

	DIN EN 61508-5 (VDE 0803-5)	DIN
	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.	VDE
ICS 35.240.50 Ersatz für DIN EN 61508-5 (VDE 0803-5):2002-11 Siehe Anwendungsbeginn Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level) (IEC 61508-5:2010); Deutsche Fassung EN 61508-5:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels (IEC 61508-5:2010); German version EN 61508-5:2010 Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 5: Exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité (CEI 61508-5:2010); Version allemande EN 61508-5:2010 Gesamtumfang 55 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2010-05-01 angenommene Europäische Norm als DIN-Norm ist 2011-02-01.

Daneben darf DIN EN 61508-5 (VDE 0803-5):2002-11 noch bis 2013-05-01 angewendet werden.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 61508-5 (VDE 0803-5):2009-06.

Für diese Norm ist das nationale Arbeitsgremium GK 914 „Funktionale Sicherheit elektrischer, elektronischer und programmierbarer elektronischer Systeme (E, E, PES) zum Schutz von Personen und Umwelt“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (www.dke.de) zuständig.

Die enthaltene IEC-Publikation wurde vom SC 65A „System aspects“ erarbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zu dem Datum (maintenance result date) unverändert bleiben soll, das auf der IEC-Website unter „<http://webstore.iec.ch>“ zu dieser Publikation angegeben ist. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees die Publikation

- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

Änderungen

Gegenüber DIN EN 61508-5 (VDE 0803-5):2002-11 wurden folgende Änderungen vorgenommen:

- a) vertiefte Diskussion der Risiken in Anhang A;
- b) Hinzufügung eines neuen Anhanges B zur Auswahl der Methoden zur Bestimmung der Sicherheits-Integritätslevel;
- c) Aufnahme der Beschreibung der Methode der Analyse der Schutzebenen (LOPA).

Frühere Ausgaben

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

Nationaler Anhang NA (informativ)

Zusammenhang mit Europäischen und Internationalen Normen

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf eine Norm ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnichtsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils neueste gültige Ausgabe der in Bezug genommenen Norm.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe der Norm.

Eine Information über den Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ist in Tabelle NA.1 wiedergegeben.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
EN 60601 (alle Teile)	IEC 60601 (alle Teile)	DIN EN 60601 (VDE 0750-1) (alle Teile)	VDE 0750-1
EN 61508-1:2010	IEC 61508-1:2010	DIN EN 61508-1 (VDE 0803-1):2011-02	VDE 0803-1
EN 61508-2:2010	IEC 61508-2:2010	DIN EN 61508-2 (VDE 0803-2):2011-02	VDE 0803-2
EN 61508-3:2010	IEC 61508-3:2010	DIN EN 61508-3 (VDE 0803-3):2011-02	VDE 0803-3
EN 61508-4:2010	IEC 61508-4:2010	DIN EN 61508-4 (VDE 0803-4):2011-02	VDE 0803-4
EN 61508-6:2010	IEC 61508-6:2010	DIN EN 61508-6 (VDE 0803-6):2011-02	VDE 0803-6
EN 61508-7:2010	IEC 61508-7:2010	DIN EN 61508-7 (VDE 0803-7):2011-02	VDE 0803-7
EN 61511 (alle Teile)	IEC 61511 (alle Teile)	DIN EN 61511 (VDE 0810-1) (alle Teile)	VDE 0810-1
EN 61800-5-2	IEC 61800-5-2	DIN EN 61800-5-2 (VDE 0160-105-2)	VDE 0160-105-2
EN 62061	IEC 62061	DIN EN 62061 (VDE 0113-50)	VDE 0113-50
EN ISO 10418:2003	ISO 10418:2003	DIN EN ISO 10418:2005-07	–
EN ISO 13849-1 :2008	ISO 13849-1:2006	DIN EN ISO 13849-1:2008-12	–
EN 31010:2010	IEC/ISO 31010	DIN EN 31010 (VDE 0050-1)	VDE 0050-1
–	ISO/TR 14121-2	–	–
–	ANSI/ISA S84:1996	–	–

