abonnements der DIN-VDE-Normen durch VDE VERLAG GMBH, 10625 Berlin, www.vde-verlag.de
Einzelverkauf auch durch Beuth Verlag GmbH, 10772 Berlin, www.beuth.de

Vorwort

Die Normen zum sicherheitsgerechten Gestalten technischer Erzeugnisse sind eng mit den auf der Titelseite angesprochenen Europäischen Richtlinien verknüpft. Erläuterungen hierzu sind im Abschnitt „Einleitung“ gegeben.

Der Geltungsbereich der 1979 als DIN 31000 (VDE 1000) veröffentlichten allgemeinen Leitsätze wird so seit Juli 2007 durch die Normenreihe DIN EN ISO 12100 „Sicherheit von Maschinen – Grundbegriffe, allgemeine Gestaltungsleitsätze“ eingeschränkt. Die Neuausgabe dieses Sonderdrucks zu DIN 31000 (VDE 1000) wurde daher entsprechend erweitert und um Grundlagen zum Thema „Funktionale Sicherheit“ ergänzt.

Der Hauptzweck der DIN EN ISO 12100 besteht darin, Konstrukteuren einen Gesamtüberblick und einen Leitfaden zu geben, um ihnen die Herstellung von Maschinen zu ermöglichen, die für ihre bestimmungsgemäße Verwendung sicher sind. Sie stellt darüber hinaus eine Strategie für die Erarbeitung von Normen zur Verfügung.

- Teil 1 legt die grundsätzliche Terminologie und die Methodologie fest, die für das Erreichen der Sicherheit von Maschinen angewandt werden. Die Festlegungen sind für Konstrukteure vorgesehen.
- Teil 2 legt technische Leitsätze fest, um Konstrukteure dabei zu unterstützen, sichere Maschinen zu konstruieren. Er ist dafür vorgesehen, bei der Betrachtung der Lösung für ein spezifisches Problem zusammen mit Teil 1 verwendet zu werden.

Für die Grundbegriffe der Sicherheitstechnik gilt DIN 820-120 „Normungsarbeit – Teil 120: Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen“. Diese ist, mit Erlaubnis des DIN, ab Seite 25. wiedergegeben. Die mit dem Änderungsentwurf DIN 820-120/A1:2008-01 vorgestellten vorgesehenen Änderungen sind vermerkt.

Dieser Sonderdruck wurde durch die DKE in enger Zusammenarbeit mit in der Berufsausbildung aktiven Ausbildern erstellt. Besonders gedankt sei hier

Frau Dr. Andrea Fluthwedel, Normenausschuss Sicherheitstechnische Grundsätze (NASG) im DIN, Berlin,
Herrn Marc Fröhlich, Berufliche Schule Farmsen, Hamburg,
Herrn Reiner Hinrichs, Ludwig-Geißler-Schule, Hanau,
Herrn Prof. Dr.-Ing. habil Gerhard Hofmann, Hochschule für Technik und Wirtschaft Dresden,
Herrn Prof. em. Dr.-Ing. Dr. h.c. Gerhard Hosemann, Marloffstein,
Herrn Klaus Kreutzer, Marinetechnikschule Parow,
Herrn Hartmut von Krosigk, Erlangen,
Herrn Robert Urbanke, Innung für Elektro- und Informationstechnik, Ausbildungszentrum, Ansbach,
Herrn Hans-Joachim Zöll, RheinEnergie AG, Ausbildungszentrum, Köln.

Die in den VDE-Auswahlreihen zusammengestellten DIN-VDE-Normen sind, wie alle als VDE-Bestimmung gekennzeichneten DIN-Normen, Sicherheitsnormen auf dem Gebiet der Elektrotechnik. Sie beschreiben den zum Zeitpunkt ihres Erscheinens aktuellen Stand der Technik. Ihre Bedeutung wird durch die Bezugnahme in Gesetzen und Verordnungen unterstrichen. So sind alle DIN-VDE-Normen eine Erkenntnisquelle für technisch ordnungsgemäßes Verhalten im Regelfall. Durch das Anwenden der DIN-VDE-Normen entzieht sich aber niemand der Verantwortung für eigenes Handeln.

Die Auszüge aus DIN-Normen ohne VDE-Klassifikation sind wiedergegeben mit Erlaubnis des DIN Deutsches Institut für Normung e. V., 10772 Berlin. Diese sind zu beziehen über den Beuth Verlag, 10772 Berlin, www.beuth.de

Die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE ist die nationale Organisation für die Erarbeitung von Normen und Sicherheitsbestimmungen in dem Bereich der Elektrotechnik, Elektronik und Informationstechnik in Deutschland. Sie ist ein Organ des DIN Deutsches Institut für Normung e.V. und des VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V. und vertritt aktiv die deutschen Interessen in den Internationalen und Europäischen Normungsorganisationen IEC, CENELEC und ETSI.

Die Normungsergebnisse der DKE werden unter Beteiligung der Öffentlichkeit über das Einspruchsverfahren zu Norm-Entwürfen erstellt. Sie sind weitgehend europäisch und international harmonisiert und werden als Deutsche Normen in das Normenwerk des DIN und, wenn sie sicherheitstechnische Festlegungen enthalten, mit einer VDE-Klassifikation gleichzeitig als VDE-Bestimmungen, VDE-Leitlinien oder VDE-Vornormen in das VDE-Vorschriftenwerk aufgenommen.

Aktuelle Informationen rund um die DKE sind im Internet unter www.dke.de zu finden.

Frankfurt am Main, im August 2008

Inhalt

Seite

Einleitung	4
Allgemeine Leitsätze	7
DIN 31000 (VDE 1000):1979-03 mit Änderung A1:2007-07	
Aktuelle Terminologie – Grundkonzept der Sicherheit	25
DIN 820-120	
Methodologie bezüglich Maschinen	31
DIN EN ISO 12100-1	
Quantifizierte Risikominderung – Erläuterung	41
Funktionale Sicherheit – Einführung	45
Funktionale Sicherheit – Grundsätze, Sicherheitslebenszyklus	59
DIN EN 61508-1 (VDE 0803-1)	
VDE-Auswahl zur funktionalen Sicherheit	69
Liste der enthaltenen Normen	
Organisation der nationalen, europäischen und internationalen Normung	Umschlagrückseite

Einleitung

Generell sind in der EU derzeit die folgenden Bestrebungen zu beobachten:

- Eine Zusammenführung und, wenn möglich, Vereinfachung unterschiedlicher Vorschriften, welche die Sicherheit der Verbraucherprodukte und Anlagen einerseits und der technischen Arbeitsmittel andererseits betreffen. Beispiele: Das deutsche Geräte- und Produktsicherheitsgesetz (GPSG) vom 6. Januar 2004 erfasst mit wenigen Ausnahmen die Sicherheit aller technischen Produkte, die bisher unterschiedlichen Gesetzen unterlagen.
- Eine erweiterte Anwendung des Subsidiaritätsprinzips nach dem „Neuen Ansatz (engl.: new approach) zur technischen Harmonisierung und Normung vom 7. Mai 1985“. Beauftragte Normenverbände interpretieren kooperativ, aber in eigener Verantwortung, die allgemein gehaltenen Inhalte und Generalklauseln technischer Gesetze und Verordnungen, z. B. der EU-Direktiven.
- Eine generelle Verwendung des in DIN 820-120:2001-10 präzisierten Risikobegriffs bei der Beurteilung aller Maßnahmen, die zur Sicherheit, Vorsorge und Meidung zu treffen sind, um Personen-, Sach- und Umweltschäden zu vermeiden. In der Sicherheitstechnik bleiben – anders als beim Management finanzieller, kommerzieller und anderer Wagnisse – die durch Technik erreichbaren Vorteile und Opportunitäten außer Betracht: Einziger, aber entscheidender Vorteil ist in der Sicherheitstechnik der ausbleibende Schaden. Güterabwägungen, die unvermeidlich vom subjektiven Bewusstsein des Entscheidenden abhängen, werden damit vermieden.
- Eine Differenzierung der nach dem Prinzip der Sicherheit, Vorsorge oder Meidung erkannten, vermuteten oder beargwöhnten Gefährdungen anhand der Kausalität des potenziellen Schadenablaufs, wie sie im DIN-Fachbericht 144 vorgenommen wird.

Ein Beispiel für einen kausalen Schadenablauf:

- Der Blumentopf auf dem Fensterbrett im Obergeschoss des Hauses ist eine potenzielle Schadenquelle, also eine **Gefährdung**.
- Grenzt das Fenster an eine Verkehrsstraße, besteht eine **Gefährdungssituation**.
- Erst durch ein auslösendes Gefährdungsereignis, z. B. das Öffnen des Fensters nach außen, wird der Topf durch seine freigesetzte potenzielle Energie zur **Gefahr**, da sein möglicher Absturz einen Personenschaden an Passanten oder einen Sach**schaden** etwa an einem Auto anrichten kann.

In der Sicherheitstechnik wird ein Vorgehen nach dem nachstehenden Bild dieser Entwicklung gerecht.

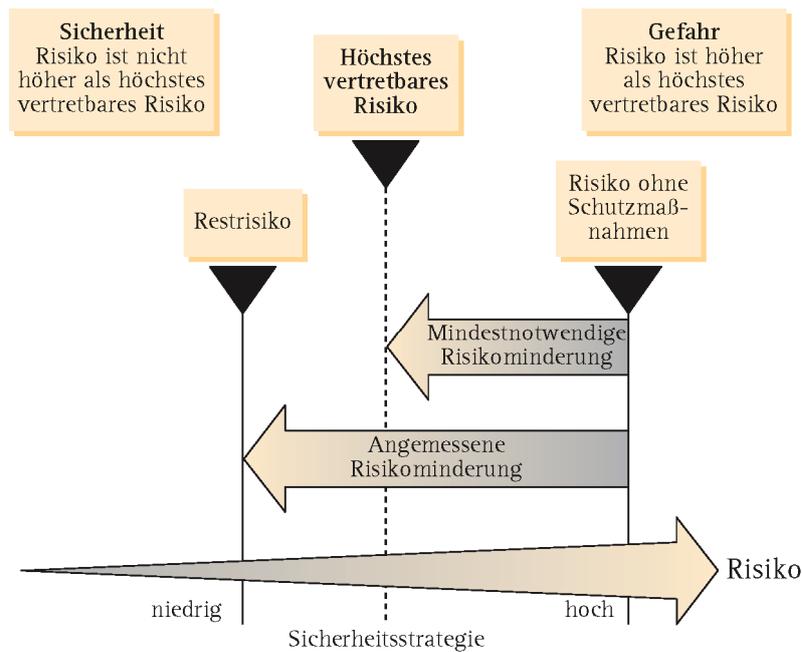
Dabei sind festgelegt:

- Vertretbares Risiko (engl.: tolerable risk): Risiko, das in einem bestimmten Zusammenhang nach den gültigen Wertvorstellungen der Gesellschaft gerechtfertigt ist (DIN 820-120:2001-10, Abschnitt 3.7). Als vertretbar sind im Allgemeinen Risiken anzusehen, welche der Bevölkerung nach Überzeugung des Garanten, d. h. einer legitimierten sachkundigen Institution oder Person, die Gewähr für gesicherte Aussagen bietet, zugemutet werden können.
- Restrisiko (engl.: residual risk): Risiko, das nach Anwendung von Schutzmaßnahmen verbleibt. Jede potenzielle Schadenquelle ist mit einem Risiko verbunden. Das Ausbleiben von Schadensereignissen ist noch kein Beweis dafür, dass das Risiko für das Auftreten einer Gefährdungssituation gering sei.

Es gibt kein „Nullrisiko“. Kriterien für das höchste vertretbare Risiko sind z. B. zu finden

- in den Inhalten der Sicherheitsnormen, die etwa von Normungsverbänden nach dem „Neuen Ansatz“ erstellt wurden,
- in den Ergebnissen wissenschaftlich abgesicherter internationaler Diskussionen.

Besonderer Schutz kann bestimmten Bevölkerungsgruppen, etwa Kindern und Hilfsbedürftigen, eingeräumt werden. Unfreiwillige Betroffenheit von Risiken ist als weit kritischer anzusehen als ihre freiwillige Übernahme. Kurzlebige Tagesmeinungen dürfen in die Ermittlung des vertretbaren Risikos nicht einfließen. Das aktuelle Risiko ohne oder mit Schutzmaßnahmen wird mit Normen zur Risikobeurteilung bestimmt.



Der Risikoeinsatz zur Beurteilung der technischen Sicherheit

Bestimmungsgemäß sind Risiken für die gesamte vorhersehbare „Lebensdauer“ der Produkte zu erfassen. Der Nutzen der technischen Produkte bleibt dabei außer Betracht. Dadurch werden Güterabwägungen vermieden. Maßnahmen zur „mindestnotwendigen Risikominderung“ in obigem Bild sind teils vom Konstrukteur, teils vom Benutzer durchzuführen. Das Restrisiko enthält beide Anteile. Eine weitergehende „angemessene“ Risikominderung ist erstrebenswert, lässt sich aber nur bei niederen Marginalkosten erreichen. Die Risikobeurteilung wird, wie DIN-Fachbericht 144 in Abschnitt 5 beschreibt, in aufeinander folgenden Schritten durchgeführt:

- Identifizierung der Gefährdung (engl. hazard identification),
- Risikoeinschätzung (engl. risk estimation),
- Risikobewertung (engl. risk evaluation).

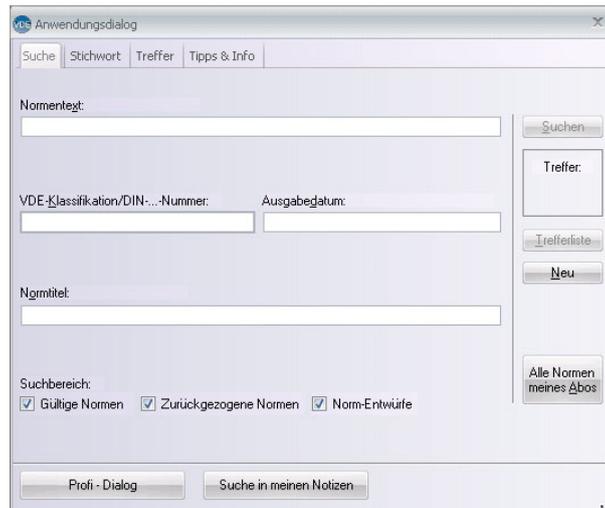
Die Risikoeinschätzung enthält in diesem Modell die beiden Dimensionen

- Schadensumfang (engl.: severity of harm) und
- Eintrittswahrscheinlichkeit (engl.: probability of occurrence) mit den fachübergreifenden Komponenten Gefährdungssituation (engl.: hazardous situation), Gefährdungereignis (engl.: hazardous event) und ergonomische Gestaltung (engl.: possibilities to avoid or limit the harm).

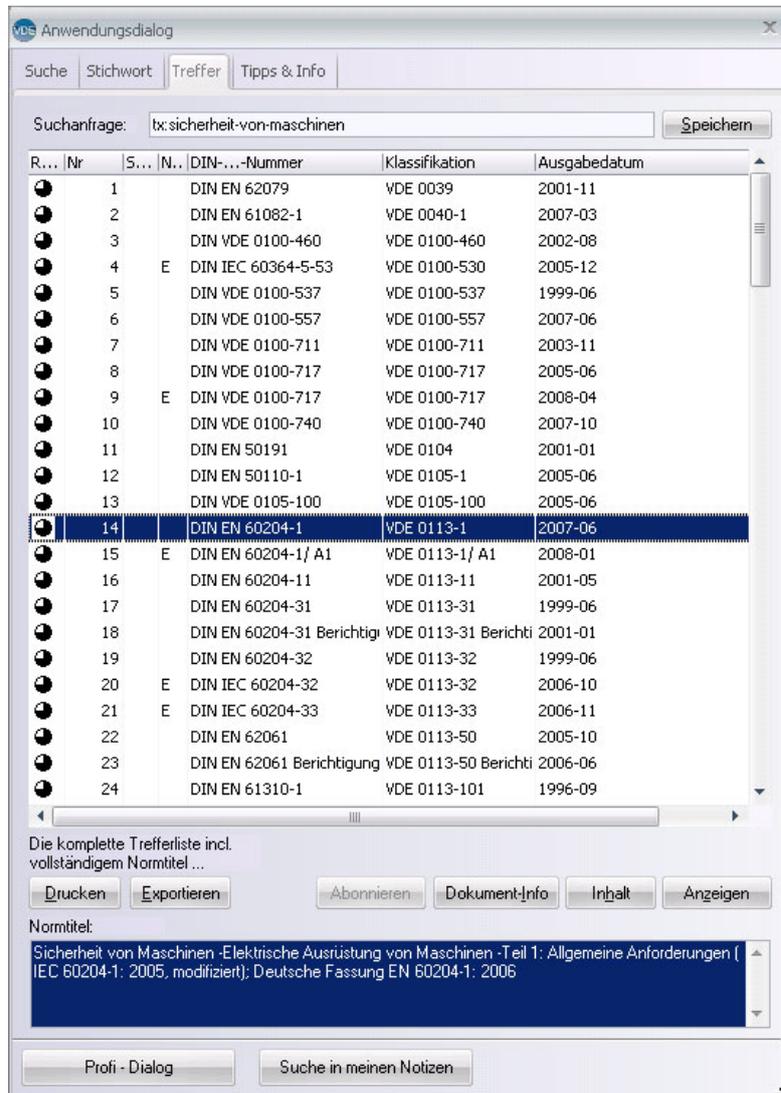
Die Risikoeinschätzung ist der letzte Teil der Risikoanalyse. Für sie wurden verschiedene Hilfsmittel entwickelt, zum Beispiel Grafen, Matrizen und Tabellen. Sie führen auf Risikoklassen unterschiedlicher Schwere. Die endgültige Entscheidung, ob ein Produkt sicher ist, kann aber erst in der anschließenden Risikobewertung jedes Einzelfalls getroffen werden. Sie trägt solchen belastenden oder entlastenden Gegebenheiten Rechnung, die in der groben Risikoeinschätzung nicht erfasst werden konnten und endet mit einem Risikovergleich mit vergleichbaren Produkten, deren Sicherheit zweifelsfrei feststeht (DIN EN ISO 14121-1:2007-12 „Sicherheit von Maschinen – Risikobeurteilung – Teil 1: Leitsätze“, Abschnitt 8.3).

Auf die Risikobeurteilung folgt die polare „Ja“/„Nein“-Entscheidung über die Sicherheit des Produkts: Kein technisches Erzeugnis, kein Verfahren oder keine Dienstleistung dürfen auf Dauer nur eingeschränkt sicher sein, denn das hieße: sicher und unsicher zugleich.

Standardsuchmaske der DVD des VDE-Vorschriftenwerks:



Trefferliste zur Suche nach „Sicherheit-von-Maschinen, gültige Normen und Entwürfe“:



Weitere Informationen zur DVD und Powerpoint-Demonstration siehe www.vde-verlag.de

	Allgemeine Leitsätze für das sicherheitsgerechte Gestalten technischer Erzeugnisse	DIN 31000
VDE	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Vorstand beschlossenen Genehmigungsverfahrens unter nebenstehenden Nummern in das VDE-Vorschriftenwerk aufgenommen und in der etz Elektrotechnische Zeitschrift bekannt gegeben worden.	Klassifikation VDE 1000
Vervielfältigung – auch für innerbetriebliche Zwecke – nicht gestattet.		

- 1 Geltungsbereich
- 2 Zweck und Anwendung
- 3 Begriffe
- 4 Grundlagen für das sicherheitsgerechte Gestalten
 - 4.1 Ziele der Sicherheitstechnik
 - 4.2 Sicherheitstechnische Sonderbedingungen
 - 4.3 Sicherheitstechnische Sondermaßnahmen
 - 4.4 Sicherheit bei der Herstellung
- 5 Allgemeine Leitsätze und Rahmen-Bestimmungen
 - 5.1 Beanspruchungen
 - 5.2 Werkstoffe
 - 5.3 Bewegte Teile
 - 5.4 Oberflächen, Ecken und Kanten
 - 5.5 Tritt- und Stehsicherheit, Gleithemmung
 - 5.6 Standsicherheit
 - 5.7 Transportgerechte Gestaltung
 - 5.8 Beim Betrieb auftretende Gefahren
 - 5.9 Elektrische Energie
 - 5.10 Pneumatische und hydraulische Ausrüstung
 - 5.11 Gastechische Ausrüstung für brennbare Gase
 - 5.12 Ausrüstung für flüssige und feste Brennstoffe
 - 5.13 Ausrüstung für Treibmittel-Energie
 - 5.14 Einrichtungen zum Schalten, Steuern und Regeln
 - 5.15 Anforderungen an die gefahrlose Funktion
 - 5.16 Wirksamkeit besonderer sicherheitstechnischer Mittel
 - 5.17 Elektrostatische Aufladung
 - 5.18 Betriebsstoffe und Arbeitsstoffe
 - 5.19 Menschengerechte (ergonomische) Gestaltung

Erläuterungen

Literaturhinweise

Beginn der Gültigkeit

Diese Norm gilt ab 1979-03-01, mit Änderung A1 ab 2007-07-01

Der Norm-Inhalt war veröffentlicht als E DIN 57000 (VDE 1000):1976 bzw. E DIN 31000/A1 (VDE 1000/A1):2006-02.

1 Geltungsbereich

1.1 Diese Norm gilt für technische Erzeugnisse **ausgenommen solcher, die in den Anwendungsbereich der Normen DIN EN ISO 12100-1 und DIN EN ISO 12100-2 fallen**. Für die Grundbegriffe der Sicherheitstechnik gilt anstelle der bereits am 1. April 2005 zurückgezogenen Norm DIN VDE 31000-2 die Norm DIN 820-120.

1.2 In ihrer Funktion als VDE-Rahmen-Bestimmung gilt diese Norm

- a) für elektrische Betriebsmittel im Sinne von 3.1.1, die bei ihrer bestimmungsgemäßen Verwendung von Laien (siehe 3.6.3) betrieben werden, von Laien berührt werden oder auf Laien einwirken sowie
- b) unter Berücksichtigung von 4.3 für elektrische Betriebsmittel im Sinne von 3.1.1, die vorzugsweise oder ausschließlich Fachkräften (siehe 3.6.1) oder unterwiesenen Personen (siehe 3.6.2) zugänglich sind und die nach Art ihres Aufbaues oder ihrer Funktion zur Verwendung in elektrischen Betriebsstätten (siehe 3.7.1) oder in abgeschlossenen elektrischen Betriebsstätten (siehe 3.7.2) bestimmt sind.

1.3 Diese Norm gilt nicht für:

- a) Werkstoffe, Hilfsstoffe, soweit sie nicht für oder in technischen Erzeugnissen Verwendung finden;
- b) nicht selbständig verwendbare Halb- oder Vorfabrikate;
- c) Bauwerke.

2 Zweck und Anwendung

2.1 Die Inanspruchnahme der Technik bringt neben wachsenden Vorteilen vielfach vermehrte Gefahren mit sich, die teils von den technischen Erzeugnissen selbst ausgehen, teils in der Verhaltensweise des Menschen im Umgang mit technischen Erzeugnissen begründet sind.

Diese Gefahren können vermieden oder verringert werden, wenn bei der Gestaltung technischer Erzeugnisse die in dieser Norm aufgeführten sicherheitstechnischen Leitsätze berücksichtigt werden.

2.2 Diese Norm vermittelt Grundlagen für das sicherheitsgerechte Gestalten technischer Erzeugnisse, gegebenenfalls auch im Sinne der einschlägigen Rechts- und sonstigen Vorschriften, z. B. Energiewirtschaftsgesetz (EnWG), Gesetz über technische Arbeitsmittel (GtA), Unfallverhütungsvorschriften (UVV'en).

In ihrer Funktion als VDE-Rahmen-Bestimmung enthält diese Norm grundlegende und für alle Arten elektrischer Betriebsmittel gemeinsam geltende sicherheitstechnische Festlegungen.

2.3 Diese Norm dient als Basis für die inhaltliche Gestaltung von Sicherheitsnormen bzw. VDE-Bestimmungen.

2.4 Diese Norm ermöglicht eine erste Beurteilung technischer Erzeugnisse hinsichtlich ihrer Sicherheit, soweit gültige, konkretisierte und vollständige Normen bzw. VDE-Bestimmungen dafür nicht oder noch nicht zur Verfügung stehen. Bei dieser Beurteilung können bereits bestehende Einzelfestlegungen für vergleichbare Sachverhalte oder für technische Erzeugnisse, die einem vergleichbaren Zweck dienen, sinngemäß angewendet werden.

Ob ein technisches Erzeugnis im ganzen gesehen sicherheitsgerecht gestaltet ist, kann jedoch mit Hilfe dieser Norm allein nicht beurteilt werden.

2.5 Die grundsätzlichen Festlegungen dieser Norm werden in Normen für einzelne Arten technischer Erzeugnisse bzw. in VDE-Bestimmungen für die einzelnen Arten elektrischer Betriebsmittel konkretisiert und durch Angaben über die zugehörigen Prüfungen ergänzt.

3 Begriffe

3.1

technische Erzeugnisse

Technische Erzeugnisse im Sinne dieser Norm sind alle verwendungsfertigen technischen Gegenstände und Einrichtungen. Hierzu gehören unter anderem:

- Einrichtungen der Energie-Erzeugung, -Verteilung, -Umwandlung und -Speicherung;
- Kraft- und Arbeitsmaschinen;
- Hebezeuge und Fördermittel;
- Prüfmaschinen und -geräte;
- Fahrzeuge (Land-, Luft- und Wasserfahrzeuge, einschließlich schwimmender Geräte und Schwimmkörper);
- Einrichtungen der Nachrichten- und Informationstechnik;
- verfahrenstechnische Einrichtungen;
- Arbeitseinrichtungen und -geräte (einschließlich Büroeinrichtungen und -geräte);
- Leitern, Tritte, verfahrbare Arbeitsbühnen und ähnliche gerüstartige Arbeitspodeste;
- Werkzeuge, Spannzeuge und Messzeuge;
- Einrichtungen zum Beheizen, Lüften, Kühlen und Beleuchten;
- Geräte und Einrichtungen für Heim und Freizeit;
- Sport-, Spiel- und Bastelgeräte;
- Bild-, Film- und Tongeräte;
- Einrichtungen der medizinischen Technik;
- Laboreinrichtungen (einschließlich Lehr-, Lern- und Ausbildungsmittel).

3.1.1 Als elektrische Betriebsmittel im Sinne dieser Norm gelten technische Erzeugnisse oder deren Bestandteile, soweit sie nach Funktion und Aufbau dem Anwenden elektrischer Energie dienen. Hierzu gehören z. B. Gegenstände zum Erzeugen, Fortleiten, Verteilen, Speichern, Messen, Überwachen, Steuern, Regeln, Umsetzen und Verbrauchen elektrischer Energie – auch im Bereich der Fernmeldetechnik – und deren Zusammenfassung zu elektrischen Ausrüstungen und elektrischen Anlagen.