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN 60601 (VDE 0750-1) (alle Teile), *Klassifikation und Kennzeichnung von Dokumenten für Anlagen, Systeme und Ausrüstungen*

DIN EN 61508-1 (VDE 0803-1):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Allgemeine Anforderungen (IEC 61508-1:2010); Deutsche Fassung EN 61508-1:2010*

DIN EN 61508-2 (VDE 0803-2):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (IEC 61508-2:2010); Deutsche Fassung EN 61508-2:2010*

DIN EN 61508-5 (VDE 0803-5):2011-02

DIN EN 61508-3 (VDE 0803-3):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software* (IEC 61508-3:2010); Deutsche Fassung EN 61508-3:2010

DIN EN 61508-4 (VDE 0803-4):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen* (IEC 61508-4:2010); Deutsche Fassung EN 61508-4:2010

DIN EN 61508-6 (VDE 0803-6):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3* (IEC 61508-6:2010); Deutsche Fassung EN 61508-6:2010

DIN EN 61508-7 (VDE 0803-7):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 7: Überblick über Verfahren und Maßnahmen* (IEC 61508-7:2010); Deutsche Fassung EN 61508-7:2010

DIN EN 61511 (VDE 0810-1) (alle Teile), *Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie*

DIN EN 61800-5-2 (VDE 0160-105-2), *Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit*

DIN EN 62061 (VDE 0113-50), *Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme*

DIN EN ISO 10418:2005-07, *Erdöl- und Erdgasindustrie – Offshore Produktionsanlagen – Analyse, Auslegung, Installation und Prüfung von grundlegenden Sicherheitssystemen von Verfahren oberhalb der Wasseroberfläche* (ISO 10418:2003); Englische Fassung EN ISO 10418:2003

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

DIN EN 31010 (VDE 0050-1), *Risikomanagement – Verfahren zur Risikobeurteilung*

Funktionale Sicherheit sicherheitsbezogener
elektrischer/elektronischer/programmierbarer elektronischer Systeme –
Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety
integrity level)
(IEC 61508-5:2010)

Functional safety of
electrical/electronic/programmable electronic
safety-related systems –
Part 5: Examples of methods for the
determination of safety integrity levels
(IEC 61508-5:2010)

Sécurité fonctionnelle des systèmes
électriques/électroniques/électroniques
programmables relatifs à la sécurité –
Partie 5: Exemples de méthodes pour la
détermination des niveaux d'intégrité de
sécurité
(CEI 61508-5:2010)

Diese Europäische Norm wurde von CENELEC am 2010-05-01 angenommen. Die CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Zentralsekretariat oder bei jedem CENELEC-Mitglied auf Anfrage erhältlich.

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

CENELEC-Mitglieder sind die nationalen elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, Ungarn, dem Vereinigten Königreich und Zypern.

CENELEC

Europäisches Komitee für Elektrotechnische Normung
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique

Zentralsekretariat: Avenue Marnix 17, B-1000 Brüssel

© 2010 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN 61508-5:2010 D

Vorwort

Der Text des Schriftstücks 65A/552/FDIS, zukünftige 2. Ausgabe von IEC 61508-5, ausgearbeitet von dem SC 65A „System aspects“ des IEC/TC 65 „Industrial-process measurement, control and automation“, wurde der IEC-CENELEC Parallelen Abstimmung unterworfen und von CENELEC am 2010-05-01 als EN 61508-5 angenommen.

Diese Europäische Norm ersetzt EN 61508-5:2001.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN und CENELEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem die EN auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2011-02-01
- spätestes Datum, zu dem nationale Normen, die der EN entgegenstehen, zurückgezogen werden müssen (dow): 2013-05-01

Der Anhang ZA wurde von CENELEC hinzugefügt.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 61508-5:2010 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

In der offiziellen Fassung sind unter „Literaturhinweise“ zu den aufgelisteten Normen die nachstehenden Anmerkungen einzutragen:

[1] IEC 61511 Reihe	ANMERKUNG	Harmonisiert in der Reihe EN 61511 (nicht modifiziert).
[2] IEC 62061	ANMERKUNG	Harmonisiert als EN 62061.
[3] IEC 61800-5-2	ANMERKUNG	Harmonisiert als EN 61800-5-2.
[9] ISO/IEC 31010	ANMERKUNG	Harmonisiert als EN 31010.
[10] ISO 10418:2003	ANMERKUNG	Harmonisiert als EN 10418:2003 (nicht modifiziert).
[12] ISO 13849-1:2006	ANMERKUNG	Harmonisiert als EN ISO 13849-1:2006 (nicht modifiziert).
[13] IEC 60601 Reihe	ANMERKUNG	Harmonisiert in der Reihe EN 60601 (teilweise modifiziert).
[14] IEC 61508-2	ANMERKUNG	Harmonisiert als EN 61508-2.
[15] IEC 61508-3	ANMERKUNG	Harmonisiert als EN 61508-3.
[16] IEC 61508-6	ANMERKUNG	Harmonisiert als EN 61508-6.
[17] IEC 61508-7	ANMERKUNG	Harmonisiert als EN 61508-7.
[18] IEC 61511-1	ANMERKUNG	Harmonisiert als EN 61511-1.

Inhalt

	Seite
Vorwort.....	2
Einleitung	6
1 Anwendungsbereich	8
2 Normative Verweisungen	10
3 Begriffe und Abkürzungen	10
Anhang A (informativ) Risiko und Sicherheitsintegrität – Allgemeine Konzepte	11
A.1 Allgemeines	11
A.2 Notwendige Risikominderung.....	11
A.2.1 Individuelles Risiko	12
A.2.2 Gesellschaftliche Risiken.....	12
A.2.3 Kontinuierliche Verbesserung.....	12
A.2.4 Risikoprofil	13
A.3 Die Rolle der sicherheitsbezogenen E/E/PE-Systeme.....	13
A.4 Sicherheitsintegrität	13
A.5 Betriebsarten und Bestimmung des SIL.....	14
A.5.1 Sicherheitsintegrität und Risikominderung für Anwendungen mit niedriger Anforderungsrate.....	14
A.5.2 Sicherheitsintegrität für Anwendungen in der Betriebsart mit hoher Anforderungsrate	16
A.5.3 Sicherheitsintegrität für Anwendungen in der Betriebsart mit kontinuierlicher Anforderung	17
A.5.4 Ausfälle infolge gemeinsamer und abhängiger Ursache.....	18
A.5.5 Sicherheits-Integritätslevel bei Verwendung mehrerer Schutzebenen	20
A.6 Risiko und Sicherheitsintegrität	20
A.7 Sicherheits-Integritätslevel und systematische Eignung	20
A.8 Zuordnung von Sicherheitsanforderungen	21
A.9 Systeme zur Schadensbegrenzung	21
Anhang B (informativ) Auswahl von Methoden zur Bestimmung der Anforderungen an den Sicherheits-Integritätslevel	23
B.1 Allgemeines	23
B.2 Die ALARP-Methode	23
B.3 Quantitative Methode der SIL-Bestimmung	24
B.4 Die Risikograph-Methode	24
B.5 Analyse der Schutzebenen (en: Layer of Protection Analysis (LOPA))	25
B.6 Matrix des Ausmaßes des gefährlichen Vorfalls	25
Anhang C (informativ) Konzepte für ALARP und tolerierbares Risiko	26
C.1 Allgemeines	26
C.2 ALARP-Modell	26
C.2.1 Einleitung	26
C.2.2 Grenzwert für das tolerierbare Risiko	27