3.2

Gefahren

Gefahren im Sinne dieser Norm sind Gefahren aller Art für Leben oder Gesundheit, soweit ihre Wirkungen bei bestimmungsgemäßer Verwendung technischer Erzeugnisse ein nach dem jeweiligen Stand der Technik zumutbares Risiko überschreiten, einschließlich der Gefahren, die durch Lärm, Erschütterungen, Luft- oder Wasserverunreinigungen, Hitzeentwicklung und durch sonstige Belastungen verursacht werden.

3.3

bestimmungsgemäße Verwendung

Bestimmungsgemäße Verwendung im Sinne dieser Norm ist diejenige Verwendung, für die das technische Erzeugnis nach Angaben des Herstellers einschließlich seiner Angaben zum Zwecke der Werbung geeignet ist. Im Zweifel ist es eine solche Verwendung, die sich aus der Bauart, Ausführung und Funktion des technischen Erzeugnisses als üblich ergibt. Zur bestimmungsgemäßen Verwendung gehört auch die Einhaltung der vorgesehenen Betriebs- und Instandhaltungsbedingungen sowie die Berücksichtigung von voraussehbarem Fehlverhalten.

3.4

sicherheitstechnische Maßnahmen

Sicherheitstechnische Maßnahmen im Sinne dieser Norm sind alle gestalterischen und beschreibenden Maßnahmen, die zur Vermeidung von Gefahren getroffen werden. Hierbei ist zwischen unmittelbarer, mittelbarer und hinweisender Sicherheitstechnik zu unterscheiden (siehe [4.1.1 bis 4.1.3](#)).

3.5

besondere sicherheitstechnische Mittel

Besondere sicherheitstechnische Mittel im Sinne dieser Norm sind alle Einrichtungen in oder an technischen Erzeugnissen, die ohne zusätzliche Funktion allein den Zweck haben, deren gefahrlose Verwendung zu fördern oder zu bewirken.

3.6 Benutzer

3.6.1^{E1)}

Fachkraft (Fachmann)

Als Fachkraft (Fachmann) gilt, wer auf Grund seiner fachlichen Ausbildung, Kenntnisse und Erfahrungen sowie Kenntnis der einschlägigen Bestimmungen die ihm übertragenen Arbeiten beurteilen und mögliche Gefahren erkennen kann.

ANMERKUNG Zur Beurteilung der fachlichen Ausbildung kann auch eine mehrjährige Tätigkeit auf dem betreffenden Arbeitsgebiet herangezogen werden.

3.6.2^{E1)}

unterwiesene Person

Als unterwiesene Person gilt, wer über die ihr übertragenen Aufgaben und die möglichen Gefahren bei unsachgemäßem Verhalten unterrichtet und erforderlichenfalls angeleitet sowie über die notwendigen Schutzeinrichtungen und Schutzmaßnahmen belehrt wurde.

3.6.3^{E1)}

Laie

Als Laie gilt, wer weder als Fachkraft nach 3.6.1 noch als unterwiesene Person nach 3.6.2 qualifiziert ist.

3.7 Elektrotechnische Begriffe

3.7.1

elektrische Betriebsstätten

Elektrische Betriebsstätten sind Räume oder Orte, die im wesentlichen zum Betrieb elektrischer Anlagen dienen und in der Regel nur von Fachkräften oder unterwiesenen Personen betreten werden.

ANMERKUNG Hierzu gehören z. B. Schalträume, Schaltwarten, Verteilungsanlagen in abgetrennten Räumen, abgetrennte elektrische Prüffelder und Laboratorien, Maschinenräume von Kraftwerken und dergleichen, deren Betriebsmittel nur von Fachkräften oder unterwiesenen Personen betätigt werden.

^{E1)} Erläuterung für die Leser dieses Sonderdrucks:

Die hier abgedruckten Definitionen sind wörtlich aus der Norm DIN 31000 (VDE 1000) von 1979. Inzwischen sind folgende neuen Definitionen gebräuchlich, aus DIN VDE 0100-200 (VDE 0100-200):2006 „Errichten von Niederspannungsanlagen – Teil 200: Begriffe“:

Fachkraft

Fachkraft ist, wer auf Grund seiner fachlichen Ausbildung, Kenntnisse und Erfahrungen sowie Kenntnis der einschlägigen Normen die ihm übertragenen Arbeiten beurteilen und mögliche Gefahren erkennen kann

ANMERKUNG Zur Beurteilung der fachlichen Ausbildung kann auch eine mehrjährige Tätigkeit auf dem betreffenden Arbeitsgebiet herangezogen werden.

elektrotechnisch unterwiesene Person

elektrotechnisch unterwiesene Person ist, wer durch eine Elektrofachkraft über die ihr übertragenen Aufgaben und die möglichen Gefahren bei unsachgemäßem Verhalten unterrichtet und erforderlichenfalls angeleitet sowie über die notwendigen Schutzeinrichtungen und Schutzmaßnahmen belehrt wurde

Laie

Person, die weder eine Elektrofachkraft noch eine elektrotechnisch unterwiesene Person ist

3.7.2

abgeschlossene elektrische Betriebsstätten

Abgeschlossene elektrische Betriebsstätten sind Räume oder Orte, die ausschließlich zum Betrieb elektrischer Anlagen dienen und unter Verschluss gehalten werden. Der Verschluss darf nur von beauftragten Personen geöffnet werden. Der Zutritt ist nur Fachkräften oder unterwiesenen Personen gestattet.

ANMERKUNG Hierzu gehören z. B. abgeschlossene Schalt- und Verteilungsanlagen, Transformatorzellen, Schalterzellen, Verteilungsanlagen in Blechgehäusen oder in anderen abgeschlossenen Anlagen, Maststationen, Triebwerksräume von Aufzügen.

3.7.3^{E2)}

Schutz gegen direktes Berühren

Als Schutz gegen direktes Berühren gelten alle Maßnahmen zum Schutz von Personen und Tieren vor Gefahren, die sich aus der Berührung mit aktiven Teilen elektrischer Betriebsmittel ergeben.

3.7.4^{E2)}

Schutz bei indirektem Berühren

Als Schutz bei indirektem Berühren gelten alle Maßnahmen zum Schutz von Personen und Tieren bei Gefahren, die durch gefährliche Berührungsspannungen an Körpern (siehe 3.7.6) entstehen.

3.7.5^{E2)}

aktive Teile

Als aktive Teile gelten Leiter und leitfähige Teile von Betriebsmitteln, die unter normalen Betriebsbedingungen unter Spannung stehen.

3.7.6^{E2)}

Körper

Als Körper gelten berührbare leitfähige Teile von Betriebsmitteln, die nicht aktive Teile sind, jedoch im Fehlerfalle unter gefährlicher Berührungsspannung stehen können.

^{E2)} Erläuterung für die Leser dieses Sonderdrucks:

Die hier abgedruckten Definitionen sind wörtlich aus der Norm DIN 31000 (VDE 1000) von 1979. Inzwischen sind folgende neuen Definitionen gebräuchlich, aus DIN VDE 0100-200 (VDE 0100-200):2006 „Errichten von Niederspannungsanlagen – Teil 200: Begriffe“:

Basisschutz

Schutz gegen elektrischen Schlag, wenn keine Fehlzustände vorliegen

ANMERKUNG Im Allgemeinen entspricht bei Niederspannungsanlagen, -netzen und -betriebsmitteln der Basisschutz dem Schutz gegen direktes Berühren.

Fehlerschutz

Schutz gegen Schlag unter den Bedingungen eines Einzelfehlers

ANMERKUNG Im Allgemeinen entspricht bei Niederspannungsanlagen, -netzen und -betriebsmitteln der Fehlerschutz dem Schutz bei indirektem Berühren, vornehmlich im Hinblick auf einen Fehler der Basisisolierung.

aktives Teil

Leiter oder leitfähiges Teil, der/das dazu vorgesehen ist, im üblichen Betrieb unter Spannung zu stehen, einschließlich eines Neutralleiters, vereinbarungsgemäß jedoch nicht eines PEN-Leiters, PEM-Leiters und PEL-Leiters

ANMERKUNG Dieser Begriff besagt nicht unbedingt, dass das Risiko eines elektrischen Schlags besteht.

ANMERKUNG Leiter, die aktive Teile sind, werden als „aktive Leiter“ bezeichnet.

Körper (eines elektrischen Betriebsmittels)

leitfähiges Teil eines elektrischen Betriebsmittels, das berührt werden kann und üblicherweise nicht unter Spannung steht, aber unter Spannung geraten kann, wenn die Basisisolierung versagt

ANMERKUNG Ein leitfähiges Teil eines elektrischen Betriebsmittels, das im Fehlerfall nur über andere Körper unter Spannung geraten kann, ist nicht als Körper zu sehen.

3.7.7^{E3)}

Masse

Als Masse gilt die Gesamtheit aller untereinander leitend verbundenen, nicht aktiven Teile eines elektrischen Betriebsmittels, die auch im Fehlerfall keine gefährliche Berührungsspannung annehmen können.

ANMERKUNG Der Begriff „Masse“ ist nicht identisch mit den Begriffen „nicht aktive Teile (inaktive Teile)“ bzw. „Körper“ (siehe 3.7.6) und der physikalischen Größe „Masse“.

4 Grundlagen für das sicherheitsgerechte Gestalten

4.1 Ziele der Sicherheitstechnik

Technische Erzeugnisse müssen so hergestellt sein, dass sie bei ordnungsgemäßer Errichtung bzw. Aufstellung und bei einer bestimmungsgemäßen Verwendung keine Gefahren verursachen.

Können die nach [Abschnitt 5](#) notwendigen Maßnahmen nicht verwirklicht werden, ohne die zur bestimmungsgemäßen Verwendung des technischen Erzeugnisses gehörenden Funktionen zu beeinträchtigen, so muss das technische Erzeugnis nach Möglichkeit an den Gefahrstellen entsprechend gekennzeichnet sein. Auf diese Angaben darf nur verzichtet werden, wenn mögliche Gefahren ohne weiteres erkennbar oder auch für den Laien offensichtlich voraussehbar sind.

Bei der sicherheitsgerechten Gestaltung ist derjenigen Lösung der Vorzug zu geben, durch die das Schutzziel technisch sinnvoll und wirtschaftlich am besten erreicht wird. Dabei haben im Zweifel die sicherheitstechnischen Erfordernisse den Vorrang vor wirtschaftlichen Überlegungen. Diese Ziele der Sicherheitstechnik sollen in nachstehender Rangfolge verwirklicht werden.

4.1.1 Unmittelbare Sicherheitstechnik

Technische Erzeugnisse sollen so gestaltet werden, dass keine Gefahren vorhanden sind.

4.1.2 Mittelbare Sicherheitstechnik

Ist eine Lösung nach 4.1.1 nicht oder nicht vollständig möglich, sollen besondere sicherheitstechnische Mittel (siehe 5.1.6) Verwendung finden.

4.1.3 Hinweisende Sicherheitstechnik

Führen die Maßnahmen der unmittelbaren oder mittelbaren Sicherheitstechnik nicht oder nicht vollständig zum Ziel, muss angegeben werden, unter welchen Bedingungen eine gefahrlose Verwendung möglich ist.

4.1.3.1 Können bestimmte Gefahren durch die Art des Transportes, der Lagerung, der Aufstellung, der Anbringung, des Anschlusses oder der Inbetriebnahme eines technischen Erzeugnisses verhütet werden, so ist darauf ausreichend hinzuweisen.

4.1.3.2 Müssen zur Verhütung von Gefahren bestimmte Regeln bei der Verwendung, Ergänzung und Instandhaltung eines technischen Erzeugnisses beachtet werden, so ist eine leicht verständliche Gebrauchs- oder Betriebsanleitung mitzuliefern. Sind die betreffenden technischen Erzeugnisse für den deutschen Markt bestimmt, so muss die Gebrauchs- oder Betriebsanleitung zumindest auch deutschsprachig sein.

^{E3)} Erläuterung für die Leser dieses Sonderdrucks:

Diese Definition bezieht sich lediglich auf die elektrische Masse.

4.2 Sicherheitstechnische Sonderbedingungen

Werden technische Erzeugnisse bei ihrer bestimmungsgemäßen Verwendung besonderen Umwelt- oder Betriebsbedingungen ausgesetzt, so müssen sie – gegebenenfalls unter Anwendung zusätzlicher Sicherheitsmaßnahmen – so beschaffen sein, dass sie dieser Norm auch unter den zu erwartenden – und dem Hersteller bekanntzugebenden – Sonderbedingungen genügen.

Besondere Bedingungen solcher Art treten z. B. auf bei Verwendung der technischen Erzeugnisse.

- a) in explosions- oder explosivstoff-, staub- oder feuergefährdeten Arbeitsstätten;
- b) unter ungewöhnlich hohen oder niedrigen Temperaturen;
- c) unter ungewöhnlicher Feuchte oder Nässe;
- d) unter besonderer chemischer, physikalischer oder biologischer Beanspruchung.

4.3 Sicherheitstechnische Sondermaßnahmen

Von den Festlegungen dieser Norm darf im einzelnen abgewichen werden, soweit die notwendige Sicherheit für den Benutzer oder Dritte durch besondere, im Ergebnis gleichwertige, von Beschaffenheit und Funktion des technischen Erzeugnisses unabhängige Maßnahmen erreicht wird.

Als besondere Maßnahmen solcher Art können z. B. angesehen werden:

- a) Einschränkung des freien Zugangs zu den technischen Erzeugnissen, z. B. durch Verwendung in abgeschlossenen oder auf andere Weise besonders gesicherten Arbeitsstätten (z. B. Kesselhaus, Versuchs- oder Prüffeld).
- b) Beschränkung der freien Verwendung der technischen Erzeugnisse auf Fachkräfte bzw. unterwiesene Personen (siehe 3.6.1 und 3.6.2), z. B. in Laboratorien, bei Hochleistungsschaltanlagen.

4.4 Sicherheit bei der Herstellung

Bei der Gestaltung technischer Erzeugnisse ist darauf zu achten, dass auch bei ihrer Herstellung, einschließlich Transport, Zusammenbau, Inbetriebnahme und Demontage, die größtmögliche Sicherheit gegeben ist.

5 Allgemeine Leitsätze und Rahmen-Bestimmungen

5.1 Beanspruchungen

Technische Erzeugnisse müssen so gestaltet werden, dass sie unter Einwirkungen, die bei bestimmungsgemäßer Verwendung zu erwarten sind, keine Gefahr hervorrufen können. Sie müssen insbesondere den zu erwartenden physikalischen und chemischen Beanspruchungen standhalten. Beanspruchungen, die zu Gefahren führen, können z. B. entstehen durch statische oder dynamische Belastungen, durch Einwirkungen von Flüssigkeiten oder Gasen, durch thermische Einwirkungen oder Belastung durch besondere Klimaeinflüsse.

Wenn damit zu rechnen ist, dass ein Missverhältnis zwischen vorgesehener und auftretender Belastung oder ein nicht rechtzeitig erkennbarer Werkstofffehler auftreten kann und dabei schädigende Wirkungen eintreten können, so sind besondere sicherheitstechnische Mittel zu verwenden. Gefahren durch Überlastung, Werkstofffehler oder Verschleiß können unwirksam gemacht werden, z. B.

- a) durch besondere sicherheitstechnische Mittel, die den technischen Prozess oder die Energiezufuhr unterbrechen oder ungefährlich machen, sobald eine Überlastung eintritt (z. B. Schmelzsicherungen, Druckbegrenzungsventile, Sollbruchstellen, Rutschkupplungen). Diese Mittel dürfen ihrerseits keine Gefahren hervorrufen;
- b) durch besondere sicherheitstechnische Mittel, die die durch Werkstofffehler, Verschleiß oder Überlastung wegfliegenden oder fallenden Teile, die eine Gefahr herbeiführen können, auffangen (z. B. Schutzkörbe unter Kreisförderern oder bei Werkstoff-Prüfmaschinen, Schleifkörperschutzhauben, Sicherungsseile oder -ketten).

5.2 Werkstoffe

5.2.1 Allgemeines

Für die Herstellung technischer Erzeugnisse dürfen nur solche Werkstoffe verwendet werden, die den bei bestimmungsgemäßer Verwendung auftretenden physikalischen und chemischen Beanspruchungen standhalten.

5.2.2 Schädigende Werkstoffe

Werkstoffe, die zu schädigenden Wirkungen führen können, sollen für die Herstellung technischer Erzeugnisse nicht verwendet werden. Sie sollen bei allen möglichen Betriebszuständen physiologisch unbedenklich sein, d. h. gefährliche Wirkungen beim Berühren, durch Gase oder Dämpfe (z. B. bei Erwärmung) und durch Strahlung dürfen nicht möglich sein. Ist das nicht sicherzustellen, müssen besondere sicherheitstechnische Mittel angewendet werden.

Reichen auch diese besonderen sicherheitstechnischen Mittel zur Abwendung von schädigenden Wirkungen nicht aus, ist in einer Gebrauchs- oder Betriebsanleitung auf die möglichen Gefahren hinzuweisen.

5.2.3 Alterungsbeständige Werkstoffe

Wo bei bestimmungsgemäßer Verwendung eine Minderung der technologischen Eigenschaften durch Alterung die Sicherheit beeinträchtigen könnte, müssen hinreichend alterungsbeständige Werkstoffe verwendet werden.

5.2.4 Korrosionsgefährdete Teile

Korrosionsgefährdete Teile müssen aus nicht korrodierendem Werkstoff bestehen oder in anderer Weise gegen Korrosion ausreichend geschützt werden, wenn ohne solche Maßnahmen die Sicherheit beeinträchtigt würde.

5.2.5 Elektrische Isolierung

5.2.5.1 Elektrische Betriebsmittel müssen ausreichend isoliert sein, damit eine gefahrlose Funktion des Gerätes und Schutz gegen Gefahren durch unmittelbare Wirkungen des elektrischen Stromes gegeben sind.

Zu diesem Zweck müssen

- a) der Ableitstrom auf den je nach Anwendungsgebiet sicherheitstechnisch als unbedenklich geltenden Grenzwert beschränkt sein und
- b) die Isolierung einen ausreichend hohen Isolationswiderstand haben und
- c) die Isolierung unter Berücksichtigung eines angemessenen Sicherheitsfaktors und von außen wirkender oder betriebsbedingter oder störungsbedingter Überspannungen eine ausreichende Spannungsfestigkeit haben.

5.2.5.2 Isolierungen, die den Schutz gegen gefährliche Berührungsspannungen im Fehlerfalle bewirken (siehe [5.9.1.3](#)), sind hierbei gesondert zu beurteilen.

5.2.5.3 Isolierteile aller Art müssen hinreichend gegen Wärme beständig sein. Isolierteile, die aktive oder stromführende Teile tragen oder abdecken – insbesondere solche, an denen betriebsmäßig Lichtbögen auftreten können, und solche, die bei bestimmungsgemäßer Verwendung in besonders hohem Maße der Erhitzung ausgesetzt sind –, müssen darüber hinaus so hergestellt sein, daß sie sich durch die Wärmebeanspruchung nicht sicherheitsgefährdend verändern.

5.2.5.4 Isolierteile, die aktive Teile (siehe [3.7.5](#)) tragen, müssen hinreichend kriechstromsicher sein, wenn bei bestimmungsgemäßer Verwendung des Betriebsmittels eine sicherheitsgefährdende Minderung der Isolierung durch Feuchte, Verschmutzung oder ähnliche Einwirkungen zu befürchten ist.

5.3 Bewegte Teile

Technische Erzeugnisse müssen so gestaltet werden, dass bewegte Teile, die eine Gefahr darstellen, nicht zugänglich sind oder nicht berührt werden können, soweit dies ohne Einschränkung der Funktion bzw. des Verwendungszweckes möglich ist. Lassen sich außenliegende und der Berührung zugängliche rotierende, oszillierende und translatorisch bewegte Teile nicht vermeiden, müssen zum Schutz gegen dadurch mögliche Gefahren besondere sicherheitstechnische Mittel Verwendung finden.

Rotierende, oszillierende und translatorisch bewegte Teile^{E4)} lassen sich häufig – der Berührung nicht zugänglich – im Maschinen- oder Gerätekörper des technischen Erzeugnisses unterbringen. Einsatzwerkzeuge können sicherheitstechnisch so gestaltet oder so in die Konstruktion einbezogen werden, dass sie nur am Wirkangriff (Arbeitsstelle) frei bleiben, soweit nicht aus funktionellen oder aus sicherheitstechnischen Gründen eine ungehinderte Beobachtung des gesamten Werkzeuges erforderlich ist.

5.4 Oberflächen, Ecken und Kanten

An technischen Erzeugnissen sind, soweit der Verwendungszweck es zulässt, scharfe Ecken und Kanten sowie rauhe Oberflächen, die zu Verletzungen führen können, zu vermeiden. Insbesondere ist darauf zu achten, dass Kanten entgratet, umgebördelt oder eingefasst werden.

5.5 Tritt- und Stehsicherheit, Gleithemmung

Bei technischen Erzeugnissen sind erforderlichenfalls besondere sicherheitstechnische Mittel zur Sicherstellung einer ausreichenden Tritt- und Stehsicherheit für das Arbeits- und Instandhaltungspersonal vorzusehen. Solche sicherheitstechnischen Mittel sind z. B. Arbeits- und Wartungsbühnen. Diese und ihre Zugänge sind gleithemmend zu gestalten und erforderlichenfalls mit Fußleisten und Geländern zu versehen.

5.6 Standsicherheit

Technische Erzeugnisse, die freistehend verwendet werden, müssen ausreichend standsicher gestaltet sein, d.h., sie dürfen auch durch Erschütterungen, durch Winddruck, durch Anstoßen oder andere zu erwartende äußere Belastungen nicht umfallen oder sich nicht unbeabsichtigt fortbewegen lassen.

Kann diese Anforderung durch Formgestalten oder stabile Gewichtsverteilung nicht oder nicht ausreichend erfüllt werden, müssen durch besondere sicherheitstechnische Mittel günstigere Schwerpunktlagen hergestellt, Bewegungen von Teilen des Erzeugnisses begrenzt, Befestigungs- bzw. Arretierungsmöglichkeiten oder, bei fahrbaren technischen Erzeugnissen mit Fahrersitz, erforderlichenfalls Umsturzsicherheitsvorrichtungen vorgesehen werden.

Kann die geforderte Standsicherheit nur durch besondere Maßnahmen am Aufstellungs- oder Verwendungsort oder durch eine bestimmte Verwendungsart erreicht werden, so muss am Erzeugnis selbst oder in Gebrauchs- oder Betriebsanleitungen darauf hingewiesen werden.

5.7 Transportgerechte Gestaltung

Technische Erzeugnisse, die nicht von Hand bewegt oder transportiert werden können, müssen mit geeigneten Anschlagseinrichtungen für den Transport mit Hebe- und Fördermitteln ausgerüstet sein oder werden können. Die Anschlagseinrichtungen müssen sich vom Transportpersonal gefahrlos erreichen lassen oder ein automatisches Anschlagen ermöglichen. Sie müssen unter Berücksichtigung des Schwerpunktes so angeordnet werden, dass die technischen Erzeugnisse bei sachgerechtem Anheben nicht kippen können.

Betriebsmäßig lösbare Teile technischer Erzeugnisse, wie z. B. Werkzeuge und Vorrichtungen, die ihres Gewichtes wegen nicht von Hand transportiert werden können, sollen durch eine Gewichtsangabe gekennzeichnet sein. Diese muss deutlich sichtbar angebracht werden und erkennen lassen, ob sich die Angabe auf das lösbare Teil oder das komplette Erzeugnis bezieht.

E4) Erläuterung für die Leser dieses Sonderdrucks:

rotierend = kreisend bzw. drehend;

oszillierend bewegt = schwingend (hin und her und/oder auf und ab bewegt);

translatorisch bewegt = gerade fortschreitend.

5.8 Beim Betrieb auftretende Gefahren

5.8.1 Wegfliegende Teile

Können beim Betrieb technischer Erzeugnisse Werkstücke, Werkzeuge oder Teile von beiden – auch Späne und Stäube – wegfliegen, sind, soweit damit Gefahren verbunden sind, besondere sicherheitstechnische Mittel anzuwenden.

Besondere sicherheitstechnische Mittel zum Vermeiden gefährlicher Auswirkungen des Wegfliegens sind beispielsweise Schutzhauben, Schutzfenster, Absauganlagen sowie Rückschlagsicherungen an Holzbearbeitungsmaschinen.

Hinweisende sicherheitstechnische Mittel dürfen nur in Ausnahmefällen verwendet werden.

5.8.2 Lärm und Erschütterungen

Technische Erzeugnisse müssen so gestaltet werden, dass Lärm- und Erschütterungen so gering wie möglich gehalten werden. Als konstruktive Maßnahmen hierzu bieten sich z. B. an: Wahl günstiger Drehzahlen, Verwenden geräuscharmer Antriebe, Verwenden schwingungsdämpfender Bauteile zwischen Maschine und Fundament.

Sind diese Maßnahmen nicht möglich oder nicht ausreichend, so muss die Lärmausbreitung durch besondere Mittel, z. B. Schalldämmung, Schalldämpfung, Schallableitung, vermindert werden.

5.8.3 Wärme und Kälte

Können warme oder unterkühlte Teile technischer Erzeugnisse zu Gefahren führen, müssen sie gegen Berühren abgeschirmt werden, soweit das ohne Beeinträchtigung der Funktion möglich ist. Auch Wärmestrahlung, die zu Gefahren führen kann, muss durch besondere sicherheitstechnische Mittel (z. B. Abschirmung) vermieden werden.

5.8.4 Betriebsmäßig auftretende Flüssigkeiten

Technische Erzeugnisse, die mit Flüssigkeiten arbeiten, müssen so gestaltet werden, dass die Flüssigkeiten nicht in gefahrbringender Weise in den Arbeitsraum, in dem sich Personen aufhalten (z. B. wegen Rutschgefahr), und an den Körper von Personen (wegen Gefährdung der Gesundheit) gelangen können.

5.8.5 Stäube, Dämpfe, Gase

Werden einem technischen Erzeugnis gefährliche Stäube, Dämpfe oder Gase für das anzuwendende Verfahren zugeführt oder entstehen im Arbeitsprozess derartige Medien, so müssen diese sicher umschlossen sein oder so abgeleitet und unschädlich gemacht werden, dass sie keine Gefahr bilden.

5.9 Elektrische Energie

5.9.1 Gefahren durch unmittelbare Wirkungen der elektrischen Energie

5.9.1.1 Allgemeines

Elektrische Betriebsmittel müssen so hergestellt sein, dass bei bestimmungsgemäßer Verwendung hinreichender Schutz gegen Gefahren durch unmittelbare Wirkungen der elektrischen Energie besteht.

Elektrische Betriebsmittel müssen so gestaltet und bemessen sein, dass unerwünschte oder unbeabsichtigte gefahrbringende Wirkungen der elektrischen Energie bei bestimmungsgemäßer Verwendung verhindert oder zumindest unschädlich gemacht sind. Die hierfür notwendigen Einrichtungen müssen der Funktion der elektrischen Betriebsmittel angemessen gestaltet und zweckmäßig angebracht sein sowie ausreichend sicher wirken.