	Seite
Anhang D (informativ) Festlegung der Sicherheits-Integritätslevel – Eine quantitative Methode.....	29
D.1 Allgemeines	29
D.2 Allgemeine Methode	29
D.3 Beispielrechnung	30
Anhang E (informativ) Bestimmung der Sicherheits-Integritätslevel – Risikograph-Methoden	32
E.1 Allgemeines	32
E.2 Aufbau des Risikographen.....	32
E.3 Kalibrierung.....	33
E.4 Mögliche andere Risikoparameter	34
E.5 Anwendung des Risikographen – Allgemeines Schema	34
E.6 Beispiel eines Risikographen.....	35
Anhang F (informativ) Semi-quantitative Methode, die eine Analyse der Schutzebenen (LOPA) verwendet	40
F.1 Allgemeines	40
F.1.1 Beschreibung	40
F.1.2 Hinweise	40
F.1.3 Beschreibung der Methode.....	40
F.2 Schadensereignis	40
F.3 Schweregrad.....	40
F.4 Auslösende Ursache.....	41
F.5 Eintrittswahrscheinlichkeit.....	41
F.6 Schutzebenen (PLs)	44
F.6.1 Allgemeines	44
F.6.2 Leit- oder Steuerungssystem.....	44
F.6.3 Alarme.....	44
F.7 und F.8 Zusätzliche Schadensbegrenzungsmaßnahmen	45
F.9 Vorläufige Wahrscheinlichkeit für das Ereignis	45
F.10 Sicherheits-Integritätslevel (SILs)	45
F.11 Tolerierbare Wahrscheinlichkeit des Ereignisses mit Schadensbegrenzung.....	46
Anhang G (informativ) Festlegung der Sicherheits-Integritätslevel – Eine qualitative Vorgehensweise – Matrix des Ausmaßes des gefährlichen Vorfalles.....	47
G.1 Allgemeines	47
G.2 Matrix des Ausmaßes des gefährlichen Vorfalles	47
Literaturhinweise	49
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen.....	51
 Bilder	
Bild 1 – Gesamtrahmen der Normenreihe IEC 61508	9
Bild A.1 – Risikominderung – Allgemeine Konzepte (Betriebsart mit niedriger Anforderungsrate).....	15
Bild A.2 – Risiko- und Sicherheitsintegritätskonzept.....	15

Bild A.3 – Risikodarstellung zu Anwendungen in der Betriebsart mit hoher Anforderungsrate 17

Bild A.4 – Risikodarstellung zu Anwendungen in der Betriebsart mit kontinuierlichen Anforderung 18

Bild A.5 – Darstellung von Ausfällen infolge gemeinsamer Ursache (CCFs) von Elementen im EUC-Leit- oder Steuerungssystem und Elementen im sicherheitsbezogenen E/E/PE-System 19

Bild A.6 – Gemeinsame Ursache zwischen zwei sicherheitsbezogenen E/E/PE-Systemen 19

Bild A.7 – Zuordnung der Sicherheitsanforderungen an die sicherheitsbezogenen E/E/PE-Systeme und andere Maßnahmen zur Risikominderung 21

Bild C.1 – Tolerierbares Risiko und ALARP 27

Bild D.1 – Zuordnung der Sicherheitsintegrität – Beispiel für eine sicherheitsbezogene Schutzeinrichtung 31

Bild E.1 – Risikograph: Allgemeine Darstellung 35

Bild E.2 – Risikograph – Beispiel (zeigt nur allgemeine Prinzipien) 36

Bild G.1 – Matrix des Ausmaßes des gefährlichen Vorfalls – Beispiel (stellt nur die allgemeinen Prinzipien dar)..... 48

Tabellen

Tabelle C.1 – Beispiel für die Risikoklassifizierung von Unfällen 28

Tabelle C.2 – Interpretation der Risikoklassen 28

Tabelle E.1 – Beispieldaten, die sich auf den Risikographen (Bild E.2) beziehen 37

Tabelle E.2 – Beispiel einer Kalibrierung des allgemeinen Risikographen 38

Tabelle F.1 – LOPA-Dokumentationsblatt 42

Einleitung

Systeme, die aus elektrischen und/oder elektronischen Elementen bestehen, werden seit vielen Jahren verwendet, um Sicherheitsfunktionen in den meisten Anwendungsbereichen auszuführen. Auf Rechnern basierende Systeme (allgemein ausgedrückt programmierbare elektronische Systeme) werden in allen Anwendungsbereichen benutzt, um Nichtsicherheitsfunktionen und zunehmend auch um Sicherheitsfunktionen auszuführen. Falls Rechnersystemtechnologie wirksam und sicherheitsgerichtet eingesetzt wird, ist es wichtig, dass die für die Entscheidungsfindung Verantwortlichen ausreichende Hilfestellung bezüglich der Sicherheitsaspekte erhalten, nach denen diese 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 (E/E/PE) Elementen bestehen 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 produkt- und anwendungsspezifischen internationalen Normen, die auf der Normenreihe IEC 61508 basieren, zu erleichtern.

ANMERKUNG 1 In den Literaturhinweisen sind Beispiele von produkt- und anwendungsspezifischen internationalen Normen, die auf der Normenreihe IEC 61508 basieren, enthalten (siehe Hinweise [1], [2] und [3]).

In den meisten Situationen wird Sicherheit durch eine Anzahl von Systemen 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, welche die Gesamtheit von sicherheitsbezogenen Systemen bilden. Daher kann diese Internationale Norm, obwohl sie sich mit sicherheitsbezogenen E/E/PE-Systemen beschäftigt, auch einen Rahmen bereitstellen, innerhalb dessen sicherheitsbezogene Systeme basierend auf anderen Technologien betrachtet werden können.

Es ist beachtet worden, dass eine große Vielfalt von Anwendungen in vielfältigen Anwendungsbereichen vorliegt, die sicherheitsbezogene E/E/PE-Systeme verwenden, und diese einen weiten Bereich in Bezug auf Komplexität, Gefährdungs- und Risikopotentiale abdecken. 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 produkt- und anwendungsspezifischen internationalen Normen und in Überarbeitungen der bereits bestehenden Normen ermöglicht.

Diese Internationale Norm:

- betrachtet alle relevanten Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus (zum Beispiel vom anfänglichen Konzept über Entwurf, Implementierung, Betrieb und Instandhaltung bis zur Außerbetriebnahme), wenn E/E/PE-Systeme 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 produkt- und anwendungsspezifischer Internationaler Normen, die sich mit sicherheitsbezogenen E/E/PE-Systemen befassen. Die Entwicklung produkt- und anwendungsspezifischer Internationaler Normen sollte innerhalb des Rahmens dieser 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 Anforderungen an die Sicherheit, die notwendig ist, um die erforderliche funktionale Sicherheit für sicherheitsbezogene E/E/PE-Systeme zu erreichen;
- verwendet einen auf dem Risiko basierenden Lösungsansatz, durch den die Anforderungen an die Sicherheitsintegrität bestimmt werden können;

- führt Sicherheits-Integritätslevel für die Festlegung der Zielvorgabe der Sicherheitsintegrität der Sicherheitsfunktionen ein, die von den sicherheitsbezogenen E/E/PE-Systemen zu implementieren sind;

ANMERKUNG 2 Diese Norm legt weder die Anforderungen an den Sicherheits-Integritätslevel für irgendeine Sicherheitsfunktion fest, noch bestimmt sie, wie der Sicherheits-Integritätslevel festgelegt wird. Stattdessen stellt sie einen risikobasierenden konzeptionellen Rahmen und Beispielverfahren bereit.

- legt Ausfallgrenzwerte für die von den sicherheitsbezogenen E/E/PE-Systemen auszuführenden Sicherheitsfunktionen fest, die mit den Sicherheits-Integritätsleveln verbunden sind;
- legt eine untere Grenze für die Ausfallgrenzwerte für eine Sicherheitsfunktion fest, die von einem einzelnen sicherheitsbezogenen E/E/PE-System ausgeführt wird. Für sicherheitsbezogene E/E/PE-Systeme, die:
 - in der Betriebsart mit einer niedrigen Anforderungsrate betrieben werden, ist die untere Grenze bei einer mittleren Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung von 10^{-5} festgelegt;
 - in der Betriebsart mit einer hohen Anforderungsrate oder mit kontinuierlicher Anforderung betrieben werden, ist die untere Grenze bei einer mittleren Häufigkeit eines gefahrbringenden Ausfalls von $10^{-9} [h^{-1}]$ festgelegt;

ANMERKUNG 3 Ein einzelnes sicherheitsbezogenes E/E/PE-System bedeutet nicht notwendigerweise eine einkanalige Architektur.