5.9.1.2 Schutz gegen direktes Berühren^{E5)}

5.9.1.2.1 Elektrische Betriebsmittel müssen unter Berücksichtigung der Betriebszustände, die der Benutzer oder Dritte herbeiführen können, so gestaltet sein, dass der Benutzer oder Dritte aktive Teile (siehe 3.7.5) ohne Hilfsmittel oder Werkzeuge nicht berühren bzw. sich ihnen nicht gefahrbringend nähern können (siehe jedoch 5.9.1.2.3).

5.9.1.2.2 Teile von elektrischen Betriebsmitteln, die den Schutz gegen direktes Berühren bewirken, dürfen nur mit Hilfe von Werkzeug oder Schlüssel entfernbar oder zu öffnen sein (siehe jedoch 5.9.1.2.3), wenn die unter Spannung stehenden Teile nicht durch das Entfernen oder Öffnen dieser Teile in einen spannungslosen Zustand versetzt werden.

5.9.1.2.3 Auf den Schutz nach den 5.9.1.2.1 und 5.9.1.2.2 darf verzichtet werden, wenn eine der folgenden Bedingungen eingehalten wird:

- a) Die anstehende Spannung übersteigt nicht einen für den jeweiligen Anwendungsfall als ungefährlich geltenden Wert und wird in einer Stromquelle erzeugt, die diesen Grenzwert auch im Falle eines Fehlers im zugehörigen Stromkreis nicht überschreiten lässt.

ANMERKUNG Durch sichere elektrische Trennung ist verhindert, dass von äußeren Stromkreisen, insbesondere von der Anschlussstelle an das Versorgungsnetz her, gefährliche Spannungen auf das elektrische Betriebsmittel übertreten können.

- b) Bei direktem Berühren (siehe Abschnitt 3.7.3) kann nur ein nach Frequenz, Einwirkungsdauer und Energieinhalt auf einen ungefährlichen Wert begrenzter Strom fließen.
- c) Bei zur selbständigen Verwendung nicht geeigneten oder bestimmten elektrischen Betriebsmitteln wird der notwendige Schutz durch Einbau in ein (größeres) elektrisches Betriebsmittel bewirkt, das seinerseits den Anforderungen zum Schutz gegen direktes Berühren genügt.
- d) Der notwendige Schutz wird durch das Aufstellen in abgeschlossenen elektrischen Betriebsstätten bewirkt.

5.9.1.3 Schutz bei indirektem Berühren^{E6)}

5.9.1.3.1 Elektrische Betriebsmittel müssen so hergestellt sein, dass Personen auch bei einem Fehler der Betriebsisolierung des elektrischen Betriebsmittels oder beim Auftreten von Lichtbögen gegen gefährliche Berührungsspannungen geschützt sind. Zu diesem Zweck müssen die elektrischen Betriebsmittel so ausgeführt sein, dass eine der in der folgenden Aufzählung a) bis c) angegebenen Schutzmaßnahmen verwirklicht ist.

- a) Die Körper (siehe 3.7.6) sind so hergestellt, dass sie in eine der mit Schutzleiter wirkenden Schutzmaßnahmen einbezogen werden können. Zu diesem Zweck ist sichergestellt, dass die vorgesehenen Anschlussmittel und Verbindungsstellen elektrisch und mechanisch einwandfrei beschaffen sind und dass alle Körper untereinander und mit dem Schutzleiter sicher verbunden sind.
- b) Berührbare leitfähige Teile sind nicht vorhanden oder von Teilen, die im Falle des Versagens der Betriebsisolierung eine gefährliche Berührungsspannung annehmen können, durch eine zusätzlich zur Betriebsisolierung vorhandene Isolierung (Schutzisolierung) getrennt. Es sind keine Vorrichtungen vorhanden, um solche Teile mit einem Schutzleiter verbinden zu können.
- c) Die elektrischen Betriebsmittel werden mit Spannungen betrieben, von denen auch im Fehlerfalle keine Gefahr ausgehen kann (siehe 5.9.1.2.3a).

ANMERKUNG zu der Aufzählung a) bis c):

Die hier aufgeführten Schutzmaßnahmen beinhalten die Grundsätze für die „Schutzklassen I, II bzw. III“ in einzelnen besonderen VDE-Bestimmungen für elektrische Betriebsmittel.

5.9.1.3.2 Innerhalb der elektrischen Betriebsmittel dürfen die Schutzmaßnahmen nach 5.9.1.3.1 miteinander kombiniert werden, soweit dadurch die Wirkung der einzelnen Schutzmaßnahmen nicht beeinträchtigt wird.

^{E5)} Inzwischen als „Basisschutz“ nach DIN VDE 0100-200 (VDE 0100-200):2006-06 bezeichnet, siehe Seite 11 dieses Sonderdrucks.

^{E6)} Inzwischen als „Fehlerschutz“ nach DIN VDE 0100-200 (VDE 0100-200):2006-06 bezeichnet, siehe Seite 11 dieses Sonderdrucks.

5.9.1.3.3 Zu selbständiger Verwendung nicht bestimmte elektrische Betriebsmittel brauchen nicht nach **5.9.1.3.1** ausgeführt zu sein, wenn der Schutz bei indirektem Berühren durch die Beschaffenheit des elektrischen Betriebsmittels gegeben ist, dessen Bestandteil sie werden.

5.9.2 Gefahren durch beabsichtigte Einwirkungen der elektrischen Energie auf Mensch und Tier

Von beabsichtigten Einwirkungen der elektrischen Energie auf Menschen und Tiere in Form von Stromleitung, Strahlung, elektrischen Feldern und dergleichen darf nur mit eigens dafür bestimmten elektrischen Betriebsmitteln Gebrauch gemacht werden und soweit dabei - gegebenenfalls durch zusätzliche Sicherheitsvorkehrungen - für den notwendigen Schutz gegen Gefahren in besonderem Maße gesorgt ist (Beispiele: elektromedizinische Geräte, Elektrozaun-Geräte).

ANMERKUNG Hierunter fallen auch elektrische Betriebsmittel, bei denen von begrenzter, ungefährlicher Stromleitung durch den menschlichen Körper bestimmungsgemäß Gebrauch gemacht wird (Beispiele: einpolige Spannungsprüfer, elektronische Tast-Schalter).

5.9.3 Gefahren durch mittelbare Wirkungen der elektrischen Energie

5.9.3.1 Elektrische Betriebsmittel müssen so hergestellt sein, dass Gefahren aus nicht leitungsgebundenen Wirkungen der elektrischen Energie (z. B. bei Röntgeneinrichtungen, Rundfunksendern, Diathermie-Geräten) nicht auftreten können. Soweit nicht leitungsgebundene Wirkungen der elektrischen Energie funktionsbedingt auftreten, muss dafür gesorgt werden, dass gefährliche Wirkungen außerhalb des gewollten Wirkungsbereiches nicht auftreten können.

Die Vorkehrungen nach dem ersten und zweiten Absatz dieses Abschnittes müssen auch dazu geeignet sein, andere elektrische Betriebsmittel gegen vorhersehbare Funktionsstörungen zu schützen, durch die Gefahren entstehen können (z. B. Störungen in ferngesteuerten elektrischen Betriebsmitteln als Folge der Einwirkungen von Funkstörungen durch andere elektrische Betriebsmittel).

5.9.3.2 Elektrische Betriebsmittel müssen so hergestellt sein, dass die in oder an ihnen – auch bei Überstrom (Überlast, Kurzschluss) – auftretenden Temperaturen die Beschaffenheit und die Funktion des Betriebsmittels und seine Umgebung nicht in sicherheitsgefährdender Weise beeinträchtigen.

5.9.3.3 Elektrische Betriebsmittel müssen so hergestellt sein, dass auch eine Gefahr durch andere, nicht elektrische Wirkungen vermieden ist. Zu diesem Zweck müssen z. B. mechanische oder thermische Wirkungen durch Kurzschluss, UV-Strahlung, Ultraschall-Strahlung, Entwicklung von gesundheitsschädlichen Gasen, Dämpfen, Wirkungen von Explosionen, Implosionen und Detonationen, Lärm, Schwingungen, Erschütterungen und dergleichen auf ein unschädliches Maß begrenzt werden.

5.9.4 Gefahren durch äußere Einwirkungen auf elektrische Betriebsmittel

5.9.4.1 Einwirkungen aus der Umgebung

Elektrische Betriebsmittel müssen gegen die zu erwartenden, sicherheitsgefährdenden Einwirkungen aus der Umgebung – z. B. durch Stoß, Druck, Feuchte, Eindringen von Fremdkörpern (auch von Staub) oder Erschütterungen – hinreichend geschützt sein.

5.9.4.2 Überlastung

5.9.4.2.1 Elektrische Betriebsmittel müssen so beschaffen sein, dass sie auch bei einer Überlastung, wie sie bei bestimmungsgemäßer Verwendung auftreten kann, nicht in sicherheitsgefährdender Weise beeinträchtigt werden können.

5.9.4.2.2 Die elektrischen Betriebsmittel müssen selbsttätig wirkende Einrichtungen zur Unterbrechung oder Begrenzung der Stromaufnahme enthalten, wenn die Forderung nach 5.9.4.2.1 ohne solche Einrichtungen nicht eingehalten werden kann. Dies gilt nur, soweit die elektrischen Betriebsmittel bei bestimmungsgemäßer Verwendung zeitweilig der Aufsicht oder der Beeinflussung durch den Benutzer entzogen sind und eine etwaige Überlastung Gefahren mit sich bringt.

5.9.5 Aufschriften und Kennzeichnung

5.9.5.1 Elektrische Betriebsmittel müssen mit dauerhaft angebrachten, leicht erkennbaren und eindeutigen Aufschriften versehen sein, aus denen alle Merkmale ersichtlich sind, die für gefahrlose Verwendung und sichere Funktion wichtig sind.

Hierzu gehören insbesondere die elektrischen Nenndaten, Angaben über den ordnungsgemäßen Anschluss bei bestimmungsgemäßer Verwendung, etwaige besondere Betriebsarten und Betriebsbedingungen. Mit Hilfe der Aufschriften müssen auch Herkunft und Typ der elektrischen Betriebsmittel identifizierbar sein.

5.9.5.2 Elektrische Betriebsmittel, die während der bestimmungsgemäßen Verwendung nach Wahl des Verwenders (Benutzers) auf unterschiedliche Betriebs- oder Funktionsarten oder -zustände eingestellt werden können, müssen Vorrichtungen oder Kennzeichnungen haben, die den jeweils gewählten Zustand (Funktion) eindeutig erkennen lassen.

Mittelbar diesem Zweck dienende Vorrichtungen (z. B. Messinstrumente, Funktionswahl-Schalter) müssen so ausgeführt sein, dass der quantitativ oder qualitativ jeweils angezeigte Wert dem tatsächlichen Wert der dargestellten Größe mit ausreichender Genauigkeit entspricht.

ANMERKUNG Unterschiedliche Betriebs- oder Funktionsart im vorstehenden Sinne ist z. B. bei Geräten gegeben, die auf verschiedene Nennspannungen eingestellt werden können.

5.9.5.3 Elektrische Betriebsmittel, von denen eine unvermeidbare, funktionsbedingte Gefahr ausgehen kann, müssen entsprechend gekennzeichnet sein. Hierauf darf nur verzichtet werden, wenn die möglichen Gefahren ohne weiteres erkennbar oder - auch für den Laien - offensichtlich voraussehbar sind.

5.9.5.4 Soweit die erforderlichen Angaben nach den Abschnitten 5.9.5.1 bis 5.9.5.3 wegen der Beschaffenheit der elektrischen Betriebsmittel nicht als Aufschrift auf diesen selbst angebracht werden können, müssen sie dem Benutzer in anderer Weise zuverlässig, eindeutig und wirksam bekanntgegeben werden, z. B. in Form der Begleitpapiere (Bedienungsanleitung, Montageanleitung). Diese gelten in einem solchen Falle als Bestandteil des elektrischen Betriebsmittels.

5.9.6 Nennbetrieb

Die elektrischen Betriebsmittel müssen so hergestellt sein, dass sie mit den in den Nenndaten angegebenen Werten bei bestimmungsgemäßer Verwendung betrieben werden können, ohne dass dabei Personen, Tiere oder Sachen gefährdet oder die Funktion des Betriebsmittels gefahrbringend beeinflusst werden.

Soweit es für die Sicherheit erforderlich ist, müssen die Abweichungen der Betriebsdaten von den Nenndaten innerhalb angemessener Toleranzen liegen.

5.9.7 Sonstige Anforderungen

5.9.7.1 Elektrischer Anschluss und elektrische Verbindungen

5.9.7.1.1 Elektrische Betriebsmittel müssen mit Einrichtungen versehen sein, die ihren sicheren Anschluss an das Netz (bei fest anzuschließenden elektrischen Betriebsmitteln durch eine Fachkraft) ermöglichen.

5.9.7.1.2 Die hierfür erforderlichen Anschlussmittel – z. B. Steckvorrichtungen, Anschluss- und Verbindungsleitungen, Klemmen – müssen den auftretenden elektrischen (Nennspannung, Nennstrom, Nennleistung), thermischen (innere und äußere Erwärmung) und mechanischen (Zug, Druck, Verdrehung usw.) Beanspruchungen standhalten. Besonders gefährdete Stellen müssen durch Anordnung, Gestaltung oder zusätzliche Einrichtungen gesichert werden.

5.9.7.1.3 Insbesondere müssen die Strombahnen und die leitenden Verbindungen stromführender oder aktiver Teile so hergestellt und erforderlichenfalls zusätzlich so gesichert sein, dass sie sich bei betriebsgemäßer Belastung nicht unzulässig erwärmen, lockern oder in anderer gefahrbringender Weise verändern.

5.9.7.2 Luftstrecken, Kriechstrecken und Abstände

5.9.7.2.1 An allen Stellen, an denen eine Gefahr infolge anstehender Spannung, Fehlerstrom, Ableitstrom oder ähnlicher Einwirkungen zu befürchten ist, müssen hinreichend bemessene Luftstrecken, Kriechstrecken und Abstände vorgesehen sein.

5.9.7.2.2 Soweit Luftstrecken und Kriechstrecken in besonderem Maße – z. B. durch Verwendung chemisch-aggressiver Flüssigkeiten, Auftreten von Kohleabriebstaub bei bestimmungsgemäßer Verwendung des Betriebsmittels – beeinträchtigt werden können, müssen diese durch Lage, Formgebung, Werkstoffauswahl oder in anderer geeigneter Weise gegen Verschmutzung, Feuchte oder andere schädliche Einwirkungen geschützt sein.

5.9.7.2.3 Von den Anforderungen der Abschnitte 5.9.7.2.1 und 5.9.7.2.2 darf abgewichen werden, wenn auf andere, mindestens gleichwertige Weise sichergestellt ist, dass im Fehlerfalle – z. B. durch Überlastung oder Kurzschluss – keine sicherheitsgefährdenden Erscheinungen infolge von Beeinträchtigungen von Luftstrecken und Kriechstrecken auftreten.

5.10 Pneumatische und hydraulische Ausrüstung

Bei der pneumatischen und hydraulischen Ausrüstung von technischen Erzeugnissen ist insbesondere darauf zu achten,

- a) dass im technischen Erzeugnis der zulässige Druck nicht überschritten werden kann (z. B. durch Druckbegrenzungseinrichtungen);
- b) dass bei Druckausfall oder -abfall keine gefährlichen Vorgänge ausgelöst werden können (z. B. bei Kraftspannfuttern);
- c) dass von austretenden Druckflüssigkeiten oder Druckgasen keine Gefahr ausgehen kann (z. B. mittels Entspannen oder Ableiten);
- d) dass pneumatische und hydraulische Ausrüstungen selbst gegen schädigende Einwirkung von außen geschützt sind.

5.11 Gastechische Ausrüstung für brennbare Gase

Bei der gastechischen Ausrüstung von technischen Erzeugnissen ist insbesondere darauf zu achten,

- a) dass ein unbeabsichtigtes Ausströmen von Gas, das zu einer Gefahr führen kann, vermieden wird (z. B. durch Druckbegrenzungseinrichtungen, Zündsicherungen, Gasmangelsicherungen);
- b) dass die Brennsicherheit bei Gasverbrauchseinrichtungen gegeben ist (z. B. durch einwandfreies Überzünden zum Hauptbrenner, einwandfreies Durchzünden der einzelnen Flammen des Hauptbrenners, Erhalten der Flammenstabilität);
- c) dass der CO-Gehalt im Abgas die zulässigen Grenzen nicht überschreitet (z. B. durch geeignete Wahl des Brenners und durch ausreichende Luftzufuhr, so dass auch ein teilweises Ansaugen von Abgas anstelle von Frischluft in den Brenner nicht möglich ist);
- d) dass eine Rückzündung in gasführende Teile verhindert wird.

5.12 Ausrüstung für flüssige und feste Brennstoffe

Bei der wärmetechnischen Ausrüstung von technischen Erzeugnissen, die mit flüssigen oder festen Brennstoffen betrieben werden, ist insbesondere darauf zu achten,

- a) dass bei der Brennstoffbeschickung keine Gefahr auftreten kann;
- b) dass – soweit eine Brennstoffbevorratung in unmittelbarer Nähe der Feuerstätte notwendig ist – sich daraus keine Gefahren ergeben;
- c) dass eine ausreichende Verbrennungsluftzufuhr gewährleistet wird;
- d) dass die Schadstoffe im Rauchgas die zulässigen Grenzen nicht überschreiten.

5.13 Ausrüstung für Treibmittel-Energie

Technische Erzeugnisse, die als Energieträger Treibmittel – insbesondere Explosivstoffe – verwenden, müssen so gestaltet sein, dass ungewollte, gefahrbringende Auslösung verhindert wird.

5.14 Einrichtungen zum Schalten, Steuern und Regeln

5.14.1 Steuerungen und Stellteile

Energien aller Art bei technischen Erzeugnissen müssen so geschaltet und gesteuert werden können, dass größtmögliche Sicherheit gegeben ist.

Stellteile müssen so gestaltet, angeordnet oder gesichert werden, dass ungewolltes, versehentliches Schalten oder Auslösen von Bewegungs- oder sonstigen Arbeitsvorgängen verhindert oder wenigstens erschwert wird. Bei handgesteuerten Vorgängen soll die Sinnfälligkeit der Schaltbewegungen gewährleistet sein.

Lässt sich das nicht verwirklichen, müssen entsprechende allgemein verständliche Bildzeichen oder auch, wenn diese nicht ausreichen, Textangaben vorhanden sein.

Bei selbsttätigen oder teilweise selbsttätig wirkenden Schalt- und Steuervorgängen muss die Folge der Funktionen so sichergestellt sein, dass gefährliche Überlagerungen oder Überkreuzungen von Vorgängen ausgeschlossen sind. Entsprechende Verriegelungen oder Begrenzungen sind vorzusehen. Steuerleitungen sind so zu gestalten, dass Beschädigungen der Leitungen nicht zu gefährdenden Schalt- und Steuervorgängen führen können.

Wenn eine Kopplung oder Verriegelung von Steuerung und besonderen sicherheitstechnischen Mitteln an technischen Erzeugnissen vorgesehen ist, müssen diese zwangsläufig wirken. Diese Forderung ist erfüllt, wenn z. B.

- a) mit Einleiten (Einschalten) des Arbeits- oder Bewegungsvorganges die sicherheitstechnischen Mittel wirksam werden;
- b) das Einleiten (Einschalten) des Arbeits- und Bewegungsvorganges erst nach Wirksamwerden der sicherheitstechnischen Mittel möglich ist;
- c) bei Annäherung an den Gefahrenbereich während der Gefährdungszeit der Arbeits- und Bewegungsvorgang zwangsläufig unterbrochen wird.

5.14.2 Gefahrenschaltungen

Kraftbetriebene technische Erzeugnisse müssen mit Gefahrenschaltung (Notschaltung)^{E7)} ausgerüstet werden, wenn

- a) im Gefahrenbereich der Betätigungsschalter zum Abschalten gefahrbringender Bewegungen nicht schnell und gefahrlos erreicht werden kann;
- b) mehrere bewegliche Einheiten vorhanden sind, von denen eine Gefahr ausgehen kann und die nicht über einen gemeinsamen, schnell und gefahrlos erreichbaren Schalter abzuschalten sind;
- c) durch Abschalten bestimmter Einheiten eine zusätzliche Gefahr eintreten kann;
- d) die technischen Erzeugnisse vom Steuerstand nicht vollständig übersehen werden können.

Gefahrenschalter müssen in ausreichender Anzahl vorhanden, von allen Steuer- und Beschickungsstellen schnell und gefahrlos erreichbar angebracht und auffällig rot gekennzeichnet sein.

Durch das Betätigen der Gefahrenschaltung darf weder bei eingeschalteten noch bei abgeschalteten technischen Erzeugnissen eine gefährliche Bewegung ausgelöst werden; erforderlichenfalls müssen auslaufende gefährdende Bewegungen abgebremst werden. Nach Abschalten durch einen Gefahrenschalter darf eine Wiederinbetriebnahme des technischen Erzeugnisses erst dann möglich sein, nachdem der Gefahrenschalter selbst

^{E7)} Erläuterung für die Leser dieses Sonderdrucks:

Siehe 9.2.5.4 „Handlungen im Notfall (NOT-HALT, NOT-AUS)“ von DIN EN 60204-1 (VDE 0113-1):2007-06 „Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen – Teil 1: Allgemeine Anforderungen (IEC 60204-1:2005, modifiziert); Deutsche Fassung EN 60204-1:2006“.

(bei mechanischer Verriegelung) oder ein anderes dafür vorgesehenes Stellteil (bei elektrischer Verriegelung) von Hand in die Einschalt- oder Zustimmungstellung gebracht wurde.

Bei selbsttätigem Arbeitsablauf muss es möglich sein, die einzelnen beweglichen Einheiten nach Umschalten auf Handbetrieb zu fahren, soweit es zur Abwendung von Gefahren erforderlich ist.

5.14.3 Besondere Sicherheitsschaltungen

Technische Erzeugnisse, bei denen es erforderlich ist, beim Einrichten, Warten, Inspizieren und Instandsetzen den Gefahrenbereich zu begehen oder mit Körperteilen (z. B. Hände oder Arme) in den Gefahrenbereich einzudringen, müssen gegen irrtümliches Inbetriebsetzen gesichert werden können.

Diese Forderung kann erfüllt werden, z. B. durch

- a) mechanisches Absichern des Gefahrenbereiches und gleichzeitige zwangsläufige Unterbrechung der Steuerung oder der Energiezufuhr des technischen Erzeugnisses (z. B. Sicherungsstützen oder -blöcke bei Pressen und Druckgießmaschinen);
- b) in „AUS“-Stellung mehrfach mit Vorhängeschlössern abschließbare Hauptschalter;
- c) Steuerungs- oder Verriegelungselemente, die sich direkt an der Gefahrenstelle befinden und nur von dort aus die Inbetriebnahme sperren oder freigeben;
- d) abziehbare Zündschlüssel.

Handgehaltene kraftbetriebene Maschinen oder Werkzeuge müssen vom Benutzer ohne Loslassen der Handgriffe des Werkzeuges ausgeschaltet werden können oder mit einem Einschalter, der sich beim Loslassen selbsttätig in die „AUS“-Stellung begibt, versehen sein.

5.15 Anforderungen an die gefahrlose Funktion

5.15.1 Technische Erzeugnisse müssen so beschaffen sein, daß sie während einer angemessenen Nutzungsdauer ihrer bestimmungsgemäßen Verwendung entsprechend sicher bleiben, d. h. keine Gefahr herbeiführen können.

Bei elektrischen Betriebsmitteln darf auch nach Ablauf der angemessenen Nutzungsdauer keine Gefahr durch noch funktionsfähige Geräte herbeigeführt werden.

5.15.2 Teile von elektrischen Betriebsmitteln, die betriebsmäßig elektrische Stromkreise schließen oder unterbrechen, müssen geeignet sein, den entsprechend ihren Nenndaten (Strom, Spannung, Frequenz, Schalthäufigkeit usw.) zu erwartenden elektrischen, thermischen und mechanischen Beanspruchungen standzuhalten.

Insbesondere muss eine sichere Schaltfunktion gegeben sein, soweit hiervon die Sicherheit abhängt.

5.15.3 Zur Abwendung von Gefahren, die von der Funktion der elektrischen Betriebsmittel – selbst bei deren einwandfreier Beschaffenheit - ausgehen können, müssen neben den nach 5.9.1.1, zweiter Absatz geforderten Maßnahmen Einrichtungen vorhanden sein, mit denen im Falle drohender Gefahr der Energiefluss unterbrochen werden kann.

Es muss die notwendige Sicherheit dagegen gegeben sein, dass solche Einrichtungen versehentlich oder irrtümlich unwirksam gemacht werden.

5.15.4 Elektrische Betriebsmittel müssen zwangsläufig und sicher wirkende Einrichtungen haben, mit denen ungewolltes Inbetriebsetzen aus den Zuständen „Außer Betrieb“ oder „Halt“ heraus verhindert ist, wenn durch unerwartetes Inbetriebsetzen Personen gefährdet werden können.

5.15.5 Besondere sicherheitstechnische Mittel müssen vor dem Inverkehrbringen als zuverlässig erprobt sein. Wenn Kopplungen oder Verriegelungen mit der Steuerung vorgesehen sind, darf das Versagen besonderer sicherheitstechnischer Mittel oder einzelner Teile davon entweder die Schutzwirkung nicht aufheben, oder es muss das Abschalten gefährlicher Vorgänge bewirkt werden. Komplizierte sicherheitstechnische Systeme sollen mit Einrichtungen zur Selbstüberwachung ausgerüstet werden.

5.16 Wirksamkeit besonderer sicherheitstechnischer Mittel

Die Wirksamkeit besonderer sicherheitstechnischer Mittel soll für die vorbestimmte Aufgabe zwangsläufig sein, d.h., es darf nicht leicht möglich sein, sie unwirksam zu machen. Kann die zwangsläufige Wirkung der besonderen sicherheitstechnischen Mittel nicht erreicht werden, muss angegeben werden (z. B. an dem Erzeugnis oder in der Gebrauchs- bzw. Betriebsanleitung), unter welchen Bedingungen eine gefahrlose Verwendung des technischen Erzeugnisses möglich ist.

5.17 Elektrostatische Aufladung

Gefährliche elektrostatische Aufladungen müssen verhindert werden; wenn das nicht möglich ist, müssen besondere sicherheitstechnische Mittel zum Unschädlichmachen bzw. Ableiten vorgesehen werden.

5.18 Betriebsstoffe und Arbeitsstoffe

5.18.1 Die für das Betreiben technischer Erzeugnisse und das Arbeiten mit technischen Erzeugnissen notwendigen Betriebsstoffe und Arbeitsstoffe sollen keine schädigenden Wirkungen haben. Kann auf gefährliche Betriebsstoffe und Arbeitsstoffe nicht verzichtet werden (z. B. bei Härtereianlagen, Farbspritzanlagen, Galvanisierungsanlagen), müssen besondere sicherheitstechnische Mittel zur Abwehr der Gefahr vorgesehen oder ersatzweise in der Gebrauchs- oder Betriebsanleitung die Bedingungen angegeben werden, unter denen eine gefahrlose Verwendung möglich ist.

5.18.2 Technische Erzeugnisse, für die Betriebsstoffe (z. B. Flüssigkeiten, Gase) benötigt werden, müssen so gestaltet werden, dass austretende Betriebsstoffe sich nicht in ihnen oder in ihrer Umgebung in gefahrdrohender Menge ansammeln können.

5.19 Menschengerechte (ergonomische) Gestaltung

Technische Erzeugnisse sollen so gestaltet werden, dass das Arbeiten mit ihnen bzw. ihre Verwendung weitgehend erleichtert wird. Damit wird auch einer möglichen Gefahr vorgebeugt. Das bedeutet, dass das Erzeugnis den Körpermaßen, den Körperkräften und den anatomischen und physiologischen Gegebenheiten des Menschen angepasst werden soll.

Erläuterungen

Zum Inhalt

Innerhalb des Deutschen Normenwerkes hat DIN 31000 (VDE 1000) die gleiche Bedeutung und Funktion wie die bisherige Vornorm DIN 31000.

Der methodische Grundgedanke kommt in den [Abschnitten 4.1.1 bis 4.1.3](#) deutlich zum Ausdruck:

Eine Drei-Stufen-Methode für das sicherheitsgerechte Gestalten im Rahmen der Gesamtlösung einer Konstruktionsaufgabe.

Der Gestalter soll zunächst versuchen, seine Aufgabe so zu lösen, dass bei der bestimmungsgemäßen Verwendung des Erzeugnisses keine Gefahren für Leben und Gesundheit vorhanden sind. Zum Beispiel wird es häufig möglich sein, die beweglichen Elemente eines Erzeugnisses so in einem Maschinen- oder Gerätekörper unterzubringen, dass sie für den Benutzer nicht erreichbar sind ([Abschnitt 4.1.1](#) „Unmittelbare Sicherheitstechnik“).

Ist das aus konstruktions- oder funktionsbedingten zwingenden Gründen nicht möglich, so sollen besondere sicherheitstechnische Mittel (Schutzmaßnahmen) angewendet werden, um die Gefahren wirkungslos zu machen. Die Mittel sind funktional in die Gesamtlösung einzubeziehen ([Abschnitt 4.1.2](#) „Mittelbare Sicherheitstechnik“).

Können auch besondere sicherheitstechnische Mittel bei Berücksichtigung der unter [Abschnitt 4.1](#) genannten Gesichtspunkte keine Anwendung finden, muss angegeben werden, unter welchen Bedingungen eine gefahrlose Verwendung des Erzeugnisses möglich ist. Soweit von der „Hinweisenden Sicherheitstechnik“ Gebrauch gemacht wird, muss sichergestellt werden, dass der Hinweis auch an den Benutzer gelangt. Dies soll z. B. durch Aufschrift oder Hinweis in der Gebrauchs- oder Betriebsanleitung geschehen.

Die „Hinweisende Sicherheitstechnik“ ist in Verbindung mit der „Unmittelbaren Sicherheitstechnik“ und der „Mittelbaren Sicherheitstechnik“ auch dann anzuwenden, wenn bei Erzeugnissen eine Gefahr nur durch ein bestimmtes Verhalten des Benutzers verhindert werden kann ([Abschnitt 4.1.3](#) „Hinweisende Sicherheitstechnik“).

Grundsätzlich sei jedoch noch einmal darauf hingewiesen, dass alle Einzelangaben dieser Norm und dabei insbesondere die „Allgemeinen Leitsätze und Rahmen-Bestimmungen“ nach [Abschnitt 5](#) unter Voraussetzung folgender grundsätzlicher Feststellungen gelten:

gem. A1

- Diese Norm gilt für alle technischen Erzeugnisse ausgenommen solcher, die in den Anwendungsbereich der Normen DIN EN ISO 12100-1 und DIN EN ISO 12100-2 fallen, sofern diese nach [Abschnitt 3.3](#) „bestimmungsgemäß“ verwendet werden.
- Nach [Abschnitt 4.1](#), erster Absatz, wird darüber hinaus eine ordnungsgemäße Errichtung bzw. Aufstellung als Voraussetzung genannt.
- Nach [Abschnitt 3.2](#) werden nur solche Gefahren berücksichtigt, deren Wirkungen ein nach dem jeweiligen Stand der Technik zumutbares Risiko überschreiten.
- Nach [Abschnitt 4.2](#) ist dem Hersteller technischer Erzeugnisse bekannt zu geben, wenn sie unter besonderen Umwelt- oder Betriebsbedingungen verwendet werden, unter denen besondere Beanspruchungen auftreten.

Die Wiederholung der grundsätzlichen Feststellungen an einigen speziellen Stellen hat lediglich den Charakter einer Erinnerung.

Neben ihrer Funktion als DIN-Norm stellt DIN 31000 (VDE 1000) zugleich auch eine VDE-Rahmen-Bestimmung dar. Deren Bedeutung und Funktion sind im grundsätzlichen in „VDE 0022/6.77 – Vorschriftenwerk des Verbandes Deutscher Elektrotechniker (VDE) e.V. – [VDE-Druckschrift]“ dargestellt. Für den vorliegenden Einzelfall sind Geltungsbereich, Zweck und Anwendung dieser VDE-Rahmen-Bestimmung in den [Abschnitten 1](#) und [2](#) klargestellt.

In der Sache stellt DIN 31000 (VDE 1000) in ihrer Funktion als VDE-Rahmen-Bestimmung alle für die Sicherheit von elektrischen Anlagen und elektrischen Betriebsmitteln wesentlichen Kriterien zusammen und trifft grundlegende Festlegungen darüber, was – unter Beachtung des sicherheitstechnischen Grundkonzeptes des gesamten VDE-Vorschriftenwerkes – bei der Errichtung und dem Betreiben von elektrischen Anlagen sowie beim Herstellen und Verwenden elektrischer Betriebsmittel zur Abwendung von Gefahren für Leben und Gesundheit des Benutzers und zum Schutz gegen Beschädigung von Sachen beachtet werden muss.

...

In Ergänzung und in Weiterführung dieser „Allgemeinen Leitsätze“ sollen fachübergreifende sicherheitstechnische Festlegungen für bestimmte Bereiche oder Schutzziele in Grundnormen (Mittelbau) zusammengefasst werden. Schließlich sollen Produktgruppen oder einzelne Produkte in Fachbereichsnormen oder Teilennormen erfasst werden.

Literaturhinweise

DIN 820-120, *Normungsarbeit – Teil 120: Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen (ISO/IEC Guide 51)*

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

DIN EN ISO 12100-2, *Sicherheit von Maschinen – Grundbegriffe, allgemeine Gestaltungsleitsätze – Teil 2: Technische Leitsätze*

DIN FB 144, *Sicherheit, Vorsorge und Meidung in der Technik*

gem. A1

	<p style="text-align: center;">Normungsarbeit Teil 120: Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen (ISO/IEC Guide 51:1999)</p>	<p style="text-align: center;">DIN 820-120</p>
--	---	--

- 1 Anwendungsbereich
 - 2 Normative Verweisungen
 - 3 Begriffe
 - 4 Verwendung der Benennungen „Sicherheits-“ und „sicher“
 - 5 Das Grundkonzept der Sicherheit
 - 6 Das Erreichen des vertretbaren Risikos
 - 7 Sicherheitsaspekte in Normen
 - 7.1 Arten von Sicherheitsnormen
 - 7.2 Analyse neuer Normungsvorschläge
 - 7.3 Wie ist die Anwendung der Norm durch diesen Personenkreis zu erwarten?
 - 7.4 Abfassung
- Literaturhinweise

Frühere Ausgaben

DIN V 820-120:1994-10

1 Anwendungsbereich

Diese Norm bietet Normenerstellern Leitlinien für die Aufnahme von Sicherheitsaspekten in Normen. Sie ist auf jeden Sicherheitsaspekt anwendbar, der sich auf Menschen, Güter, die Umwelt oder auf Kombinationen davon (z. B. Menschen allein, Menschen und Güter, Menschen, Güter und die Umwelt) bezieht.

Diese Norm setzt eine Konzeption um, die auf die Reduzierung des **Risikos** gerichtet ist, welches aus der Nutzung von Erzeugnissen, Verfahren oder Dienstleistungen entsteht. Es wird der vollständige Lebenszyklus eines Erzeugnisses, eines Verfahrens oder einer Dienstleistung einschließlich der **bestimmungsgemäßen Verwendung** und des **vernünftigerweise vorhersehbaren Missbrauchs** in Betracht gezogen.

ANMERKUNG 1 Qualität ist kein Synonym für **Sicherheit**, folglich sollten die Funktionen von Qualität und Sicherheit nicht miteinander vermischt werden. Es kann allerdings notwendig werden, Qualitätsanforderungen in Normen aufzunehmen, um sicherzustellen, dass die Sicherheitsanforderungen konsequent eingehalten werden.

...

3 Begriffe

Für die Anwendung dieser Norm gelten die folgenden Begriffe.

ANMERKUNG In anderen Publikationen dürfen die gleichen Benennungen mit leicht abgeänderten Definitionen angewendet werden, aber die Begriffe sind weitgehend gleich.

3.1

Sicherheit

Freiheit von unvertretbarem **Risiko**

ANMERKUNG Angepasst an ISO/IEC Guide 2:1996, Begriff 2.5.

3.2

Risiko

Kombination der Wahrscheinlichkeit eines **Schadenseintritts** und seines **Schadensausmaßes**

3.3

Schaden

physische Verletzung oder Schädigung der Gesundheit von Menschen oder Schädigung von Gütern oder der Umwelt

3.4

Schadensereignis

Vorkommnis, bei dem eine **Gefährdungssituation** zu einem **Schaden** führt

3.5

Gefährdung

potentielle **Schadensquelle**

ANMERKUNG Die Benennung **Gefährdung** kann spezifiziert werden, um den Ursprung oder die Art des erwarteten Schadens näher zu bezeichnen (z. B. Gefährdung durch elektrischen Schlag, Gefährdung durch Stoß, Gefährdung durch Schneiden, Gefährdung durch Gift, Gefährdung durch Feuer, Gefährdung durch Ertrinken).

3.6

Gefährdungssituation

Zustand, in dem Menschen, Güter oder die Umwelt einer oder mehreren **Gefährdungen** ausgesetzt sind

3.7

vertretbares Risiko

Risiko, das in einem bestimmten Zusammenhang nach den gültigen Wertvorstellungen der Gesellschaft akzeptiert wird

ANMERKUNG Siehe 5.3.

siehe Hinweis
zu 3.14

3.8

Schutzmaßnahme

Mittel zur Verminderung des **Risikos**

ANMERKUNG Schutzmaßnahmen umfassen Risikoverminderung durch sicherheitsbezogene Konstruktion, Schutzeinrichtungen, persönliche Schutzausrüstungen, Informationen über Errichtung und Anwendung sowie Schulungsmaßnahmen.

3.9

Restrisiko

Risiko, das nach der Anwendung von **Schutzmaßnahmen** verbleibt

3.10

Risikoanalyse

systematische Auswertung verfügbarer Informationen, um **Gefährdungen** zu identifizieren und **Risiken** einzuschätzen

3.11

Risikobewertung

auf der **Risikoanalyse** basierendes Verfahren, nach dem festgestellt wird, ob das **vertretbare Risiko** erreicht wurde

3.12

Risikobeurteilung

Gesamtheit des Verfahrens, das **Risikoanalyse** und **Risikobewertung** umfasst

3.13

bestimmungsgemäße Verwendung

Verwendung eines Erzeugnisses, eines Verfahrens oder einer Dienstleistung in Übereinstimmung mit den Informationen, die vom Lieferer bereitgestellt wurden

3.14

vernünftigerweise vorhersehbarer Missbrauch

Verwendung eines Erzeugnisses, eines Verfahrens oder einer Dienstleistung in einer Weise, die vom Lieferer nicht vorgesehen war, aber aus leicht vorhersehbaren menschlichen Verhaltensweisen resultieren kann

künftig im gesamten Dokument zu ersetzen durch:
„**vernünftigerweise vorhersehbare Fehlanwendung**“
laut Entwurf E DIN 820-120/A1:2008-01

4 Verwendung der Benennungen „Sicherheits-“ und „sicher“

Der Gebrauch der Wörter „**Sicherheits-**“ und „sicher“ als Bestimmungswort bzw. beschreibendes Adjektiv sollte vermieden werden, weil diese keine nutzbringende Zusatzinformationen enthalten und außerdem leicht als die Zusicherung garantierter Freiheit von **Risiken** aufgefasst werden können.

Es wird empfohlen, die Wörter „**Sicherheits-**“ und „sicher“. (als beschreibendes Adjektiv) wo immer möglich durch die Angabe des Zwecks zu ersetzen.

Beispiele sind:

- „Schutzhelm“ statt „Sicherheitshelm“;
- „Schutzimpedanzeinrichtung“ statt „Sicherheitsimpedanz“;
- „rutschhemmender Fußbodenbelag“ statt „Sicherheitsmaterial“.

5 Das Grundkonzept der Sicherheit

5.1 Sicherheit wird in der Normungsarbeit in vielen unterschiedlichen Formen, über weite Bereiche der Technik und im Zusammenhang mit den meisten Erzeugnissen, Verfahren und Dienstleistungen behandelt. Die wachsende Komplexität der auf den Markt kommenden Erzeugnisse, Verfahren und Dienstleistungen macht es erforderlich, dass der Berücksichtigung von **Sicherheitsaspekten** eine hohe Priorität eingeräumt wird.

Es kann keine absolute Sicherheit geben; ein gewisses **Risiko** wird zurückbleiben, in diesem Leitfaden als **Restrisiko** definiert. Deshalb kann ein Erzeugnis, ein Verfahren oder eine Dienstleistung nur relativ sicher sein.

5.2 Sicherheit wird erreicht durch Verminderung des **Risikos** auf ein vertretbares Niveau – definiert in diesem Leitfaden als **vertretbares Risiko**. Das **vertretbare Risiko** ist bestimmt durch die Suche nach einem optimalen Ausgleich zwischen dem Ideal der absoluten Sicherheit und den an ein Erzeugnis, ein Verfahren oder eine Dienstleistung zu stellenden Anforderungen und Faktoren wie Nutzen für den Anwender, Eignung für den vorgesehenen Verwendungszweck, Kostengünstigkeit und Konventionen in der betroffenen Gesellschaft. Daraus folgt die Notwendigkeit einer kontinuierlichen Überprüfung des vertretbaren Niveaus, im Besonderen wenn Entwicklungen in der Technik und im Wissensstand zu ökonomisch machbaren Verbesserungen führen können, damit bei der Anwendung des Erzeugnisses, des Verfahrens oder der Dienstleistung ein verträgliches minimales Risiko erreicht wird.

5.3 Vertretbares Risiko wird durch das iterative Verfahren von **Risikobeurteilung (Risikoanalyse und Risikobewertung)** und Risikominderung erreicht (siehe Bild 1).

siehe Hinweis
zu 3.14

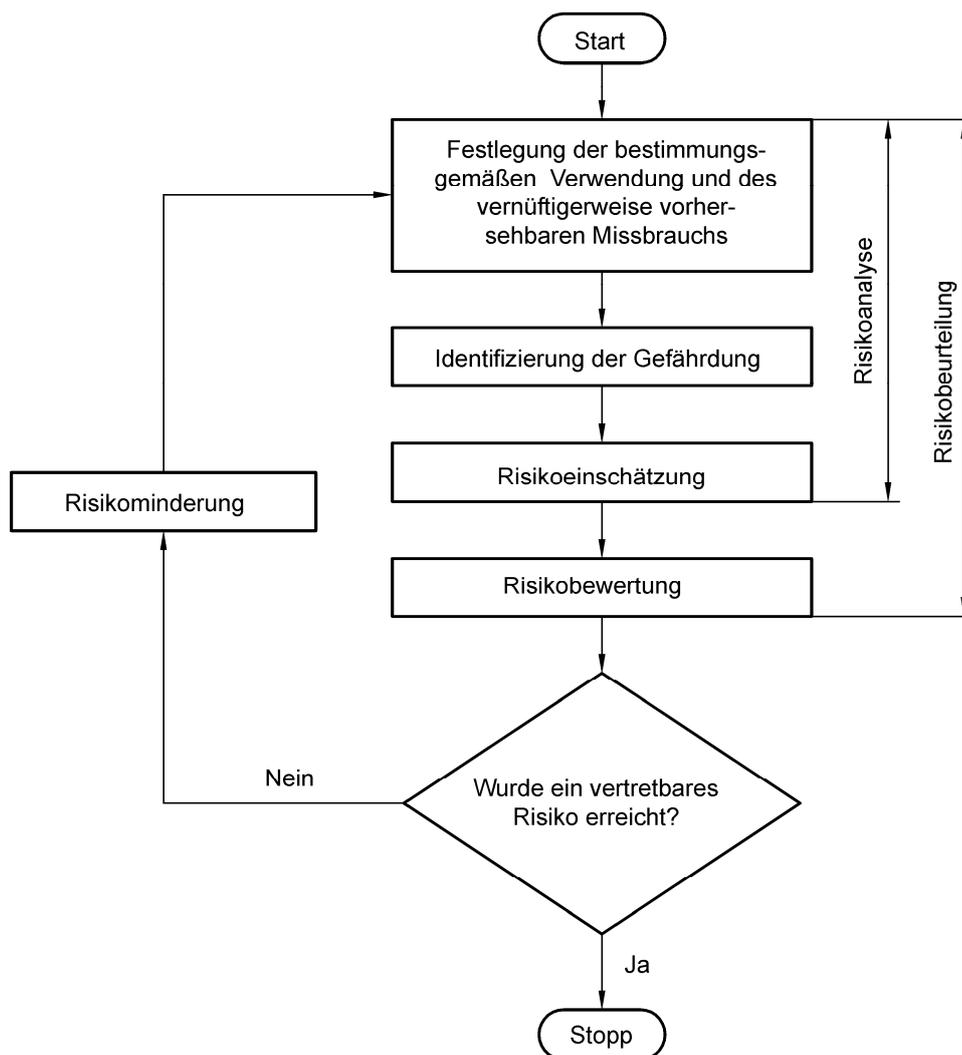


Bild 1 – Iteratives Verfahren von Risikobeurteilung und Risikominderung

6 Das Erreichen des vertretbaren Risikos

Das folgende Verfahren (siehe Bild 1) sollte zur Verminderung von **Risiken** auf ein vertretbares Niveau angewendet werden:

siehe Hinweis zu 3.14

- a) Die voraussichtliche(n) Anwendergruppe(n) für das Erzeugnis, das Verfahren oder die Dienstleistung (einschließlich derer mit besonderen Bedürfnissen) und alle Gruppen, die erfahrungsgemäß mit dem Erzeugnis, dem Verfahren oder der Dienstleistung in Kontakt kommen können (z. B. Anwendung/Kontakt durch Kleinkinder), sind zu identifizieren.
- b) Die **bestimmungsgemäße Verwendung** ist zu identifizieren, und der **vernünftigerweise vorhersehbare Missbrauch** des Erzeugnisses, des Verfahrens oder der Dienstleistung ist zu beurteilen.
- c) Jede **Gefährdung** (einschließlich aller **Gefährdungssituationen** und **Schadensereignisse**), die in allen Phasen und Zuständen der Anwendung des Erzeugnisses, des Verfahrens oder der Dienstleistung (einschließlich Installation, Wartung, Reparatur und Vernichtung/Entsorgung) auftreten kann, ist zu identifizieren.
- d) Das aus den identifizierten Gefährdungen erwachsende **Risiko** ist für jede Anwender- und Kontaktgruppe abzuschätzen und zu bewerten (siehe Bild 1).
- e) Es ist zu entscheiden, ob das **Risiko** vertretbar ist (z. B. durch Vergleich mit ähnlichen Erzeugnissen, Verfahren oder Dienstleistungen).
- f) Falls das **Risiko** nicht vertretbar ist, ist es zu vermindern, bis es vertretbar wird.

Bei der Verminderung des **Risikos** sollte die Reihenfolge der Prioritäten wie folgt eingehalten werden:

- 1) sicherheitsbezogene Konstruktion;
- 2) Schutzeinrichtungen;
- 3) Informationen für den Anwender.

Dieses Verfahren beruht auf der Annahme, dass sich der Anwender an der Risikominderung beteiligt, indem er der vom Entwickler/Lieferer bereitzustellenden Information nachkommt (siehe Bild 2).

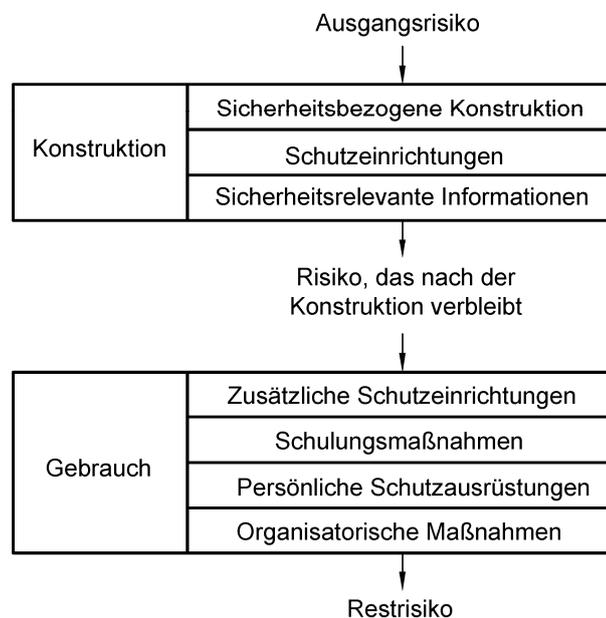


Bild 2 – Risikominderung

7 Sicherheitsaspekte in Normen

7.1 Arten von Sicherheitsnormen

...

- Sicherheitsgrundnormen, die grundsätzliche Begriffe, Prinzipien und Anforderungen zu allgemeinen Sicherheitsaspekten behandeln, welche auf eine breite Palette von Erzeugnissen, Verfahren und Dienstleistungen anwendbar sind;
- Sicherheitsgruppennormen, die Sicherheitsaspekte behandeln, welche auf mehrere bzw. eine Gruppe ähnlicher Erzeugnisse, Verfahren und Dienstleistungen anwendbar sind, die von mehr als einem Komitee bearbeitet werden, wobei diese Normen so weit wie möglich auf Sicherheitsgrundnormen verweisen;
- Produktsicherheitsnormen, die einen oder mehrere Sicherheitsaspekte behandeln, welche auf ein spezifisches Erzeugnis, Verfahren oder eine spezifische Dienstleistung oder eine Gruppe davon anwendbar sind, die von einem einzigen Komitee bearbeitet werden, wobei die Normen so weit wie möglich auf Sicherheitsgrundnormen und Sicherheitsgruppennormen verweisen;
- Produktnormen, die Sicherheitsaspekte enthalten, aber nicht ausschließlich Sicherheitsaspekte behandeln; diese Normen sollten auf Sicherheitsgrundnormen und Sicherheitsgruppennormen verweisen.

Für ein strukturiertes Vorgehen auf dem Gebiet der Elektrotechnik und Elektronik siehe IEC Guide 104.

...

DIN EN ISO 12100-1

DIN

**Sicherheit von Maschinen –
Grundbegriffe, allgemeine Gestaltungsleitsätze –
Teil 1: Grundsätzliche Terminologie, Methodologie (ISO 12100-1:2003)
Deutsche Fassung EN ISO 12100-1:2003**

- 1 Anwendungsbereich
- 2 Normative Verweisungen
- 3 Begriffe
- 4 Gefährdungen, die bei der Konstruktion von Maschinen zu berücksichtigen sind
 - 4.1 Allgemeines
 - 4.2 Mechanische Gefährdung
 - 4.3 Elektrische Gefährdung
 - 4.4 Thermische Gefährdung
 - 4.5 Gefährdung durch Lärm
 - 4.6 Gefährdungen durch Schwingungen
 - 4.7 Gefährdungen durch Strahlung
 - 4.8 Gefährdungen durch Materialien und Substanzen
 - 4.9 Gefährdungen durch Vernachlässigung ergonomischer Grundsätze bei der Konstruktion von Maschinen
 - 4.10 Gefährdungen durch Ausrutschen, Stolpern und Stürzen
 - 4.11 Gefährdungskombinationen
 - 4.12 Gefährdungen in Zusammenhang mit der Einsatzumgebung der Maschine
- 5 Strategie zur Risikominderung
 - 5.1 Allgemeine Vorkehrungen
 - 5.2 Festlegung der Grenzen der Maschine
 - 5.3 Identifizierung der Gefährdungen, Risikoeinschätzung und Risikobewertung
 - 5.4 Beseitigung von Gefährdungen oder Minderung des Risikos durch Schutzmaßnahmen
 - 5.5 Erreichen der Ziele zur Risikominderung

Anhang A (informativ) Schematische Darstellung einer Maschine

Frühere Ausgaben

DIN EN 292-1:1991-11

1 Anwendungsbereich

Diese Norm legt die grundsätzliche Terminologie und die Methodologie fest, die für das Erreichen der Sicherheit von Maschinen angewandt werden.

Die Festlegungen in dieser Norm sind für Konstrukteure vorgesehen.

Diese Norm behandelt keine Schäden an Haustieren, Eigentum und Umwelt.

...

4 Gefährdungen, die bei der Konstruktion von Maschinen zu berücksichtigen sind

4.1 Allgemeines

Zweck dieses Abschnitts ist es, grundlegende Gefährdungen zu beschreiben und damit den Konstrukteur bei der Identifizierung von relevanten und signifikanten Gefährdungen zu unterstützen. Dies sind Gefährdungen, die von der betrachteten Maschine ausgehen können, und solche, die mit der Umgebung in Verbindung stehen, in der die Maschine für den Einsatz vorgesehen ist (siehe auch 5.3).

ANMERKUNG Zur detaillierteren Übersicht über maschinenbezogene mögliche Gefährdungen und Gefährdungssituationen siehe ISO 14121:1999, Anhang A.

4.2 Mechanische Gefährdung

4.2.1 Mechanische Gefährdungen, die mit einer Maschine, Teilen oder Oberflächen von Maschinen, Werkzeugen, Werkstücken, Lasten oder herausgeschleuderten festen oder flüssigen Materialien in Verbindung stehen, können zu Folgendem führen:

- Quetschen;
- Scheren;
- Schneiden oder Abschneiden;
- Erfassen;
- Einziehen oder Fangen;
- Stoß;
- Durchstich oder Einstich;
- Reibung oder Abschürfung;
- Hochdruckinjektion (Herausspritzen von Flüssigkeiten unter hohem Druck).