ANMERKUNG 4 Es kann für einfache Systeme möglich sein, Entwürfe von sicherheitsbezogenen Systemen mit niedrigeren Zielwerten für die Sicherheitsintegrität zu erreichen, aber diese Grenzen werden als das betrachtet, was für relativ komplexe Systeme (zum Beispiel sicherheitsbezogene programmierbare elektronische Systeme) gegenwärtig erreicht werden kann.

- legt Anforderungen für die Vermeidung und Beherrschung von systematischen Fehlern fest, die auf Erfahrungen und Urteilsvermögen beruhen, die durch praktische Erfahrung in der Industrie gewonnen wurden. Wenn auch die Wahrscheinlichkeit des Auftretens systematischer Ausfälle im Allgemeinen nicht quantifiziert werden kann, erlaubt die Norm jedoch für eine festgelegte Sicherheitsfunktion den Anspruch zu erheben, dass der mit der Sicherheitsfunktion verbundene Ausfallgrenzwert als erreicht betrachtet werden kann, wenn alle Anforderungen dieser Norm erfüllt worden sind;
- führt die systematische Eignung ein, die für ein Element im Hinblick auf das Vertrauen gilt, dass die systematische Sicherheitsintegrität die Anforderungen des festgelegten Sicherheits-Integritätslevels erfüllt;
- lässt einen weiten Bereich von Prinzipien, Verfahren und Maßnahmen zu, um funktionale Sicherheit für sicherheitsbezogene E/E/PE-Systeme zu erreichen, verwendet aber nicht ausdrücklich das Fail-Safe-Konzept. „Fail-Safe“-Konzepte und „inhärent sichere“ Prinzipien können jedoch anwendbar sein, und der Einsatz solcher Konzepte ist zulässig, vorausgesetzt, dass die Anforderungen der zutreffenden Abschnitte in der Norm erfüllt werden.

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level)

1 Anwendungsbereich

1.1 Dieser Teil der IEC 61508 liefert Informationen über

- die zugrunde liegenden Konzepte des Risikos und den Zusammenhang zwischen Risiko und Sicherheitsintegrität (siehe [Anhang A](#));
- eine Anzahl von Methoden, die es ermöglichen, den Sicherheits-Integritätslevel für die sicherheitsbezogenen E/E/PE-System festzulegen (siehe [Anhänge C, D, E, F und G](#)).

Die ausgewählte Methode hängt vom Anwendungsgebiet und den betrachteten besonderen Umständen ab. Die [Anhänge C, D, E, F und G](#) erläutern quantitative und qualitative Verfahren und wurden vereinfacht, um die zugrunde gelegten Prinzipien zu erläutern. Diese Anhänge wurden aufgenommen, um die allgemeinen Prinzipien einer Anzahl von Methoden aufzuzeigen, aber sie liefern keine endgültige Darstellung. Diejenigen, die die Anwendung der in den Anhängen aufgeführten Methoden beabsichtigen, sollten das angegebene Quellenmaterial zu Rate ziehen.

ANMERKUNG Für weitere Informationen bezüglich der in den [Anhängen B und E](#) dargestellten Vorgehensweisen siehe die Verweise [\[5\]](#) und [\[8\]](#) in den Literaturhinweisen. Siehe ebenfalls den Verweis [\[6\]](#) in den Literaturhinweisen zur Beschreibung einer zusätzlichen Vorgehensweise.

1.2 IEC 61508-1, IEC 61508-2, IEC 61508-3 und IEC 61508-4 sind Sicherheitsgrundnormen, dieser Status ist aber im Zusammenhang mit einfachen sicherheitsbezogenen E/E/PE-Systemen nicht anwendbar (siehe IEC 61508-4, 3.4.3). Als Sicherheitsgrundnormen sind sie zur Verwendung durch technische Komitees bei der Erstellung von Normen entsprechend den in IEC Guide 104 und ISO/IEC Guide 51 enthaltenen Grundsätzen vorgesehen. IEC 61508-1, IEC 61508-2, IEC 61508-3 und IEC 61508-4 sind ebenfalls zur Verwendung als eigenständige Veröffentlichungen vorgesehen. Die horizontale Sicherheitsfunktion dieser Internationalen Norm trifft nicht auf Medizingeräte in Übereinstimmung mit der Normenreihe IEC 60601 zu.