4.2.2 Die mechanischen Gefährdungen, die von einer Maschine, von Maschinenteilen (einschließlich Haltevorrichtungen für Arbeitsmaterialien), Werkstücken oder Lasten ausgehen können, werden unter anderem von folgenden Faktoren bestimmt:

- Form (Schneidelemente, scharfe Kanten, spitze Teile, selbst wenn sich die Teile nicht bewegen);
- relative Lage, die Quetsch-, Scher-, Einziehbereiche hervorrufen kann, wenn sich die Teile bewegen;
- Standfestigkeit gegen Umkippen (unter Berücksichtigung der kinetischen Energie);
- Masse und Standfestigkeit (potentielle Energie von Teilen, die sich unter dem Einfluss der Schwerkraft bewegen können);
- Masse und Geschwindigkeit (kinetische Energie von Teilen bei kontrollierter und unkontrollierter Bewegung);
- Beschleunigung/Abbremsen;
- unzulängliche mechanische Festigkeit, die zu gefährlichen Brüchen oder zu gefährlichem Bersten führen kann;
- potentielle Energie von elastischen Elementen (Federn), von Flüssigkeiten oder Gasen unter Druck oder im Vakuum;
- Einsatzumgebung.

4.3 Elektrische Gefährdung

Diese Gefährdung kann zu Verletzungen oder Tod durch elektrischen Schlag oder Verbrennungen führen, verursacht durch:

- Berührung durch Personen von
- spannungsführenden Teilen, d. h. elektrischen Leitern oder Teilen, die bestimmungsgemäß Spannung führen (direkte Berührung);
- Teilen, die im Fehlerzustand, besonders bei Isolationsfehler, Spannung führen (indirekte Berührung);
- Annäherung von Personen an spannungsführende Teile, besonders im Bereich von Hochspannung;
- Isolierung, die für vernünftigerweise vorhersehbare Anwendungsbedingungen nicht geeignet ist;
- elektrostatische Vorgänge, wie z. B. Berührung von aufgeladenen Teilen durch Personen;
- Wärmestrahlung;
- Vorgänge wie Wegspritzen von geschmolzenen Teilen und chemische Reaktionen bei Kurzschlüssen oder Überlastungen.

Sie kann auch dazu führen, dass Personen infolge eines durch elektrischen Schlag hervorgerufenen Überraschungsmoments stürzen (oder dass Personen Gegenstände fallen lassen).

4.4 Thermische Gefährdung

Thermische Gefährdung kann folgende Auswirkungen haben:

- Verbrennungen und Verbrühungen durch Berührung von Gegenständen oder Materialien mit extremer Temperatur, Flammen oder Explosionen und durch Strahlung von Wärmequellen;
- Gesundheitsschädigungen durch heiße oder kalte Arbeitsumgebung.

4.5 Gefährdung durch Lärm

Lärm kann führen zu:

- bleibendem Gehörverlust;
- Tinnitus (Ohrensausen);
- Müdigkeit, Stress;
- weiteren Auswirkungen wie Gleichgewichtsstörungen, Bewusstseinsverlust;
- Beeinträchtigung der Sprachkommunikation oder der Wahrnehmung akustischer Signale.

4.6 Gefährdungen durch Schwingungen

Schwingungen können auf den gesamten Körper (bei Verwendung beweglicher Ausrüstungen) und besonders auf Hände und Arme (bei Einsatz handgehaltener und handgeführter Maschinen) übertragen werden.

Sehr starke Schwingungen (oder weniger starke Schwingungen über einen längeren Zeitraum) können ernste Erkrankungen (Erkrankungen der Lendengegend, Wirbelsäulenverletzungen), starkes Unbehagen durch Ganzkörperschwingungen und Gefäßerkrankungen verursachen, z. B. Weissfingerkrankheit, neurologische Erkrankungen, Knochengelenkschäden durch Hand-Arm-Schwingungen.

4.7 Gefährdungen durch Strahlung

Diese Gefährdungen, die sofortige Auswirkungen (z. B. Verbrennungen) oder Langzeitauswirkungen (z. B. genetische Veränderungen) haben können, werden von unterschiedlichen Quellen erzeugt und können durch nichtionisierende oder ionisierende Strahlung verursacht werden:

- Elektromagnetische Felder (z. B. Felder im Niederfrequenz-, Hochfrequenz- und Mikrowellenbereich);
- Infrarotes Licht, sichtbares Licht und UV-Licht;
- Laserlicht;
- Röntgen- und γ -Strahlen;
- α -, β -Strahlen, Elektronen- oder Ionenstrahlen, Neutronenstrahlen.

4.8 Gefährdungen durch Materialien und Substanzen

Materialien und Substanzen, die von Maschinen verarbeitet, verwendet, produziert oder abgegeben werden, und Materialien, die zum Bau von Maschinen verwandt werden, können mehrere unterschiedliche Gefährdungen hervorrufen:

- Gefährdungen über Nahrungsaufnahme, Berührung mit Haut, Augen und Schleimhäuten oder Einatmen von Flüssigkeiten, Gasen, Nebeln, Dämpfen, Fasern, Stäuben oder Aerosolen, die z. B. schädliche, giftige, korrodierende, teratogene (fruchtschädigende), krebserzeugende, Erbgut verändernde, Reiz auslösende oder sensibilisierende Wirkungen haben;
- Gefährdungen durch Feuer und Explosion;
- biologische (z. B. Schimmel) und mikrobiologische (virale oder bakterielle) Gefährdungen.

4.9 Gefährdungen durch Vernachlässigung ergonomischer Grundsätze bei der Konstruktion von Maschinen

Mangelnde Anpassung der Maschinen an die Eigenschaften und Fähigkeiten des Menschen können sich wie folgt darstellen:

- physiologische Wirkungen (z. B. Muskel-Skelett-Störungen), die z. B. auf ungesunde Körperhaltung, übermäßige oder wiederholte körperliche Anstrengungen zurückzuführen sind;
- psychophysiologische Wirkungen, hervorgerufen z. B. durch psychischer Über- oder Unterbelastung, oder Stress, verursacht durch Betrieb, Überwachung oder Instandhaltung einer Maschine innerhalb der Grenzen ihrer bestimmungsgemäßen Verwendung;
- menschliches Fehlverhalten.

4.10 Gefährdungen durch Ausrutschen, Stolpern und Stürzen

Vernachlässigung der Oberflächenbeschaffenheit von Fußböden und Zugängen kann zu Verletzungen durch Rutschen, Stolpern und Stürzen führen.

4.11 Gefährdungskombinationen

Einige bei individuellem Auftreten als gering eingeschätzte Gefährdungen können bei gemeinsamem Auftreten zu einer signifikanten Gefährdung werden.

4.12 Gefährdungen in Zusammenhang mit der Einsatzumgebung der Maschine

Gefährdungen, die durch den Betrieb unter bestimmten Umgebungsbedingungen auftreten können (z. B. Temperatur, Wind, Schnee, Blitzschlag), müssen berücksichtigt werden.

5 Strategie zur Risikominderung

5.1 Allgemeine Vorkehrungen

5.1.1 Es wird davon ausgegangen, dass eine an einer Maschine vorhandene Gefährdung früher oder später zu einem Schaden führt, falls keine Schutzmaßnahme(n) durchgeführt wird (werden).

5.1.2 Schutzmaßnahmen sind eine Kombination der vom Konstrukteur und der vom Benutzer durchgeführten Maßnahmen (siehe Bild 1^{E8}). Maßnahmen, die bereits in der Konstruktionsphase getroffen werden können, sind den vom Benutzer durchgeführten Maßnahmen vorzuziehen und im Allgemeinen wirksamer als diese.

5.1.3 Unter Berücksichtigung der Erfahrungen von Benutzern ähnlicher Maschinen und des Informationsaustausches mit den potentiellen Benutzern (wann immer dies möglich ist) muss der Konstrukteur in der unten angegebenen Reihenfolge vorgehen (siehe Bild 2^{E9}):

- Festlegen der Grenzen und der bestimmungsgemäßen Verwendung der Maschine (siehe 5.2);
- Identifizieren von Gefährdungen und zugehörigen Gefährdungssituationen (siehe Abschnitt 4 und 5.3);
- Einschätzen des Risikos für jede identifizierte Gefährdung und Gefährdungssituation (siehe 5.3);
- Bewerten des Risikos und Treffen von Entscheidungen über die Notwendigkeit zur Risikominderung (siehe 5.3);
- Beseitigen der Gefährdung oder Vermindern des mit der Gefährdung verbundenen Risikos durch Schutzmaßnahmen (siehe 5.4 und 5.5).

Die ersten vier oben genannten Punkte beziehen sich auf die Risikobeurteilung, zu der detaillierte Informationen in ISO 14121 zu finden sind.

5.1.4 Das zu erreichende Ziel besteht in der größtmöglichen Risikominderung unter Berücksichtigung der vier unten angegebenen Faktoren. Die vorstehend festgelegte Strategie ist im Flussdiagramm im Bild 2 dargestellt. Der Prozess ist iterativ, und es können bei bestmöglicher Anwendung der zur Verfügung stehenden Technologien mehrere aufeinander folgende Wiederholungen erforderlich sein, um das Risiko zu mindern.

Bei der Durchführung dieses Prozesses ist es erforderlich, die folgende Rangfolge zu berücksichtigen:

- Sicherheit der Maschine in sämtlichen Phasen ihrer Lebensdauer;
- Fähigkeit der Maschine, ihre Funktion auszuführen;
- Benutzerfreundlichkeit der Maschine;
- Herstellungs-, Betriebs- und Demontagekosten der Maschine.

ANMERKUNG 1 Die ideale Anwendung dieser Grundsätze erfordert Kenntnisse über den Einsatz der Maschine, des Unfallgeschehens und der Bilanz der gesundheitlichen Auswirkungen, der verfügbaren Verfahren zur Risikominderung und des gesetzlichen Regelwerks, dem die Maschine unterliegt.

ANMERKUNG 2 Eine zu einem bestimmten Zeitpunkt annehmbare Maschinenkonstruktion ist möglicherweise nicht mehr vertretbar, wenn die technologische Entwicklung die Konstruktion einer gleichwertigen Maschine mit geringerem Risiko erlaubt.

5.1.5 Für den dauerhaft sicheren Betrieb einer Maschine ist es wichtig, dass die Schutzmaßnahmen eine einfache Verwendung der Maschine zulassen und die bestimmungsgemäße Verwendung nicht beeinträchtigen. Andernfalls könnte das zum Umgehen von Schutzmaßnahmen führen, um die maximale Nutzbarkeit der Maschine zu erzielen.

5.1.6 Wenn für eine Emission genormte (oder weitere geeignete) Messverfahren vorliegen, dann sollten sie mit den bestehenden Maschinen oder Prototypen für die Bestimmung der Emissionswerte und vergleichenden Emissionsdaten angewendet werden. Dies versetzt den Konstrukteur in die Lage,

- das mit den Emissionen verbundene Risiko einzuschätzen;
- die Wirksamkeit der in der Konstruktionsphase ausgeführten Schutzmaßnahmen zu bewerten;

^{E8}) Siehe Seite 39 dieses Sonderdrucks.

^{E9}) Siehe Seite 40 dieses Sonderdrucks.

- den potentiellen Käufern in den technischen Unterlagen quantitative Angaben zu Emissionen zu geben;
- dem Benutzer in der Benutzerinformation quantitative Angaben zu Emissionen zu geben.

Andere Gefährdungen als Emissionen, die durch messbare Parameter beschrieben sind, können in vergleichbarer Weise behandelt werden.

5.2 Festlegung der Grenzen der Maschine

Die Konstruktion der Maschine beginnt mit der Festlegung ihrer Grenzen (siehe auch [Abschnitt 5](#) von ISO 14121:1999):

- Verwendungsgrenzen:
- bestimmungsgemäße Verwendung der Maschine einschließlich der verschiedenen Betriebsarten, Verwendungsphasen und unterschiedlichen Eingriffsmöglichkeiten für die Bedienpersonen;
- vernünftigerweise vorhersehbare Fehlanwendung der Maschine;
- räumliche Grenzen (z. B. Bewegungsraum, Platzbedarf für die Installation und Instandhaltung der Maschine, Schnittstellen „Mensch/Maschine“ und „Maschine/Energieversorgung“);
- zeitliche Grenzen: vorhersehbare „Lebensdauer“ der Maschine und/oder einiger ihrer Teile (z. B. Werkzeuge, Verschleißteile, elektrische Bauteile) unter Berücksichtigung ihrer bestimmungsgemäßen Verwendung.

5.3 Identifizierung der Gefährdungen, Risikoeinschätzung und Risikobewertung

Hat der Konstrukteur die verschiedenen Gefährdungen identifiziert, die von der Maschine ausgehen können (dauerhaft vorhandene Gefährdungen und solche, die unerwartet auftreten können: siehe 3.6 und [Abschnitt 4](#)), muss er – soweit wie möglich auf der Grundlage der quantifizierbaren Faktoren – das Risiko für jede Gefährdung abschätzen. Er muss dann entscheiden, ob im Ergebnis der Risikobewertung eine Risikominderung (siehe [5.4](#)) erforderlich ist. Hierzu muss er die verschiedenen Betriebsarten und unterschiedlichen Eingriffsmöglichkeiten berücksichtigen, insbesondere:

- a) Eingreifen durch Personen während der gesamten Lebensdauer der Maschine, wie unten beschrieben:
 - 1) Herstellung;
 - 2) Transport, Zusammenbau und Installation;
 - 3) Inbetriebnahme;
 - 4) Verwendung:
 - Einrichten, Teachen/Programmieren oder Umrüsten;
 - Betrieb;
 - Reinigung;
 - Fehlersuche;
 - Instandhaltung;
 - 5) Außerbetriebnahme, Demontage und, sofern die Sicherheit betroffen ist, Entsorgung;
- b) mögliche Betriebszustände der Maschine:
 - 1) Die Maschine führt die vorgesehene Funktion aus (Normalbetrieb);
 - 2) die Maschine führt aus verschiedenen Gründen ihre vorgesehene Funktion nicht aus (d. h., sie versagt), z. B.:
 - Veränderung einer Eigenschaft oder einer Abmessung des zu verarbeitenden Materials oder des Werkstückes;
 - Ausfall eines (oder mehrerer) ihrer Bauteile oder Versorgungseinrichtungen;
 - Störungen von außen (z. B. Stöße, Schwingungen, elektromagnetische Störungen);
 - Konstruktionsfehler oder -mängel (z. B. Software-Fehler);
 - Störung der Energieversorgung;
 - Umgebungsbedingungen (z. B. beschädigte Böden);

- c) unbeabsichtigtes Verhalten der Bedienerperson oder vernünftigerweise vorhersehbare Fehlanwendung der Maschine, z. B.:
- Verlust der Kontrolle der Bedienerperson über die Maschine (besonders bei handgehaltenen oder beweglichen Maschinen);
 - reflexartiges Verhalten einer Person im Falle einer Fehlfunktion, eines Störfalls oder Ausfalls während des Gebrauchs der Maschine;
 - Verhalten durch Konzentrationsmangel oder Unachtsamkeit;
 - Verhalten, das bei der Bewältigung einer Aufgabe auf die Wahl des „Weges des geringsten Widerstandes“ zurückzuführen ist;
 - Verhalten unter dem Druck, die Maschine unter allen Umständen in Betrieb zu halten;
 - Verhalten von bestimmten Personen (z. B. Kinder, Behinderte).

Risikoeinschätzung und -bewertung sind im Anschluss an jeden einzelnen der drei unter 5.4 festgelegten und im [Bild 2](#) dargestellten Stufen zur Risikominderung vorzunehmen.

Bei der Durchführung einer Risikobeurteilung muss für jede festgestellte Gefährdung das Risiko aus dem wahrscheinlichsten Ausmaß des durch diese Gefährdung verursachten Schadens berücksichtigt werden. Es muss jedoch auch das größte vorhersehbare Ausmaß des Schadens berücksichtigt werden, selbst wenn die Eintrittswahrscheinlichkeit eines Schadens solchen Ausmaßes nicht sehr groß ist.

5.4 Beseitigung von Gefährdungen oder Minderung des Risikos durch Schutzmaßnahmen

Dieses Ziel kann durch Beseitigung der Gefährdungen oder durch getrennte oder gleichzeitige Minderung jedes der beiden Elemente erreicht werden, die das Risiko bestimmen:

- a) Ausmaß des Schadens aus der betrachteten Gefährdung;
- b) Eintrittswahrscheinlichkeit dieses Schadens.

Alle Schutzmaßnahmen, die zum Erreichen dieses Ziels angewendet werden, sind in der folgenden, als „3-Stufen-Methode“ bezeichneten Reihenfolge zu ergreifen (siehe auch [Bilder 1](#) und [2](#)):

- inhärent sichere Konstruktion (siehe ISO 12100-2:2003, Abschnitt 4);

ANMERKUNG Diese Phase ist die einzige, in der Gefährdungen beseitigt werden können. Dadurch erübrigt sich die Notwendigkeit für zusätzliche Schutzmaßnahmen wie technische Schutzmaßnahmen oder ergänzende Schutzmaßnahmen.

- technische Schutzmaßnahmen und eventuell ergänzende Schutzmaßnahmen (siehe ISO 12100-2:2003, Abschnitt 5);
- Benutzerinformation hinsichtlich des Restrisikos (siehe ISO 12100-2:2003, Abschnitt 6).

Die Benutzerinformation darf kein Ersatz für die korrekte Anwendung der inhärent sicheren Konstruktion, der technischen Schutzmaßnahmen oder der ergänzenden Schutzmaßnahmen sein.

Angemessene Schutzmaßnahmen für jede Betriebsart und jedes Eingriffsverfahren (siehe [5.3](#)) hindern Bedienerpersonen daran, sich verleiten zu lassen, gefährdende Eingriffsmethoden wegen technischer Schwierigkeiten anzuwenden.

5.5 Erreichen der Ziele zur Risikominderung

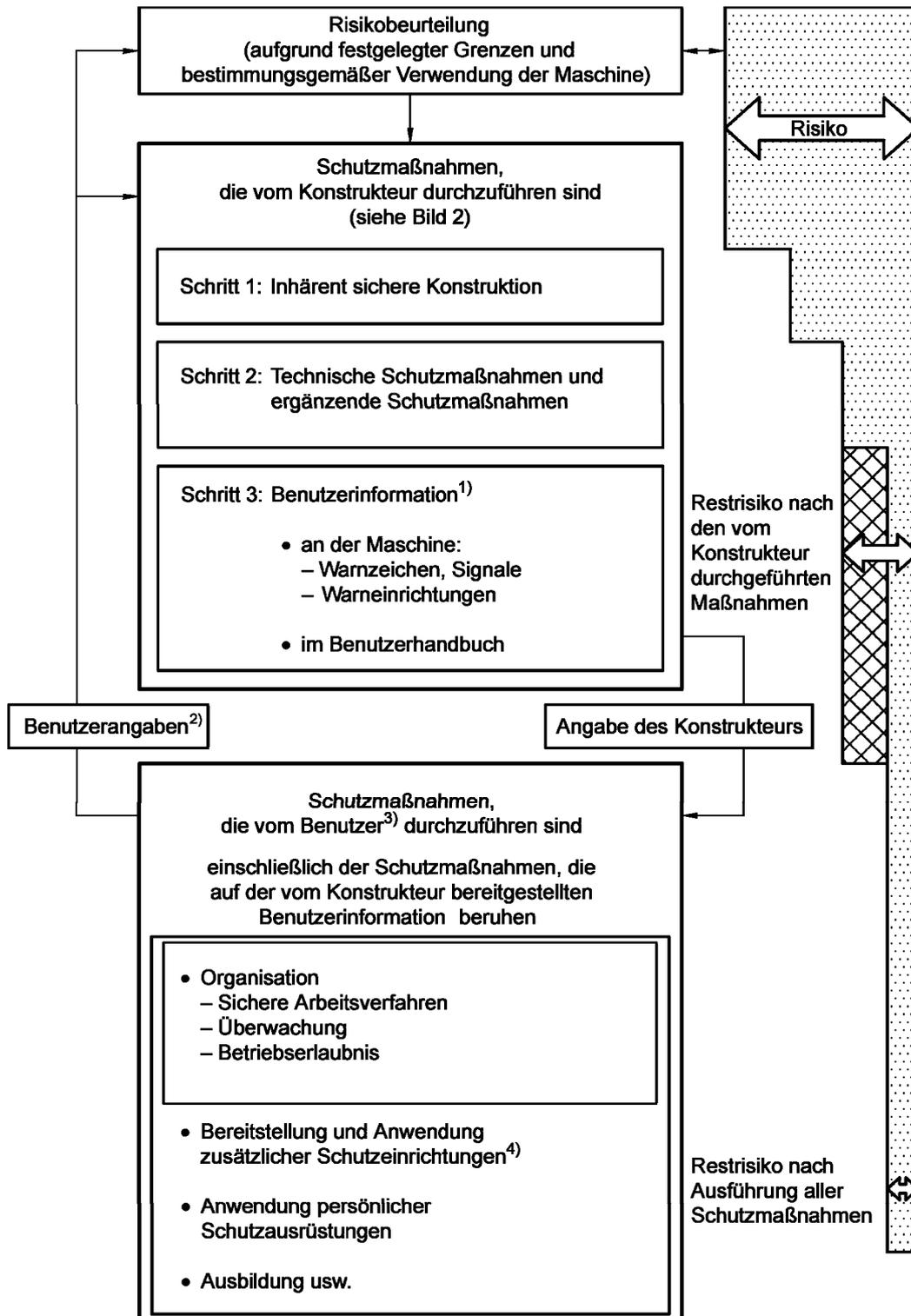
Der iterative Prozess der Risikominderung nach 5.4 und [Bild 2](#) kann nach Erreichen der Ziele zur hinreichenden Risikominderung und soweit anwendbar eines positiven Ergebnisses des Risikovergleichs abgeschlossen werden (siehe ISO 14121, 8.3).

Die Ziele zur hinreichenden Risikominderung können als erreicht angesehen werden, wenn eine positive Antwort zu jeder der folgenden Fragen gegeben werden kann:

- Wurden alle Betriebsbedingungen und alle Eingriffsverfahren berücksichtigt?
- Wurde das unter 5.4 angegebene Verfahren angewendet?

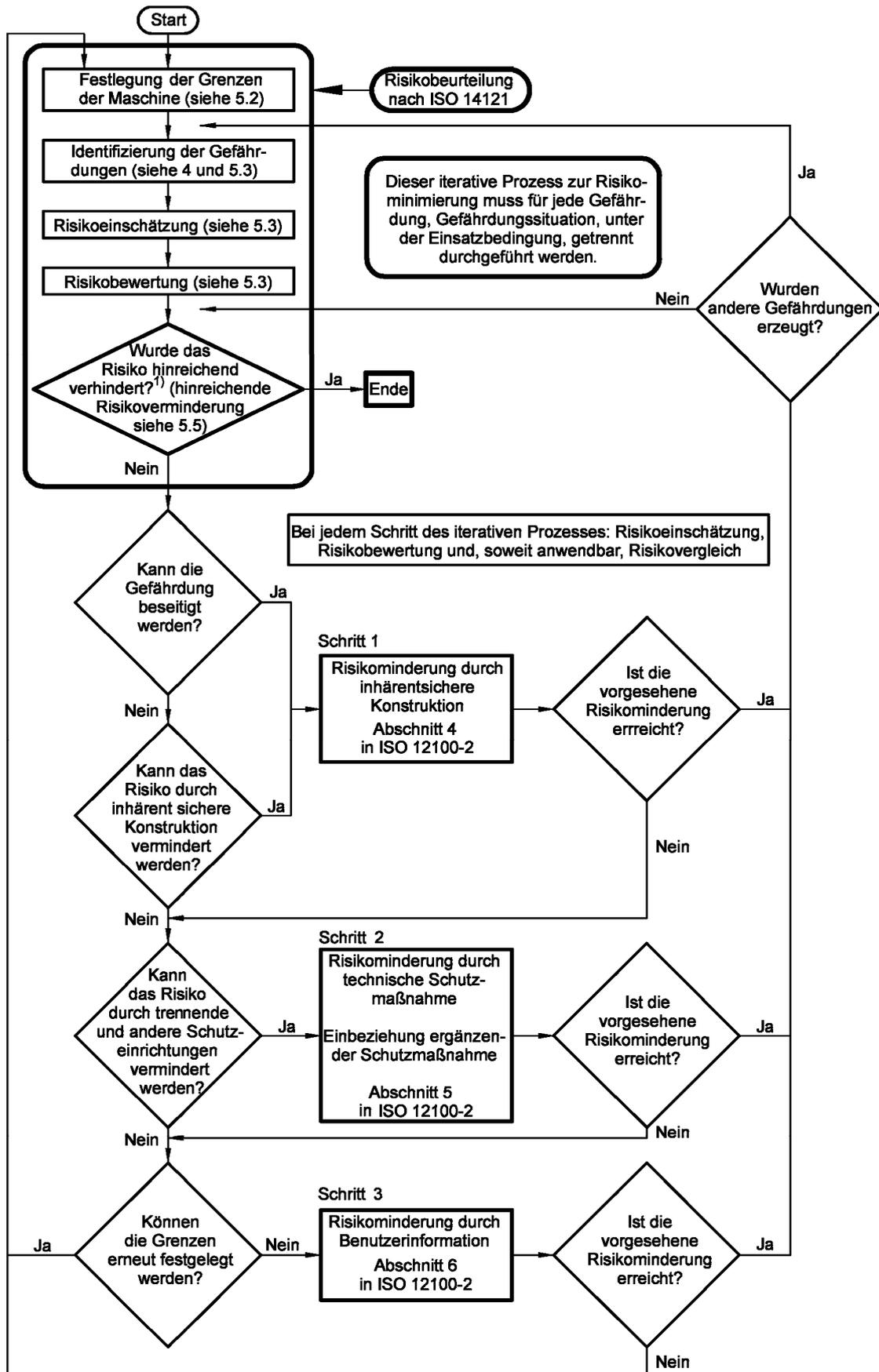
- Wurden die Gefährdungen beseitigt oder die Risiken der Gefährdungen soweit vermindert, wie dies praktisch umsetzbar ist?
- Ist sichergestellt, dass die durchgeführten Maßnahmen nicht neue Gefährdungen schaffen?
- Sind die Benutzer hinsichtlich der Restrisiken ausreichend informiert und gewarnt?
- Ist sichergestellt, dass die Arbeitsbedingungen der Bedienpersonen durch die ergriffenen Schutzmaßnahmen nicht konterkariert worden sind?
- Sind die durchgeführten Schutzmaßnahmen miteinander vereinbar?
- Wurden die Folgen ausreichend berücksichtigt, die durch den Gebrauch einer für gewerbliche/industrielle Zwecke konstruierten Maschine beim Gebrauch im nicht gewerblichen/nicht industriellen Bereich entstehen können?
- Ist sichergestellt, dass die durchgeführten Maßnahmen die Fähigkeit der Maschine zur Erfüllung ihrer Funktion nicht übermäßig beeinträchtigen?

...



- 1 Die Bereitstellung einer angemessenen Benutzerinformation ist Teil des Beitrages des Konstrukteurs zur Risikominderung; die betreffenden Schutzmaßnahmen werden jedoch erst mit ihrer Umsetzung durch den Benutzer wirksam.
- 2 Benutzerangaben sind Informationen, die dem Konstrukteur entweder von den Benutzern hinsichtlich der bestimmungsgemäßen Verwendung der Maschine im Allgemeinen oder von einem bestimmten Benutzer gegeben werden.
- 3 Bei den verschiedenen vom Benutzer durchzuführenden Schutzmaßnahmen besteht keine bestimmte Hierarchie. Diese Schutzmaßnahmen liegen außerhalb des Anwendungsbereiches dieser Norm.
- 4 Schutzmaßnahmen, die für besondere, im Rahmen der bestimmungsgemäßen Verwendung der Maschine nicht vorgesehene Prozesse oder für besondere, durch den Konstrukteur nicht beeinflussbare Installationsbedingungen erforderlich sind.

Bild 1 – Prozess zur Risikominderung aus Sicht des Konstrukteurs



¹⁾ Beim erstmaligen Stellen der Frage wird sie mit dem Ergebnis der Ausgangsrisikobewertung beantwortet.

Bild 2 – Schematische Darstellung des 3-stufigen iterativen Prozesses zur Risikominderung

	Quantifizierte Risikominderung	
	Erläuterung	

Das Bild „Der Risikoansatz zur Beurteilung der technischen Sicherheit“ in der Einleitung auf Seite 5 unterscheidet zwischen der mindestnotwendigen und dem Beispiel einer angemessenen Risikominderung, mit denen sich Sicherheit bei noch vertretbarem Risiko erreichen lässt. Das grundsätzliche Vorgehen zur Risikominderung beschreiben auf den Seiten 28 und 29 die aus DIN 820-120 entnommenen Abschnitte 5 und 6. Die dort unter 6e) angeführte Entscheidung, ob das Risiko eines technischen Produktes vertretbar ist oder nicht, wird im Prinzip durch einen qualitativen Risikovergleich mit einem sicheren, vergleichbarem und möglichst ähnlichem Produkt getroffen. Im einfachsten Fall bilden Sicherheitsnormen das Vergleichsobjekt.

Zur Gefahrenabwehr und Risikominderung werden Schutzmaßnahmen aller Art angewandt. Dies lässt auf Seite 39 das Bild 1 aus DIN ISO 12100-1 am Beispiel der Sicherheit von Maschinen erkennen. Den Konstrukteur interessiert vor allem die im Streifendiagramm am rechten Bildrand angedeutete Risikominderung, die er mit den von ihm durchzuführenden und zu verantwortenden Schutzmaßnahmen erreichen will. Am Ende des hierzu nach den Angaben auf den Seiten 35 bis 40 iterativ ablaufenden Prozesses muss er nach Bild 2 klar entscheiden, ob die jeweils beabsichtigte Risikominderung erreicht wurde oder nicht. Diese Entscheidung von mitunter großer Tragweite muss eindeutig entweder mit „Ja“ oder mit „Nein“ getroffen werden. Ein ausweichendes „Vielleicht“ ist ausgeschlossen.

Schutzmaßnahmen können jedoch aus höchst unterschiedlichen Gründen ausfallen oder versagen. Für einen vorgegebenen Schadensumfang bestimmt in solchem Fall die Ausfallwahrscheinlichkeit der Schutzmaßnahmen das noch verbleibende Risiko. Überlegungen über dessen Größe werden durch quantifizierte Angaben zur Ausfallwahrscheinlichkeit wesentlich erleichtert. Für einfache Schutzeinrichtungen, wo die Ausfallarten der Bauteile bekannt und das Verhalten der kompletten technischen Einrichtung unter Fehlerbedingungen völlig geklärt sind, liegen solche Angaben im Allgemeinen vor. Als Beispiel nennt DIN EN 61508-4 (VDE 0803-4), 3.4.4 geläufige Schaltungen, die mit Grenztastern und Schützen einen Elektromotor spannungsfrei schalten. Ähnliches gilt für serienmäßige Schutzrelais, die der Produktbeobachtungspflicht des Produzenten unterliegen.

Die vorstehend für Schutzsysteme angestellten Überlegungen gelten sinngemäß auch für Steuerungssysteme: Beide dienen letzten Endes der Gefahrenvermeidung und Risikobeherrschung. Die Normenreihe DIN EN 61508 (VDE 0803) fasst daher die Schutz- und Steuerungssysteme, deren Funktion die Sicherheit eines technischen Produktes positiv beeinflussen, als „sicherheitsbezogene Systeme“ zusammen. Sie führen in Gefährdungssituationen so genannte „Sicherheitsfunktionen“ mit dem Ziel durch, die Sicherheit eines technischen Produkts oder Systems wieder zu erreichen oder zu erhalten.

DIN EN 61508 (VDE 0803) spricht von „funktionaler Sicherheit“, wenn Freiheit von unvermeidbaren Risiken vorliegt, welche speziell von der korrekten Funktion dieser sicherheitsbezogenen Systeme abhängen. Die funktionale Sicherheit ist demnach ein Beitrag zur Sicherheit der technischen Erzeugnisse, Verfahren und Dienstleistungen nach DIN 820-120, 3.1. Die für DIN EN 61508 (VDE 0803) verbindlichen speziellen Begriffserklärungen sind in deren Teil 4 zusammengestellt.

Es trifft sich gut, dass die Wahrscheinlichkeiten zufälliger Ausfälle sich nicht nur für einfache, sondern auch für komplexe Systeme ermitteln lassen: Wenn nämlich die Ausfälle der typischen Bauteile eines solchen Systems statistisch erfasst und bekannt sind, lässt sich daraus und mit Hilfe von Rechenregeln der Stochastik die Ausfallwahrscheinlichkeit des Gesamtsystems bestimmen, wie die Beispiele in DIN EN 61508-6 (VDE 0803-6) zeigen. So kann im Einzelfall der rechnerische Nachweis erbracht werden, dass der in den Tabellen 2 und 3 von DIN EN 61508-1 (VDE 0803-1) niedergelegte Ausfallgrenzwert einer Sicherheitsfunktion nicht überschritten wird.

DIN EN 61508-1 (VDE 0803-1) nutzt nun diese Möglichkeit: Die Norm setzt für Sicherheitsfunktionen, die von Einrichtungen zur Risikoreduktion ausgeführt werden, klassifizierte numerische Ausfallgrenzwerte fest. Hierzu stellt DIN EN 61508-1 (VDE 0803-1) vier gestufte Klassen zur Entwicklung von sicherheitsbezogenen Systemen zur Auswahl. Sie sind sowohl für den Ersteller anwendungsspezifischer Normen bestimmt, als auch für den Konstrukteur, dem keine solchen Normen vorliegen. Die Werte der Tabelle 2 gelten für das gelegentliche

Eingreifen zum Beispiel einer Schutzeinrichtung, die Werte der Tabelle 3 für das fortgesetzte Einwirken etwa einer Steuerungseinrichtung. Die Klassen haben den Charakter von Schutzpegeln, werden aber als „safety integrity level – Sicherheits-Integritätslevel“ bezeichnet und mit „SIL 1“ bis „SIL 4“ klassifiziert.

**Ausfallgrenzwerte für eine Sicherheitsfunktion,
die in der Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung betrieben wird**
[Tabelle 3 aus DIN EN 61508-1 (VDE 0803-1):2002-11]

Sicherheits- Integritätslevel	Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung (Wahrscheinlichkeit eines gefährbringenden Ausfalls pro Stunde)
4	$\geq 10^{-9}$ bis $< 10^{-8}$
3	$\geq 10^{-8}$ bis $< 10^{-7}$
2	$\geq 10^{-7}$ bis $< 10^{-6}$
1	$\geq 10^{-6}$ bis $< 10^{-5}$
ANMERKUNG Siehe nachfolgende Anmerkungen 3 bis 9 für Einzelheiten zur Interpretation dieser Tabelle.	

ANMERKUNG 3 Zur Definition der Ausdrücke "Betriebsart mit niedriger Anforderungsrate" und "Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung" siehe 3.5.12 von IEC 61508-4.

ANMERKUNG 4 Der Parameter "Wahrscheinlichkeit eines gefährbringenden Ausfalls pro Stunde" für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung in Tabelle 3 wird manchmal als Häufigkeit von gefährbringenden Ausfällen oder Rate gefährbringender Ausfälle, in der Einheit gefährbringende Ausfälle pro Stunde, verwendet.

ANMERKUNG 5 Für ein sicherheitsbezogenes E/E/PE-System, das in der Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung betrieben wird und das für eine definierte Einsatzzeit, während der keine Reparatur ausgeführt werden kann, betrieben wird, kann der erforderliche Sicherheits-Integritätslevel für eine Sicherheitsfunktion wie folgt hergeleitet werden: Die erforderliche Wahrscheinlichkeit eines Ausfalls der Sicherheitsfunktion während der Einsatzzeit wird bestimmt und durch die Einsatzzeit geteilt. Dies ergibt die erforderliche Wahrscheinlichkeit eines Ausfalls pro Stunde. Danach wird Tabelle 3 verwendet, um den erforderlichen Sicherheits-Integritätslevel herzuleiten.

ANMERKUNG 6 Diese Norm legt eine untere Grenze für die Ausfallgrenzwerte fest, die für Ausfälle mit gefährbringendem Verhalten angegeben werden können. Diese sind als untere Grenze des Sicherheits-Integritätslevels 4 festgelegt (d. h. eine mittlere Wahrscheinlichkeit eines Ausfalls der entworfenen Funktion bei Anforderung von 10^{-5} oder eine Wahrscheinlichkeit eines gefährbringenden Ausfalls von 10^{-9} pro Stunde). Es kann möglich sein, dass sicherheitsbezogene Systeme geringer Komplexität mit niedrigeren Werten für die Ausfallgrenzwerte entworfen werden. Es wird jedoch angenommen, dass die Zahlen in den Tabellen die Grenze darstellen, die mit relativ komplexen Systemen (zum Beispiel sicherheitsbezogene Systeme in programmierbarer Elektronik) in der heutigen Zeit erreicht werden kann.

ANMERKUNG 7 Die Ausfallgrenzwerte, die angegeben werden können, wenn zwei oder mehr sicherheitsbezogene E/E/PE-Systeme verwendet werden, können unter der Voraussetzung, dass ausreichende Unabhängigkeitsgrade erreicht werden, besser als die der Tabellen 2 und 3 sein.

ANMERKUNG 8 Es ist wichtig anzumerken, dass die Ausfallwerte für die Sicherheits-Integritätslevel 1, 2, 3 und 4 Ausfallgrenzwerte sind. Es ist allgemein anerkannt, dass es nur hinsichtlich der Sicherheitsintegrität der Hardware (siehe 3.5.5 von IEC 61508-4) möglich ist, quantitativ zu arbeiten und Methoden zur Voraussage der Zuverlässigkeit bei der Beurteilung, ob die Ausfallgrenzwerte erreicht worden sind, anzuwenden. Um die Ausfallgrenzwerte im Hinblick auf die systematische Sicherheitsintegrität (siehe 3.5.4 von IEC 61508-4) zu erreichen, müssen qualitative Methoden und Beurteilungen unter Berücksichtigung der erforderlichen Vorsichtsmaßnahmen angewendet werden.

ANMERKUNG 9 Die Anforderungen zur Sicherheitsintegrität jeder Sicherheitsfunktion müssen geeignet sein, anzuzeigen, ob der Zielparameter der Sicherheitsintegrität entweder:

- die mittlere Wahrscheinlichkeit eines Ausfalls der entworfenen Funktion bei Anforderung (für eine Betriebsart mit niedriger Anforderungsrate), oder
- die Wahrscheinlichkeit eines gefährbringenden Ausfalls pro Stunde (für eine Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung) ist.

Den SIL-Größen werden aber nicht nur numerische Anforderungen in der Form von Ausfallgrenzwerten für Sicherheitsfunktionen zugeordnet, sondern auch beschreibende Anforderungen an die Qualität sicherheitsbezogener Systeme. Denn es gibt ja auch Fälle im „Lebenszyklus“ des Systems vom Entwurf bis zur Entsorgung, in denen sich keine Ausfallwahrscheinlichkeiten ermitteln lassen. Beispiele sind die kausal determinierten „systematischen“ Ausfälle als Folge von Fehlern, Mängeln und Störungen im Gesamtsystem. Ähnliche Situationen liegen bei Systemen mit frei programmierbaren Rechnern vor: Die Wahrscheinlichkeit dafür, dass ihre Programme einwandfrei ablaufen, hängt nach DIN EN 61508-4 (VDE 0803-4), 3.5.2 von vielen Faktoren ab, die nicht genau zu quantifizieren sind. Verfahren und Maßnahmen, mit denen sich diese beschreibenden Anforderungen bei „SIL 1“ bis „SIL 4“ erfüllen lassen, sind in DIN EN 61508-2 (VDE 0803-2) und DIN EN 61508-3 (VDE 0803-3) aufgeführt. Durch die Kombination numerischer und beschreibender Anforderungen trägt der SIL dazu bei, Risikominderungen rational zu bestimmen und wirkungsvoll auszuführen.

Das Einhalten des SIL und eine positive Beurteilung der funktionalen Sicherheit nach DIN EN 61508-1 (VDE 0803-1), Abschnitt 8, sind eine zwar notwendige, aber noch nicht hinreichende Bedingung für die Sicherheit eines geschützten oder gesteuerten technischen Produktes oder Systems. Außerhalb des Schutz- und Steuerungssystems sind auch die mechanischen, elektrischen, thermischen und weiteren Gefährdungen zu bedenken. Für Maschinen sind Beispiele aus DIN EN ISO 12100-1, Abschnitt 4 auf den *Seiten 32 bis 34* aufgeführt. Auch Fragen zur Vertretbarkeit des Restrisikos, der bestimmungsgemäßen Verwendung, der vernünftigerweise vorhersehbaren Fehlanwendung nach *Seite 27* und andere Einflüsse müssen durch eine abschließende Risikobeurteilung erfasst werden. Für Maschinen gibt DIN EN ISO 12100-1, 5.5 auf *Seite 37* hierzu Hinweise.

Die umfangreiche Normenreihe DIN EN 61508 (VDE 0803) lässt sich branchenweit und erweiterbar für die funktionale Sicherheit der Schutz- und Steuerungssysteme im Personen-, Sach- und Umweltschutz anwenden. Sie dient sie dem Konstrukteur als eine wertvolle Erfahrungssammlung und „Anweisung zum rechten Handeln“.

Prof. em. Dr.-Ing. Dr. h.c. Gerhard Hosemann und Dipl.-Ing. Hartmut von Krosigk
Marloffstein und Erlangen, im Juli 2008

Kostenloses Ansichtsexemplar. Vervielfältigung und Weitergabe an Dritte sind untersagt.

Sonderdruck „Sicherheitsgerechtes Gestalten technischer Erzeugnisse“
– Quantifizierte Risikominderung – Erläuterung



– Frei für Notizen –

	Funktionale Sicherheit	
	Einführung	

1 Einleitung

Bei Betrieb und Verwendung technischer Einrichtungen ist die Sicherheit von Menschen und Umwelt häufig davon abhängig, dass diese Einrichtungen korrekt funktionieren. Zum Beispiel können Fehlfunktionen wie unbeabsichtigter Anlauf einer Maschine oder Versagen einer Bremse Personen und Umwelt erheblich gefährden. Der Schutz vor solchen Gefährdungen wird als „funktionale Sicherheit“ bezeichnet.

2 Grundprinzipien der funktionalen Sicherheit nach IEC 61508

Sicherheit ist aus Sicht des zu schützenden Gutes unteilbar und erfordert den umfassenden Schutz vor Gefährdung verschiedener Ursachen. Technische Maßnahmen zum Erzielen der Sicherheit können, je nach Ursache der möglichen Gefährdung, sehr unterschiedlich sein, deshalb unterscheidet man neuerdings verschiedene Arten von Sicherheit (siehe Bild 1). So spricht man z. B. von "elektrischer Sicherheit", wenn der Schutz vor der Gefährdung durch Elektrizität zum Ausdruck gebracht werden soll, oder von "funktionaler Sicherheit", wenn die Sicherheit von der korrekten Funktion einer Einrichtung abhängt.

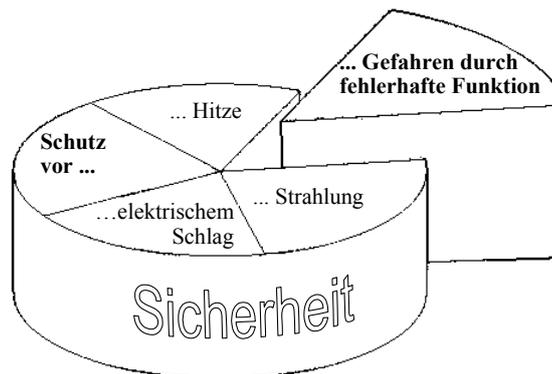


Bild 1 – Teilaspekte von Sicherheit

Wichtig bei der funktionalen Sicherheit ist der Fokus auf die korrekte Funktion, d. h. die mögliche Gefährdung resultiert aus dem Versagen oder dem Fehler einer Funktion. Ein Risiko besteht immer dann, wenn eine Funktion sicherheitsrelevant ist und ihr Versagen oder eine Fehlfunktion zu einer Gefährdung führen kann.

Ein wesentlicher Parameter zur Bemessung eines Risikos ist neben der Größe des Schadens die Wahrscheinlichkeit für das Eintreten des gefährlichen Ereignisses. Aus dieser Betrachtung leitet sich das risiko-orientierte, probabilistische Prinzip von IEC 61508 ab. Durch sicherheitsrelevante Steuer- oder Überwachungsfunktionen wird die Wahrscheinlichkeit für das Eintreten eines gefährlichen Ereignisses um die Versagenswahrscheinlichkeit dieser Funktion vermindert. Die Norm verwendet für dieses Maß den Begriff "Safety Integrity" (Sicherheitsintegrität) und definiert dazu 4 konkrete Stufen, "Safety Integrity Level" genannt (siehe [Tabelle 1](#)).

2.1 Was ist funktionale Sicherheit?

Funktionale Sicherheit ist die Sicherheit vor Gefährdung, die aus der (fehlerhaften) Funktion einer Einrichtung resultiert. Funktionen, deren Versagen zu einer Gefährdung führen kann, werden als sicherheitsrelevante Funktionen oder kurz Sicherheitsfunktionen bezeichnet.

Beispiele:

- Der Zugang zum Gefahrenbereich einer Maschine ist durch Absperrvorrichtungen gesichert. Ihre sicherheitsrelevante Funktion besteht darin, den Zugang zur laufenden Maschine zu verhindern bzw. die Maschine zum Stillstand zu bringen, wenn jemand in den Gefahrenbereich kommt.

- Für Arbeiten an einer Maschine wird deren Bewegungsgeschwindigkeit auf einem ungefährlichen Niveau gehalten. Ein Versagen des Geschwindigkeitsreglers kann zu einer gefährlichen Erhöhung der Geschwindigkeit führen.
- Die Airbagsteuerung in einem Auto darf den Airbag nur bei einem Aufprall auslösen. Eine unbeabsichtigte Auslösung würde zu einer Gefährdung führen.

Entsprechend der Höhe des zu vermeidenden Risikos müssen Sicherheitsfunktionen unterschiedliche sicherheitsbezogene Leistungsfähigkeit haben. Das Maß dafür ist die Sicherheitsintegrität (Safety Integrity).

Definitionen:

funktionale Sicherheit

Teil der Gesamtsicherheit, bezogen auf die EUC (equipment under control) und die EUC-Betriebseinrichtung, die von der korrekten Funktion des E/E/PE-sicherheitsbezogenen Systems (elektrisch/elektronisch/programmierbar elektronisch), Sicherheitssystemen anderer Technologie und externer Einrichtungen zur Risikominderung abhängt

Sicherheitsfunktion

Funktion, die von einem E/E/PE-sicherheitsbezogenem System, einem sicherheitsbezogenem System anderer Technologie oder externer Einrichtungen zur Risikoreduzierung ausgeführt wird mit dem Ziel, unter Berücksichtigung eines festgelegten unerwünschten Ereignisses einen sicheren Zustand für die EUC zu erreichen oder aufrechtzuerhalten

Sicherheitsintegrität

Wahrscheinlichkeit, dass ein sicherheitsbezogenes System die geforderten Sicherheitsfunktionen unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraumes anforderungsgemäß ausführt

Sicherheits-Integritätslevel (SIL)

Eine von vier diskreten Stufen zur Spezifizierung der Anforderung für die Sicherheitsintegrität der Sicherheitsfunktionen, die dem E/E/PE-sicherheitsbezogenen System zugeordnet werden, wobei der Sicherheits-Integritätslevel 4 die höchste Stufe der Sicherheitsintegrität und der Sicherheits-Integritätslevel 1 die niedrigste darstellt

Tabelle 1 – Safety Integrity Level (Stufen der Sicherheitsintegrität)

SIL 1	Nicht mehr als ein gefahrbringender Ausfall der Sicherheitsfunktion in	10 Jahren
SIL 2	Nicht mehr als ein gefahrbringender Ausfall der Sicherheitsfunktion in	100 Jahren
SIL 3	Nicht mehr als ein gefahrbringender Ausfall der Sicherheitsfunktion in	1 000 Jahren
SIL 4	Nicht mehr als ein gefahrbringender Ausfall der Sicherheitsfunktion in	10 000 Jahren

2.2 Bewertung des Risikos

Wesentliche Parameter zur Bemessung eines Risikos sind die Größe des möglichen Schadens und die Wahrscheinlichkeit des Eintretens des gefährlichen Ereignisses. Sicherheitsrelevante Steuer- und Überwachungsfunktionen vermindern die Wahrscheinlichkeit des Eintretens eines gefährlichen Ereignisses um die „Versagenswahrscheinlichkeit“ der Funktion und vermindern so das Risiko.

Definitionen:

Risiko

Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens

2.3 Anwendung einer Steuerung als Sicherheitssystem

Ein Risiko kann von einer Maschine oder Anlage ausgehen, z.B. durch unerwarteten Anlauf der Maschine oder Bersten eines Kessels, wenn die betreffende Steuerungsfunktion fehlerhaft arbeitet oder versagt. Die Risikominderung erfolgt in diesen Fällen dadurch, dass die Versagenswahrscheinlichkeit der Steuerung, die diese Steuerungsfunktion ausführt, verringert wird.

2.4 Wodurch wird funktionale Sicherheit erreicht?

Zielsetzung zur Erreichung funktionaler Sicherheit ist die Begrenzung der Wahrscheinlichkeit eines gefahrbringenden Versagens der Sicherheitsfunktion. Daraus resultieren die Anforderungen von IEC 61508 an sicherheitsbezogene Steuerungen:

- Begrenzung der Wahrscheinlichkeit gefährlicher zufälliger Ausfälle
- ausreichende Hardwarefehler toleranz
- Vermeidung oder Beherrschung systematischer Fehler

Die Vermeidung ungefährlicher Ausfälle dient der Wirtschaftlichkeit, nicht der Sicherheit.

2.5 Fehlerarten

Bei der Betrachtung möglicher Ursachen für die inkorrekte Ausführung einer Funktion durch Steuerungssysteme oder deren Versorgungen unterscheidet man verschiedene Ausfall- bzw. Fehlerarten. Dabei wird bzgl. der möglichen Auswirkungen zwischen "ungefährlichem Ausfall" und "gefährbringendem Ausfall" (siehe Definitionen) und im Bezug auf die Ausfallursache zwischen "systematischem Ausfall" und "zufälligem Hardwareausfall" unterschieden.

Jede Fehlerart kann natürlich jede der genannten Ursachen haben. In Bezug auf Sicherheit ist nur die Wahrscheinlichkeit gefährbringender Fehler bzw. Ausfälle von Bedeutung, unabhängig von ihrer Ursache.

Für die Bestimmung der Ausfallwahrscheinlichkeit ist jedoch die Fehlerursache wichtig. Im Zusammenhang mit "random hardware failures" können Ausfallwahrscheinlichkeiten berechnet werden, da die verursachenden Fehler zufällig auftreten. Bei systematischen Fehlern ist dies kaum möglich. Sie sind permanent im System vorhanden und werden abhängig von bestimmten Ereignissen (z. B. Funktionsabläufen oder Umgebungsbedingungen) wirksam. Deshalb kann eine Wahrscheinlichkeit für ihr Auftreten im Allgemeinen nicht bestimmt werden. IEC 61508 wendet folglich im Zusammenhang mit systematischen Fehlern die probabilistische Betrachtung nicht an, sondern verlangt angemessene Maßnahmen zu ihrer Vermeidung oder Beherrschung.

Definitionen:

Fehler

nicht normale Bedingung, die eine Verminderung oder den Verlust der Fähigkeit einer Funktionseinheit verursachen kann, eine geforderte Funktion auszuführen

Ausfall

Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen

ungefährlicher Ausfall

Ausfall ohne das Potential, das sicherheitsbezogene System in einen gefährlichen oder funktionsunfähigen Zustand zu setzen

gefährbringender Ausfall

Ausfall mit dem Potenzial, das sicherheitsbezogene System in einen gefährlichen oder funktionsunfähigen Zustand zu setzen

systematischer Ausfall

Ausfall, bei dem eindeutig auf eine Ursache geschlossen werden kann, die nur durch eine Veränderung des Entwurfs oder des Fertigungsprozesses, der Art und Weise des Betriebes, der Bedienungsanleitung oder anderer Einflussfaktoren beseitigt werden kann.

zufälliger Hardwareausfall

Ausfall, der zu einem zufälligen Zeitpunkt auftritt und der aus einem oder mehreren möglichen Mechanismen in der Hardware resultiert, die zu einer Verschlechterung der Eigenschaften der Bauteile führen

2.6 Spezifikation der Sicherheitsanforderungen

Ausgangsbasis für die Entwicklung eines sicherheitsrelevanten Systems ist eine Spezifikation der Sicherheitsanforderungen, in der alle Funktionen mit ihren Sicherheitseigenschaften sowie die zugehörigen Umgebungsbedingungen festgelegt sind. Diese Festlegungen resultieren aus einer anwendungsbezogenen Gefährdungs- und Risiko-Analyse mit deren Hilfe die sicherheitsrelevanten Funktionen bestimmt werden, der jeweils notwendige SIL gewählt wird und die Umgebungsbedingungen festgeschrieben werden. Analyse und Spezifikation sind Aufgabe der für die Anlage verantwortlichen Planer. Der Steuerungshersteller muss die Spezifikation erfüllen und mit entsprechenden Methoden an seinen Produkten nachweisen.