1.3 Es steht in der Verantwortung eines Technischen Komitees, zur Vorbereitung und Erstellung eigener Veröffentlichungen soweit möglich die Sicherheitsgrundnormen anzuwenden. In diesem Zusammenhang gilt, dass die Anforderungen, Prüfverfahren oder Prüfbedingungen dieser Sicherheitsgrundnorm nicht anzuwenden sind, außer in den Veröffentlichungen der Technischen Komitees wird speziell darauf verwiesen oder sie werden eingebunden.

1.4 [Bild 1](#) zeigt den gesamten Rahmen der Reihe IEC 61508 und zeigt die Rolle, die die IEC 61508-5 zum Erreichen der funktionalen Sicherheit der sicherheitsbezogenen E/E/PE-Systeme spielt.

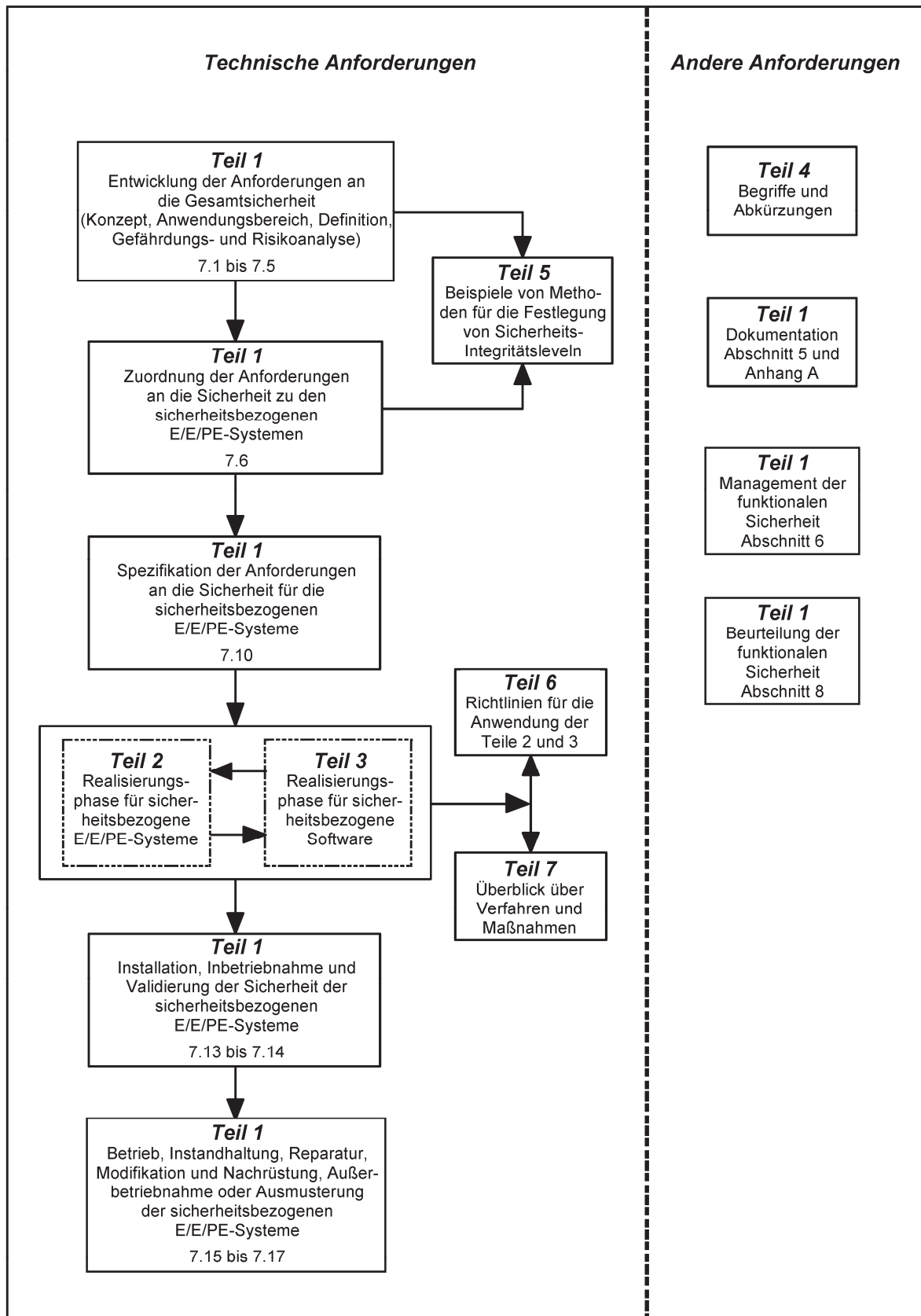


Bild 1 – Gesamtrahmen der Normenreihe IEC 61508

2 Normative Verweisungen

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

IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations of terms*

3 Begriffe und Abkürzungen

Für die Anwendung dieses Dokumentes gelten die in der IEC 61508-4 aufgeführten Begriffe und Abkürzungen.

Anhang A (informativ)

Risiko und Sicherheitsintegrität – Allgemeine Konzepte

A.1 Allgemeines

Dieser Anhang liefert Informationen über die zugrunde liegenden Konzepte des Risikos und den Zusammenhang zwischen Risiko und Sicherheitsintegrität.

A.2 Notwendige Risikominderung

Die notwendige Risikominderung (siehe IEC 61508-4, 3.5.18) ist die Minderung des Risikos, die erreicht werden muss, um das tolerierbare Risiko für eine bestimmte Situation zu erreichen (welches entweder qualitativ ¹⁾ oder quantitativ ²⁾ angegeben werden darf). Das Konzept der notwendigen Risikominderung ist für die Entwicklung der Spezifikation der Sicherheitsanforderungen für die sicherheitsbezogenen