Functional Safety in Automation

Content

- **Introduction to Functional Safety**
 - What is „functional safety“
 - Application of functional safety
 - How to achieve functional safety
 - Risk oriented approach of IEC 61508



Safety Terms

- **Risk =**
combination of the probability of occurrence of harm and the severity of that harm





Safety Terms

- **Safety =**
freedom from unacceptable risk



Hartmut von Krosigk

Functional Safety in Automation

3



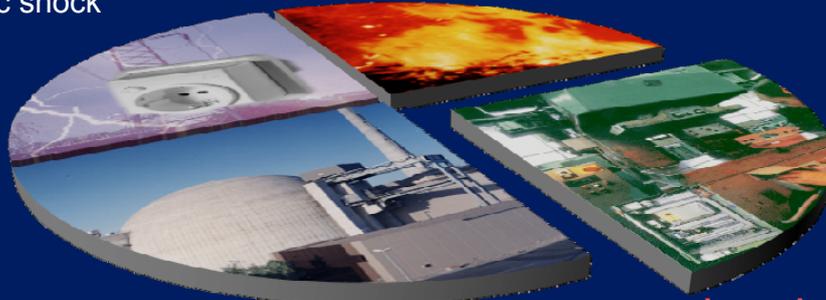
Safety Terms

- **Functional Safety =**
part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures

Safety requires protection against ...

electric shock

heat and fire



dangerous radiation and emissions

hazards due to malfunction

Hartmut von Krosigk

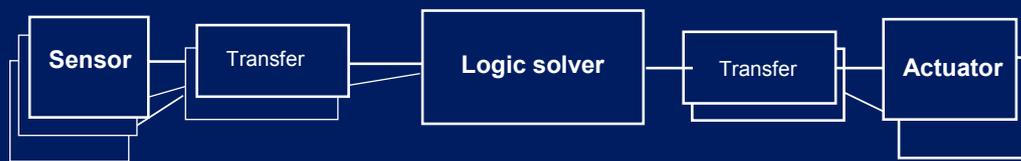
Functional Safety in Automation

4



Safety Terms

- **Safety function =** function, ..., which is intended to achieve or maintain a safe state of the EUC



Complete function:

Acquire information ⇒ **Evaluate information** ⇒ **Execute actions**



Safety Terms

- **Safety-related system =** designated system that both implements the required safety function and is intended to achieve the necessary safety integrity





Risk oriented approach

- **Risk exists**
 - where a failure of a function can cause a hazard.

- **Main parameters to quantify a risk are**
 - severity of harm
 - probability of occurrence of harm



- **Risk oriented probabilistic approach of IEC 61508 of functional safety**

⇒ to limit the risk the probability of occurrence of a hazardous event is limited.



Limit of probability of failure

- **Safety integrity =**
probability of satisfactorily performing the required safety functions (specified by SIL)

Target failure measure:

Safety integrity level	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

e.g. SIL 3: not more than 1 dangerous failure per 1000 years



Safety function: Example Machinery

To protect people.

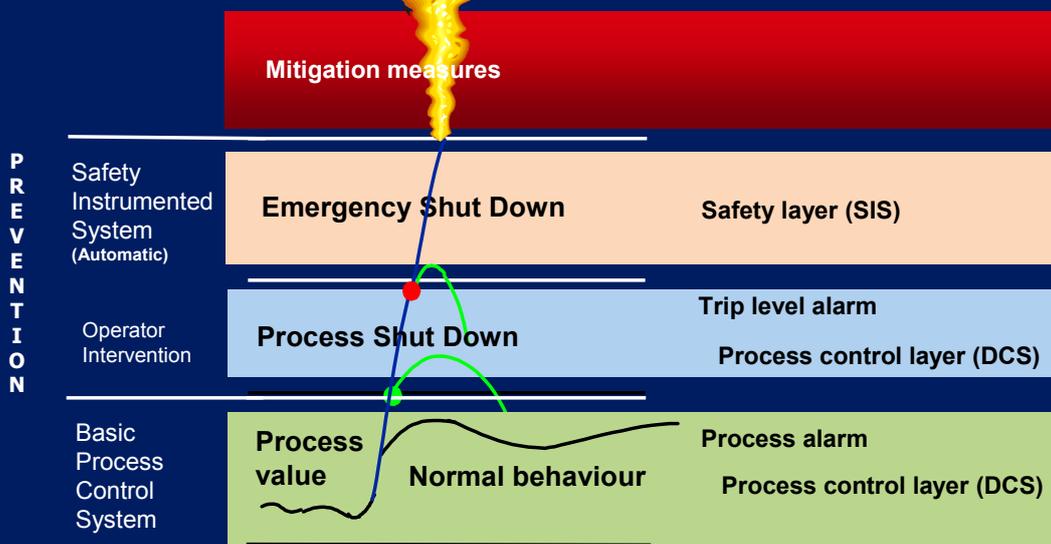
- Guards are used to prevent people from accessing to the dangerous zones while the machine is producing.
- During setting or maintenance the machine must be stopped or its speed must be reduced. Unexpected start or acceleration must be prevented.

→ For safety it is important that control functions operate correctly and protective measures do not fail.



Safety function: Example process plant

In case of failure of the process control system the safety instrumented system is demanded to keep the process in a safe state.





How to achieve functional safety ?

- **Target**
 - ➔ To limit the maximum probability of a dangerous failure of a safety function
- **Solution by IEC 61508**
 - Limitation of the probability of dangerous random hardware failure (hardware safety integrity)
 - Sufficient hardware fault tolerance
 - Avoidance or control of systematic failures (systematic safety integrity)



Types of failure: dangerous failure

- Functional safety will be achieved by avoidance of dangerous failure

Definition

dangerous failure

- Failure which has the potential to put the safety-related system in a hazardous or fail-to-function state





Types of failure: safe failure

- Avoidance of safe failure increases the economic efficiency but not the safety

Definition

safe failure

- failure which does not have the potential to put the safety-related system in a hazardous or fail-to-function state



Reasons of failure

- Random hardware failure
 - The probability of failure can be calculated
- Systematic failure
 - Systematic failure are permanently present in the system
 - Occur depending on certain events like operational conditions, environmental conditions and so on.

Definition

random hardware failure

- failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware

systematic failure

- failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors



Limiting the probability of failure

Design target:

- **The probability of dangerous hardware failure must not exceed the limit set by the SIL.**

Approach:

- **To achieve sufficient low probability of failure subsystems need**
 - diagnostics to detect faults that could cause dangerous failure
 - Redundancy that enables the system to react if a fault has been detected and, if necessary
 - Redundancy to reduce the probability of failure

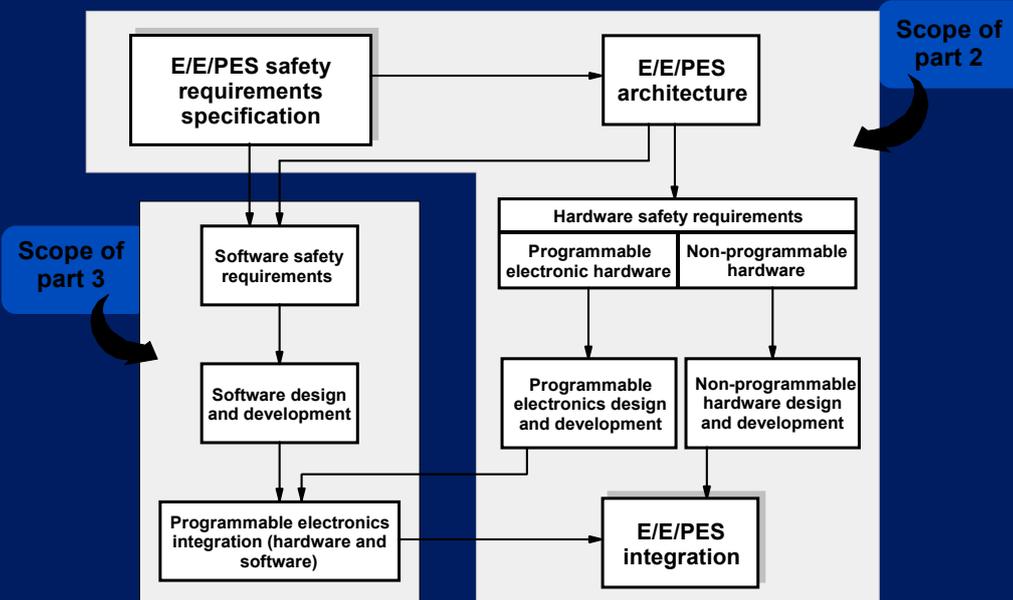


Avoidance of systematic failure

- **Systematic failures are an important part of failures**
 - Comprehensive measures are necessary to avoid them
- **Systematic failures may be caused by:**
 - Mistakes during each phase of the lifecycle
 - Ambiguities in the documentation
 - Misinterpretation of documents
 -
- **Avoidance of systematic failures requires:**
 - A well structured design process
 - Quality management
 - Verification of results of each development step



Software



Hartmut von Krosigk

Functional Safety in Automation

17



Software failures are systematic

- **Systematic failures may be caused by e.g.:**
 - Mistakes during each phase of the lifecycle
 - Ambiguities in the documentation
 - Design mistakes
 - Failures of tools, e.g. compiler
- **Avoidance of systematic failures requires e.g.:**
 - A well structured design process
 - Quality management
 - Verification of results of each development step
- **Control of systematic failures requires e.g.:**
 - Control measure to be implemented in the operational system

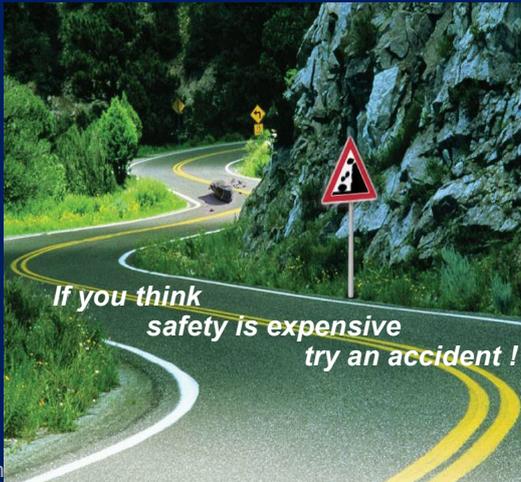
Hartmut von Krosigk

Functional Safety in Automation

18



Questions?



Hartm

Safety in Automation

19

Dipl.-Ing. Hartmut von Krosigk
Erlangen, im Juli 2008

Kostenloses Ansichtsexemplar. Vervielfältigung und Weitergabe an Dritte sind untersagt.

Sonderdruck „Sicherheitsgerechtes Gestalten technischer Erzeugnisse“

– Funktionale Sicherheit – Einführung



– Frei für Notizen –

November 2002

	Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen (IEC 61508-1:1998 + Corrigendum 1999); Deutsche Fassung EN 61508-1:2001	DIN EN 61508-1
VDE	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Vorstand beschlossenen Genehmigungsverfahrens unter nebenstehenden Nummern in das VDE-Vorschriftenwerk aufgenommen und in der etz Elektrotechnische Zeitschrift bekannt gegeben worden.	Klassifikation VDE 0803 Teil 1

Vervielfältigung – auch für innerbetriebliche Zwecke – nicht gestattet.

Einleitung

- 1 Anwendungsbereich
 - 2 Normative Verweisungen
 - 3 Begriffe und Abkürzungen
 - 4 Übereinstimmung mit dieser Norm
 - 5 Dokumentation
 - 6 Management der funktionalen Sicherheit
 - 7 Anforderungen zum gesamten Sicherheitslebenszyklus
 - 7.1 Allgemeines
 - 7.2 Konzept
 - 7.3 Definition des gesamten Anwendungsbereiches
 - 7.4 Gefährdungs- und Risikoanalyse
 - 7.5 Gesamte Sicherheitsanforderungen
 - 7.6 Zuordnung der Sicherheitsanforderungen
 - 7.7 Planung des Gesamtbetriebs und der gesamten Instandhaltung
 - 7.8 Planung der Sicherheits-Gesamtvalidierung
 - 7.9 Planung der Gesamtinstallation und Gesamtinbetriebnahme
 - 7.10 Realisierung: E/E/PES
 - 7.11 Realisierung: Sicherheitsbezogene Systeme anderer Technologie
 - 7.12 Realisierung: Externe Einrichtungen zur Risikominderung
 - 7.13 Gesamtinstallation und Gesamtinbetriebnahme
 - 7.14 Sicherheits-Gesamtvalidierung
 - 7.15 Gesamtbetrieb, gesamte Instandhaltung und Reparatur
 - 7.16 Gesamtmodifikation und gesamte Nachrüstung
 - 7.17 Außerbetriebnahme oder Ausmusterung
 - 7.18 Verifikation
 - 8 Beurteilung der funktionalen Sicherheit
- Anhang A (informativ) Beispiel einer Dokumentationsstruktur
Anhang B (informativ) Kompetenz von Personen

Beginn der Gültigkeit

Die EN 61508-1 wurde am 2001-07-03 angenommen.

Der Norm-Inhalt war veröffentlicht als E DIN IEC 65A/179/CDV (VDE 0801 Teil 1):1995-12.

Vorwort

...

Der CENELEC-Bericht ROBT-004, der auf der 103. Sitzung des technischen Büros im März 2000 angenommen wurde, geht davon aus, dass einige IEC-Normen, die bereits veröffentlicht sind oder gerade erarbeitet werden, Implementierung der IEC 61508 für ein bestimmtes Anwendungsgebiet darstellen, z. B.:

- IEC 61511, Functional safety – Safety instrumented systems for the process industry sector;
- IEC 62061, Safety of machinery – Functional safety of electrical, electronic and programmable electronic control systems;
- IEC 61513, Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems.

Für das Anwendungsgebiet des Eisenbahnwesens wurde ebenfalls eine Reihe Europäischer Normen erstellt (EN 50126; EN 50128 und prEN 50129).

ANMERKUNG EN 50126 und EN 50128 beruhen auf früheren Entwürfen der IEC 61508. prEN 50129 beruht auf den Grundsätzen der jetzt gültigen Fassung der IEC 61508.

Diese Aufzählung schließt nicht aus, dass weitere Implementierungen der IEC 61508 für bestimmte Anwendungsgebiete, die sich gerade in der Erarbeitung oder Veröffentlichung innerhalb IEC oder CENELEC befinden, erscheinen.

...

Einleitung

Systeme, die aus elektrischen und/oder elektronischen Bauteilen bestehen, werden seit vielen Jahren verwendet, um Sicherheitsfunktionen in vielen Anwendungsbereichen auszuführen. Auf Rechnern basierende Systeme (allgemein ausgedrückt programmierbare elektronische Systeme (PES)) werden in allen Anwendungsbereichen benutzt, um Nichtsicherheitsfunktionen und zunehmend auch um Sicherheitsfunktionen auszuführen. Falls Rechnersystemtechnologie wirksam und sicherheitsgerecht eingesetzt wird, ist es wichtig, dass die für die Entscheidungsfindung Verantwortlichen ausreichende Hilfestellung bezüglich der Sicherheitsaspekte erhalten, nach denen Entscheidungen getroffen werden.

Diese Internationale Norm beschreibt einen allgemeinen Lösungsweg für alle Tätigkeiten während des Sicherheitslebenszyklus für Systeme, die aus elektrischen und/oder elektronischen und/oder programmierbaren elektronischen Bauteilen bestehen (elektrische/elektronische/programmierbare elektronische Systeme (E/E/PES)) und die eingesetzt werden, um Sicherheitsfunktionen auszuführen. Dieser allgemeine Lösungsweg wurde gewählt, um ein sinnvolles und konsistentes technisches Verfahren für alle elektrischen Sicherheitssysteme zu entwickeln. Ein Hauptziel ist es, die Entwicklung von anwendungsspezifischen Normen zu erleichtern.

In den meisten Situationen wird Sicherheit durch eine Anzahl von Schutzsystemen erreicht, die auf vielerlei Technologien (zum Beispiel Mechanik, Hydraulik, Pneumatik, Elektrik, Elektronik, programmierbare Elektronik) basieren. Jede Sicherheitsstrategie muss deshalb nicht nur alle Elemente innerhalb eines Einzelsystems (zum Beispiel Sensoren, Steuereinheiten und Aktoren) betrachten, sondern auch all die sicherheitsbezogenen Systeme, die einzelne Teile einer Gesamtheit sind. Da sich diese Internationale Norm mit sicherheitsbezogenen elektrischen/elektronischen/programmierbaren elektronischen (E/E/PE) Systemen beschäftigt, kann sie einen Rahmen bereitstellen, innerhalb dessen sicherheitsbezogene Systeme, basierend auf anderen Technologien, betrachtet werden können.

Es ist berücksichtigt worden, dass eine große Vielfalt von E/E/PES-Anwendungen in vielfältigen Anwendungsbereichen vorliegt und diese einen weiten Bereich in Bezug auf Komplexität, Gefährdungs- und Risikopotentiale abdeckt. In jeder speziellen Anwendung sind die erforderlichen Sicherheitsmaßnahmen von vielen anwendungsspezifischen Faktoren abhängig. Dadurch, dass diese Internationale Norm allgemein gehalten ist, wird die Formulierung solcher Maßnahmen in zukünftigen anwendungsspezifischen Internationalen Normen ermöglicht.

Diese Internationale Norm:

- betrachtet alle relevanten sicherheitsbezogenen Phasen des Gesamtsystems der E/E/PES und des Software-Sicherheitslebenszyklus (zum Beispiel vom anfänglichen Konzept über Entwurf, Durchführung, Betrieb und Instandhaltung bis zur Außerbetriebnahme), wenn E/E/PES benutzt werden, um Sicherheitsfunktionen auszuführen;

- wurde unter Berücksichtigung einer sich schnell entwickelnden Technologie entworfen. Der Betrachtungsrahmen ist ausreichend robust und ausführlich genug, um auch für zukünftige Entwicklungen verwendbar zu sein;
- ermöglicht die Erstellung anwendungsspezifischer Internationaler Normen, die sich mit sicherheitsbezogenen E/E/PES befassen. Die Entwicklung anwendungsspezifischer Normen sollte innerhalb des Rahmens dieser Internationalen Norm zu einem hohen Grad an Übereinstimmung (zum Beispiel von zugrunde liegenden Prinzipien, Terminologie usw.) führen, sowohl innerhalb der Anwendungsbereiche als auch über die Anwendungsbereiche hinweg. Dies hat sowohl sicherheitstechnische als auch wirtschaftliche Vorteile;
- liefert eine Methode für die Entwicklung der Spezifikation der Sicherheitsanforderungen, die notwendig ist, um die notwendige funktionale Sicherheit des sicherheitsbezogenen E/E/PE-Systems zu erreichen;
- verwendet Sicherheits-Integritätslevel für die Spezifikation der Zielvorgabe der Sicherheitsintegrität der Sicherheitsfunktionen, die in dem sicherheitsbezogenen E/E/PE-System implementiert werden;
- verwendet einen auf dem Risiko basierenden Lösungsansatz für die Festlegung der Anforderungen der Sicherheits-Integritätslevel;
- setzt numerische Ausfallgrenzwerte für sicherheitsbezogene E/E/PE-Systeme, die mit Sicherheits-Integritätsleveln verbunden sind;
- setzt eine untere Grenze des Ausfallgrenzwertes für eine gefahrbringende Ausfallart, der für ein einzelnes sicherheitsbezogenes E/E/PE-System beansprucht werden kann. Für sicherheitsbezogene E/E/PE-Systeme, die:
 - in der Betriebsart mit einer niedrigen Anforderungsrate betrieben werden, ist die untere Grenze der mittleren Wahrscheinlichkeit, die entworfene Funktion auf Anforderung nicht auszuführen, auf 10^{-5} festgelegt;
 - in der Betriebsart mit einer hohen oder ununterbrochenen Anforderungsrate betrieben werden, ist die untere Grenze der Wahrscheinlichkeit eines gefahrbringenden Ausfalls auf 10^{-9} pro Stunde festgelegt;

ANMERKUNG Ein einzelnes sicherheitsbezogenes E/E/PE-System bedeutet nicht auch notwendigerweise eine einkanalige Architektur.

- lässt einen weiten Bereich von Prinzipien, Techniken und Maßnahmen zu, um funktionale Sicherheit für sicherheitsbezogene E/E/PE-Systeme zu erreichen, verwendet aber nicht das Fail-safe-Konzept, das genutzt werden kann, wenn das Ausfallverhalten gut definiert und das Niveau der Komplexität verhältnismäßig niedrig ist. Das Fail-safe-Konzept wurde wegen des weiten Bereiches der Komplexität von sicherheitsbezogenen E/E/PE-Systemen, die im Rahmen der Norm behandelt werden, als ungeeignet betrachtet.

1 Anwendungsbereich

1.1 Diese Internationale Norm behandelt diejenigen Gesichtspunkte, die zu betrachten sind, wenn elektrische/elektronische/programmierbar elektronische Systeme (E/E/PES) zur Ausführung von Sicherheitsfunktionen eingesetzt werden. Ein Hauptziel dieser Norm ist es, für ein bestimmtes Anwendungsgebiet die Entwicklung einer entsprechenden Internationalen Norm durch das jeweils verantwortliche Komitee zu ermöglichen. Dies wird es erlauben, alle wichtigen Einflussgrößen dieses Anwendungsgebietes vollständig zu berücksichtigen und damit dessen besonderen Erfordernissen nachzukommen. Ein zweites Ziel dieser Norm ist es, die Entwicklung eines elektrischen/elektronischen/programmierbar elektronischen (E/E/PE) sicherheitsbezogenen Systems, für dessen Anwendungsgebiet noch keine Internationale Norm besteht, zu ermöglichen.

1.2 Insbesondere:

- a) gilt diese Norm für sicherheitsbezogene Systeme, wenn eines oder mehrere dieser Systeme elektrische/elektronische/programmierbar elektronische Geräte enthalten;

ANMERKUNG 1 Für einfache sicherheitsbezogene E/E/PE-Systeme geringer Komplexität können bestimmte, in dieser Norm festgelegte Anforderungen unnötig sein, und eine Befreiung von der Normerfüllung in Bezug auf solche Anforderungen ist möglich (siehe 4.2 und Definition eines einfachen sicherheitsbezogenen E/E/PE-Systems in 3.4.4 von IEC 61508-4).

ANMERKUNG 2 Obwohl eine Person ein Teil eines sicherheitsbezogenen Systems sein kann (siehe 3.4.1 von IEC 61508-4), werden Anforderungen zu menschlichen Faktoren in Bezug auf den Entwurf der sicherheitsbezogenen E/E/PE-Systeme in dieser Norm nicht im Detail betrachtet.

- b) ist diese Norm allgemein gültig und auf alle sicherheitsbezogenen E/E/PE-Systeme, unabhängig von der Anwendung, anwendbar;

- c) behandelt diese Norm mögliche Gefährdungen, die durch Ausfälle der durch die sicherheitsbezogenen E/E/PE-Systeme ausgeführten Sicherheitsfunktionen bedingt sind, diese sind verschieden von Gefährdungen, die von der E/E/PE-Einrichtung selbst ausgehen (zum Beispiel elektrischer Schlag usw.);
- d) behandelt diese Norm nicht E/E/PE-Systeme, bei denen:
 - ein einzelnes E/E/PE-System fähig ist, die notwendige Risikominderung zu liefern, und
 - die erforderliche Sicherheitsintegrität des E/E/PE-Systems geringer als die Sicherheitsintegrität ist, die für den Sicherheits-Integritätslevel 1 (dem geringsten Sicherheits-Integritätslevel in dieser Norm) festgelegt ist;
- e) befasst sich diese Norm hauptsächlich mit den sicherheitsbezogenen E/E/PE-Systemen, deren Ausfall einen Einfluss auf die Sicherheit von Personen und/oder die Sicherheit der Umwelt haben könnte – es ist jedoch bekannt, dass die Auswirkungen von Ausfällen auch ernsthafte wirtschaftliche Auswirkungen haben können. In solchen Fällen kann diese Norm verwendet werden, um ein beliebiges E/E/PE-System, das zum Schutz von Einrichtungen oder Produkten verwendet wird, festzulegen;

ANMERKUNG Siehe 3.1.1 und 7.3.1.2 der IEC 61508-4.

- f) betrachtet diese Norm sicherheitsbezogene E/E/PE-Systeme, sicherheitsbezogene Systeme anderer Technologie und externe Einrichtungen zur Risikominderung, damit die Spezifikation der Sicherheitsanforderungen für die sicherheitsbezogenen E/E/PE-Systeme in einer systematischen, risikoorientierten Art und Weise festgelegt werden kann;
- g) verwendet diese Norm als technischen Rahmen das Modell eines gesamten Sicherheitslebenszyklus, um diejenigen Tätigkeiten systematisch zu behandeln, die für die Sicherstellung der funktionalen Sicherheit der sicherheitsbezogenen E/E/PE-Systeme notwendig sind;

ANMERKUNG 3 Die frühen Phasen des gesamten Sicherheitslebenszyklus schließen notwendigerweise die Berücksichtigung anderer Technologien (wie auch die sicherheitsbezogenen E/E/PE-Systeme) und externe Einrichtungen zur Risikominderung ein, damit die Spezifikation der Sicherheitsanforderungen für die sicherheitsbezogenen E/E/PE-Systeme in einer systematischen, risikoorientierten Art und Weise entwickelt werden kann.

ANMERKUNG 4 Obwohl der gesamte Sicherheitslebenszyklus vornehmlich mit sicherheitsbezogenen E/E/PE-Systemen befasst ist, kann er auch einen technischen Rahmen für die Betrachtung eines beliebigen sicherheitsbezogenen Systems, ungeachtet der Technologie dieses Systems (zum Beispiel Mechanik, Hydraulik oder Pneumatik), liefern.

- h) legt diese Norm nicht die Sicherheits-Integritätslevel für spezifische Anwendungen (welche sich auf ausführliche Informationen und Kenntnis über die spezifische Anwendung stützen müssen) fest. Die für die spezifischen Anwendungen verantwortlichen technischen Komitees müssen, wenn dies angebracht ist, die Sicherheits-Integritätslevel in anwendungsspezifischen Normen festlegen;
- i) liefert diese Norm allgemeine Anforderungen für sicherheitsbezogene E/E/PE-Systeme, für die keine anwendungsspezifischen Normen vorhanden sind;
- j) enthält diese Norm nicht die Vorsichtsmaßnahmen, die notwendig sein können, um zu verhindern, dass unberechtigte Personen die funktionale Sicherheit von sicherheitsbezogenen E/E/PE-Systemen schädigen und/oder anderweitig ungünstig beeinflussen.

1.3 Dieser Teil von IEC 61508 legt die allgemeinen Anforderungen fest, die auf alle Teile anwendbar sind. Andere Teile von IEC 61508 konzentrieren sich mehr auf spezifische Themen:

- Die Teile 2 und 3 enthalten zusätzliche und besondere Anforderungen für sicherheitsbezogene E/E/PE-Systeme (für Hardware und Software);
- Teil 4 enthält Definitionen und Abkürzungen, die in der ganzen Norm verwendet werden;
- Teil 5 liefert anhand von Beispielen Hinweise für die Anwendung von Teil 1 zur Festlegung von Sicherheits-Integritätsleveln;
- Teil 6 liefert Hinweise für die Anwendung der Teile 2 und 3;
- Teil 7 enthält einen Überblick über Methoden und Maßnahmen.

1.4 Die Teile 1, 2, 3 und 4 dieser Norm sind Sicherheits-Grundnormen, dieser Status ist aber im Zusammenhang mit einfachen E/E/PE-sicherheitsbezogenen Systemen nicht anwendbar (siehe 3.4.4 von Teil 4). Als Sicherheits-Grundnormen sind sie zur Verwendung durch technische Komitees bei der Erstellung von Normen nach IEC Guide 104 und ISO/IEC Guide 51 vorgesehen. Die IEC 61508 ist ebenfalls zur Verwendung als eigenständige Norm vorgesehen.

Es steht in der Verantwortlichkeit eines Technischen Komitees, zur Vorbereitung und Erstellung eigener Festlegungen soweit möglich die Sicherheits-Grundnormen anzuwenden. In diesem Zusammenhang gilt, dass die Anforderungen, Prüfverfahren oder Prüfbedingungen dieser Sicherheits-Grundnorm nur dann anwendbar sind, wenn in den Festlegungen der Technischen Komitees darauf verwiesen wird oder diese eingebunden werden.

ANMERKUNG In den USA und Kanada können vorhandene nationale Sicherheitsnormen für den Bereich der Prozessindustrie auf Basis der IEC 61508 (d. h. ANSI/ISA S84.01-1996) (siehe Hinweis [8] in Anhang C) anstelle der IEC 61508 verwendet werden, bis die beabsichtigte sektorspezifische Umsetzung der IEC 61508 als eine Internationale Norm in den USA und Kanada veröffentlicht wird.

1.5 [Bild 1](#) zeigt den Gesamtrahmen für die Teile 1 bis 7 der IEC 61508 und zeigt die Rolle, die die IEC 61508-1 beim Erreichen der funktionalen Sicherheit für sicherheitsbezogene E/E/PE-Systeme spielt.

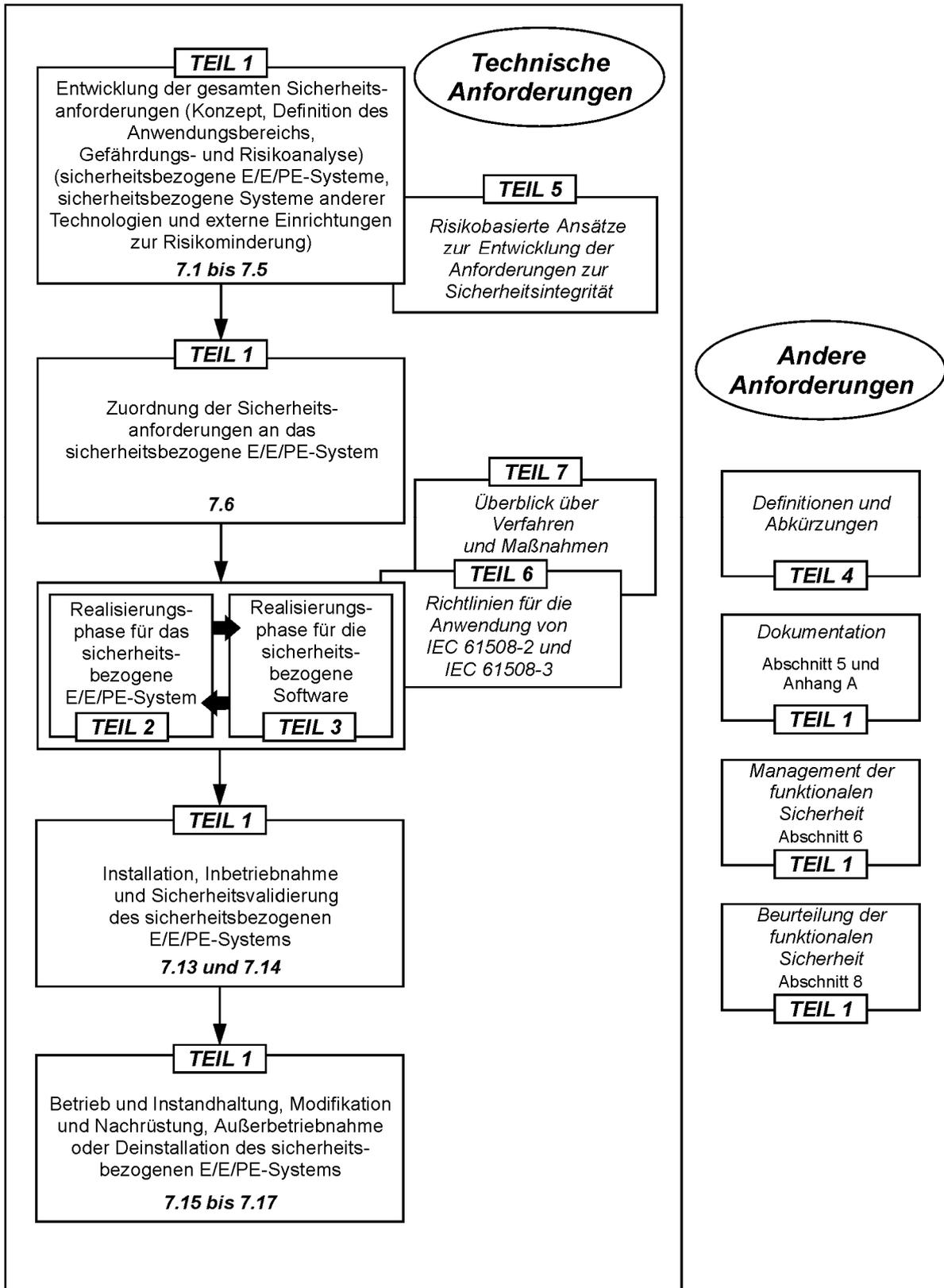


Bild 1 – Gesamtrahmen dieser Norm

7 Anforderungen zum gesamten Sicherheitslebenszyklus

7.1 Allgemeines

7.1.1 Einleitung

7.1.1.1 Um auf systematische Art und Weise alle Tätigkeiten, die zum Erreichen des erforderlichen Sicherheits-Integritätslevels für die sicherheitsbezogenen E/E/PE-Systeme notwendig sind, abzuhandeln, verwendet diese Norm als technischen Rahmen einen gesamten Sicherheitslebenszyklus (siehe [Bild 2](#)).

ANMERKUNG Für den Anspruch auf Übereinstimmung mit dieser Norm sollte der gesamte Sicherheitslebenszyklus als Grundlage verwendet werden. Es kann jedoch ein von dem im [Bild 2](#) gezeigten verschiedener gesamter Sicherheitslebenszyklus verwendet werden, vorausgesetzt, die Ziele und Anforderungen jedes Abschnitts dieser Norm werden erfüllt.

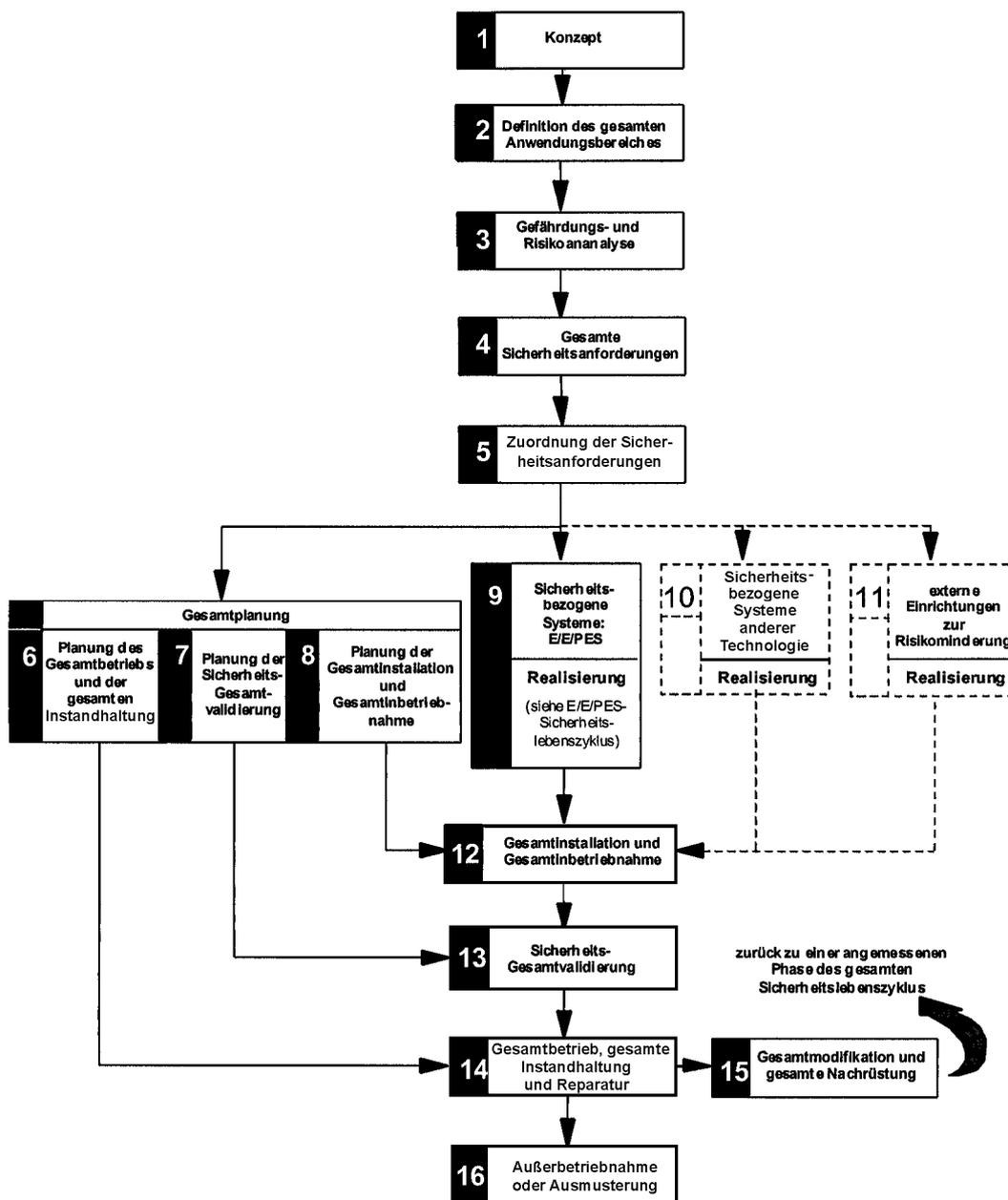
7.1.1.2 Der gesamte Sicherheitslebenszyklus enthält folgende Maßnahmen zur Risikominderung:

- sicherheitsbezogene E/E/PE-Systeme;
- sicherheitsbezogene Systeme anderer Technologie;
- externe Einrichtungen zur Risikominderung.

7.1.1.3 Der Teil des gesamten Sicherheitslebenszyklus, der sich mit sicherheitsbezogenen E/E/PE-Systemen beschäftigt, wird in [Bild 3](#) erweitert und gezeigt. Dieser wird E/E/PES-Sicherheitslebenszyklus genannt und bildet den technischen Gesamtrahmen für IEC 61508-2. Der Software-Sicherheitslebenszyklus wird in [Bild 4](#) gezeigt und bildet den technischen Gesamtrahmen für IEC 61508-3. Die Beziehung des gesamten Sicherheitslebenszyklus zum E/E/PES-Sicherheitslebenszyklus und zum Software-Sicherheitslebenszyklus für sicherheitsbezogene Systeme wird in [Bild 5](#) gezeigt.

7.1.1.4 Die Bilder zum gesamten Sicherheitslebenszyklus, zum E/E/PES-Sicherheitslebenszyklus und zum Software-Sicherheitslebenszyklus ([Bilder 2 bis 4](#)) sind vereinfachte Betrachtungen der Realität und zeigen als solche nicht alle Iterationen bezüglich der speziellen Phasen oder Zwischenphasen. Iterationen sind aber innerhalb des gesamten Sicherheitslebenszyklus, des E/E/PES-Sicherheitslebenszyklus und des Software-Sicherheitslebenszyklus ein notwendiger und wichtiger Teil der Entwicklung.

7.1.1.5 Tätigkeiten in Bezug auf das Management der funktionalen Sicherheit (Abschnitt 6), Verifikation (7.18) und Beurteilung der funktionalen Sicherheit (Abschnitt 8) werden nicht in dem gesamten Sicherheitslebenszyklus, dem E/E/PES-Sicherheitslebenszyklus oder dem Software-Sicherheitslebenszyklus gezeigt. Dies erfolgte, um die Komplexität der Bilder zum gesamten Sicherheitslebenszyklus, zum E/E/PES-Sicherheitslebenszyklus und zum Software-Sicherheitslebenszyklus zu reduzieren. Diese Tätigkeiten müssen, wo erforderlich, in den Phasen des gesamten Sicherheitslebenszyklus, des E/E/PES-Sicherheitslebenszyklus und des Software-Sicherheitslebenszyklus berücksichtigt werden.



ANMERKUNG 1 Tätigkeiten in Bezug auf **Verifikation, Sicherheit und Beurteilung der funktionalen Sicherheit** sind zur besseren Übersicht nicht gezeigt, gehören jedoch zu allen Phasen des gesamten Sicherheitslebenszyklus, des E/E/PES-Sicherheitslebenszyklus und des Software-Sicherheitslebenszyklus.

ANMERKUNG 2 Die Phasen, die durch die Kästen 10 und 11 dargestellt werden, liegen außerhalb des Anwendungsbereiches dieser Norm.

ANMERKUNG 3 IEC 61508-2 und IEC 61508-3 behandeln Kasten 9 (Realisierung), sie beschäftigen sich jedoch auch, wo zutreffend, mit Aspekten der programmierbaren Elektronik (Hardware und Software) der Kästen 13, 14 und 15.

Bild 2 – Gesamter Sicherheitslebenszyklus

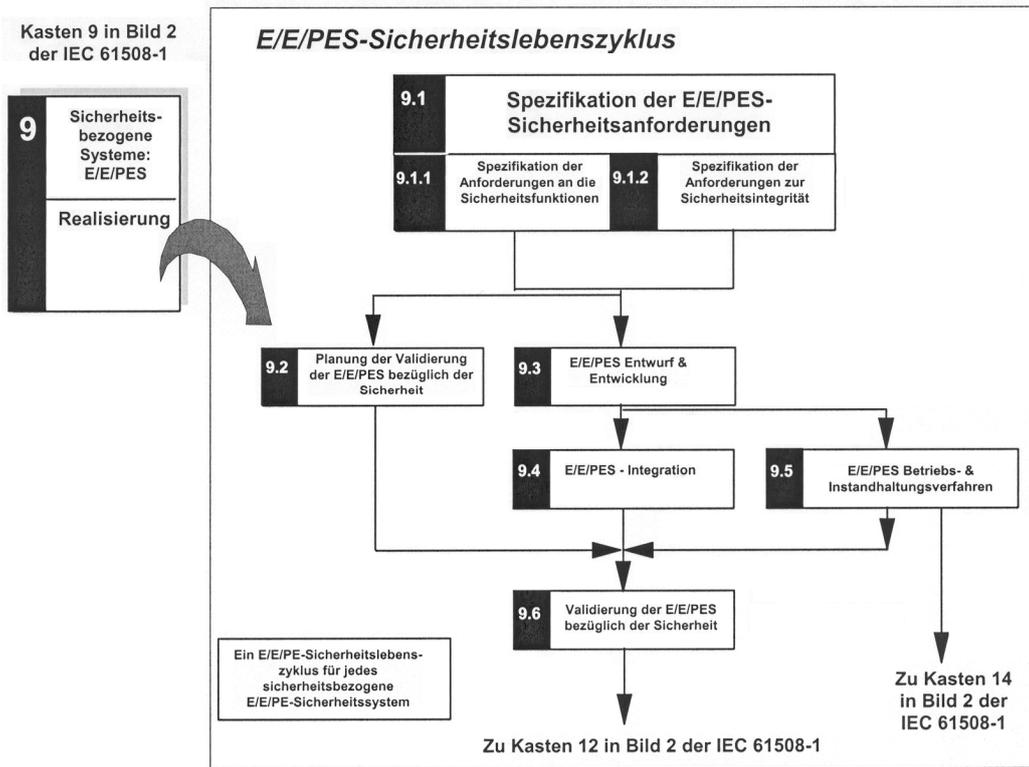


Bild 3 – E/E/PES-Sicherheitslebenszyklus (in der Realisierungsphase)

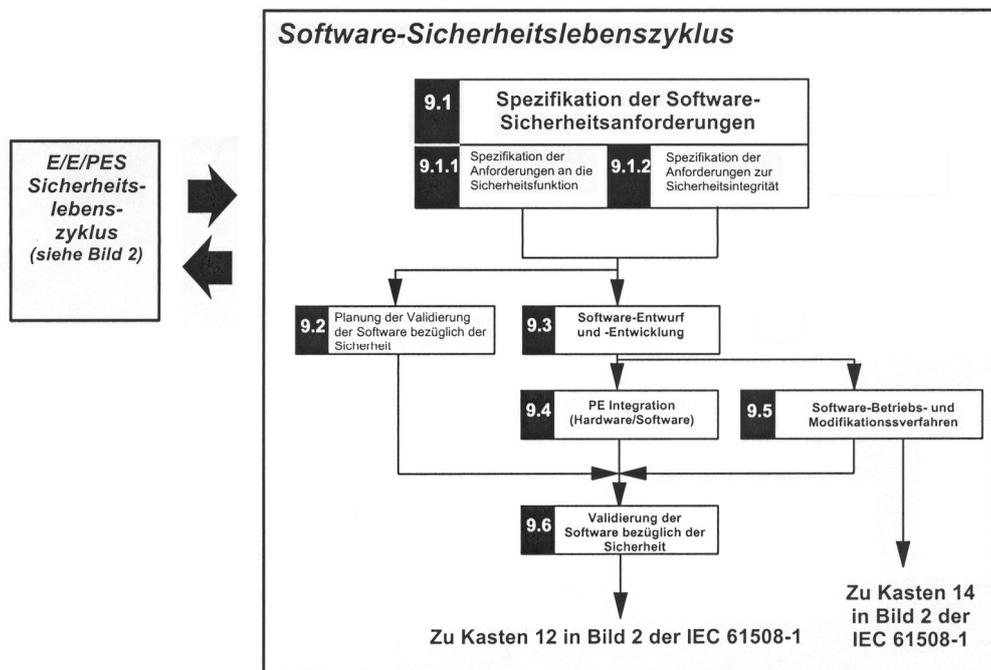


Bild 4 – Software-Sicherheitslebenszyklus (in der Realisierungsphase)

Kostenloses Ansichtsexemplar. Vervielfältigung und Weitergabe an Dritte sind untersagt.

Sonderdruck „Sicherheitsgerechtes Gestalten technischer Erzeugnisse“
aus DIN EN 61508-1 (VDE 0803-1):2002-11



– Frei für Notizen –

Gezielt zusammengestellte VDE-Auswahlreihen
als wichtige Grundausstattungen im Angebot des VDE VERLAGS

VDE-Auswahl zur funktionalen Sicherheit

Liste der enthaltenen Normen
Stand Oktober 2008

Weitere Informationen siehe

<http://www.vde-verlag.de/normen/auswahlen.html>

VDE 0022:2008-08

Satzung für das Vorschriftenwerk des VDE Verband der Elektrotechnik Elektronik Informationstechnik e. V.

DIN EN 62079 (**VDE 0039**):2001-11

Erstellen von Anleitungen – Gliederung, Inhalt und Darstellung

DIN EN 60204-1 (**VDE 0113-1**):2007-06

Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen – Teil 1: Allgemeine Anforderungen

DIN EN 62061 (**VDE 0113-50**):2005-10

Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme

DIN EN 62061 (**VDE 0113-50**) Berichtigung 1:2006-06

Berichtigungen zu DIN EN 62061 (VDE 0113-50):2005-10

DIN EN 61310-1 (**VDE 0113-101**):2008-09

Sicherheit von Maschinen – Anzeigen, Kennzeichen und Bedienen – Anforderungen an sichtbare, hörbare und tastbare Signale

DIN EN 61310-2 (**VDE 0113-102**):2008-09

Sicherheit von Maschinen – Anzeigen, Kennzeichen und Bedienen – Anforderungen an die Kennzeichnung

DIN EN 61310-3 (**VDE 0113-103**):2008-09

Sicherheit von Maschinen – Anzeigen, Kennzeichen und Bedienen – Anforderungen an die Anordnung und den Betrieb von Bedienteilen (Stellteilen)

DIN EN 61496-1 (**VDE 0113-201**):2005-01

Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 1: Allgemeine Anforderungen und Prüfungen

DIN EN 61496-3 (**VDE 0113-203**):2002-01

Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Besondere Anforderungen an diffuse Reflektion nutzende aktive optoelektronische Schutzeinrichtungen (AOPDDR)

DIN EN 50126 (**VDE 0115-103**):2000-03

Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS)

DIN EN 50126 (**VDE 0115-103**) Berichtigung 1:2006-09

Berichtigungen zu DIN EN 50126 (VDE 0115-103):2000-03

DIN EN 50156-1 (**VDE 0116-1**):2005-03

Elektrische Ausrüstung von Feuerungsanlagen – Teil 1: Bestimmungen für die Anwendungsplanung und Errichtung

DIN VDE 0119-207-6 (**VDE 0119-207-6**):2004-04

Zustand der Eisenbahnfahrzeuge – Leittechnik – Teil 207-6: Fahrzeugeinrichtung – PZB-Indusi

DIN EN 61800-5-2 (**VDE 0160-105-2**):2008-04

Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit

DIN EN 60073 (**VDE 0199**):2003-05

Grund- und Sicherheitsregeln für die Mensch-Maschine-Schnittstelle, Kennzeichnung – Codierungsgrundsätze für Anzeigengeräte und Bedienteile

DIN EN 50402 (**VDE 0400-70**):2006-03

Elektrische Geräte für die Detektion und Messung von brennbaren oder toxischen Gasen und Dämpfen oder Sauerstoff – Anforderungen an die funktionale Sicherheit von ortsfesten Gaswarnsystemen

DIN IEC 61513 (**VDE 0491-2**):2002-10

Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen

DIN IEC 61513/A100 (**VDE 0491-2/A100**):2005-02

Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen – Nationaler Anhang ND (informativ): Mitgeltende Festlegungen aus anderen IEC-Normen

DIN IEC 60987 (**VDE 0491-3-1**):2008-04

Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die Hardwareauslegung rechnerbasierter Systeme

DIN IEC 60880 (**VDE 0491-3-2**):2007-08

Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A

DIN IEC 62241 (**VDE 0491-5-2**):2006-05

Kernkraftwerke – Hauptwarte – Funktionen zur Meldung und Anzeige von Störungen

DIN EN 61508 Beiblatt 1 (**VDE 0803 Beiblatt 1**):2005-10

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 0: Funktionale Sicherheit und die IEC 61508

DIN EN 61508-1 (**VDE 0803-1**):2002-11

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Allgemeine Anforderungen

DIN EN 61508-2 (**VDE 0803-2**):2002-12

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme

DIN EN 61508-3 (**VDE 0803-3**):2002-12

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Anforderungen an Software

DIN EN 61508-4 (**VDE 0803-4**):2002-11

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Begriffe und Abkürzungen

DIN EN 61508-5 (**VDE 0803-5**):2002-11

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level)

DIN EN 61508-6 (**VDE 0803-6**):2003-06

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3

DIN EN 61508-7 (**VDE 0803-7**):2003-06

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 7: Anwendungshinweise über Verfahren und Maßnahmen

DIN EN 61511-1 (**VDE 0810-1**):2005-05

Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie – Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Software und Hardware

DIN EN 61511-2 (**VDE 0810-2**):2005-05

Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie – Teil 2: Anleitungen zur Anwendung des Teils 1

DIN EN 61511-3 (**VDE 0810-3**):2005-05

Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie – Teil 3: Anleitung für die Bestimmung der erforderlichen Sicherheits-Integritätslevel

DIN EN 50159-1 (**VDE 0831-159-1**):2001-11

Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante Kommunikation in geschlossenen Übertragungssystemen

DIN EN 50159-2 (**VDE 0831-159-2**):2001-12

Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante Kommunikation in offenen Übertragungssystemen

DIN EN 61326-1 (**VDE 0843-20-1**):2006-10

Elektrische Mess-, Steuer-, Regel- und Laborgeräte – EMV-Anforderungen – Teil 1: Allgemeine Anforderungen

DIN EN 61326-1 Berichtigung 1 (**VDE 0843-20-1 Berichtigung 1**):2008-06

Berichtigungen zu DIN EN 61326-1 (VDE 0843-20-1):2006-10

DIN VDE 0845 Beiblatt 1 (**VDE 0845 Beiblatt 1**):2007-01

Überspannungsschutz von Einrichtungen der Informationstechnik (IT-Anlagen)

Organisation der nationalen, europäischen und internationalen Normung

	Elektrotechnik	Telekommunikation	Alle anderen Bereiche
Welt	 International Electrotechnical Commission (Genf) <i>gegr. 1906</i>	 International Telecommunication Union (Genf) <i>gegr. 1865</i>	 International Organization for Standardization (Genf) <i>gegr. 1946</i>
Europa	 Comité Européen de Normalisation Electrotechnique (Brüssel) <i>gegr. 1959 [CENELCOM]</i>	 European Telecommunications Standards Institute (Sophia Antipolis) <i>gegr. 1988</i>	 Comité Européen de Normalisation (Brüssel) <i>gegr. 1961</i>
Deutschland	 DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (Frankfurt am Main) <i>gegr. 1893 [VDE]</i>	 DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (Frankfurt am Main) <i>gegr. 1893 [VDE]</i>	 Deutsches Institut für Normung e.V. (Berlin) <i>gegr. 1917</i>

Die DKE ist das deutsche Mitglied in IEC und CENELEC, das DIN ist das deutsche Mitglied in ISO und CEN.

Die DKE ist Normenausschuss des DIN für die von ihr bearbeiteten Gebiete und somit für die nationalen DIN-Normen, die europäische und internationale deutsche Interessenvertretung in ihrem Sektor sowie deren Umsetzung als Deutsche Normen verantwortlich.

Organisatorisch ist sie Teil des VDE.

IEC und ISO haben eine gemeinsame Geschäftsordnung. Lediglich in Ausführungsdetails bestehen Unterschiede aufgrund der unterschiedlichen internationalen Orientierung je nach Fachgebiet. Sie konkurrieren nicht, sondern ergänzen sich gegenseitig und decken zusammen mit ITU das komplette Spektrum der Internationalen Normung ab.

Entsprechendes gilt für CENELEC und CEN auf europäischer Ebene.

Ergänzende Kooperationsvereinbarungen bestehen zwischen IEC und CENELEC: z. B. die parallele Abstimmung zu IEC-Entwürfen, welche bei Einbeziehung in ein paralleles Verfahren zugleich als Europäische Entwürfe (prEN) angesehen werden ohne dass ein separates europäisches Dokument erstellt und verteilt wird. Ein ähnliches Kooperationsabkommen besteht auch zwischen ISO und CEN.