E/E/PE-Systeme von grundlegender Bedeutung (insbesondere der Teil der Anforderungen zur Sicherheitsintegrität in der Spezifikation der Anforderungen an die Sicherheit). Der Zweck der Festlegung des tolerierbaren Risikos für einen bestimmten gefährlichen Vorfall ist es, darzulegen, was im Hinblick sowohl auf die Häufigkeit (oder Wahrscheinlichkeit) des gefährlichen Vorfalls als auch auf seine besonderen Auswirkungen für annehmbar gehalten wird. Sicherheitsbezogene Systeme werden entworfen, um die Häufigkeit (oder Wahrscheinlichkeit) des gefährlichen Vorfalls und/oder die Auswirkungen des gefährlichen Vorfalls zu mindern.

Das tolerierbare Risiko hängt von vielen Faktoren ab (zum Beispiel der Schwere der Verletzung, der Anzahl der Personen, die einer Gefahr ausgesetzt sind, der Häufigkeit, mit der eine Person oder Personen einer Gefahr ausgesetzt sind, und der Dauer der Einwirkung). Wichtige Faktoren werden die Wahrnehmung und die Ansichten derjenigen sein, die dem gefährlichen Vorfall ausgesetzt sind. Zur Festlegung des tolerierbaren Risikos einer bestimmten Anwendung werden die folgenden Punkte betrachtet:

- gesetzliche Anforderungen, sowohl allgemeine als auch diejenigen, die sich direkt auf die spezifische Anwendung beziehen;
- Leitfäden der entsprechenden Behörden, die Sicherheitsregeln erstellen;
- Diskussionen und Übereinkünfte mit den verschiedenen Parteien, die an der Anwendung beteiligt sind;
- Industrienormen und -leitfäden;
- internationale Diskussionen und Übereinkünfte; die Rolle nationaler und internationaler Normen gewinnt zunehmend an Wichtigkeit, um die Kriterien für das tolerierbare Risiko bei bestimmten Anwendungen festzulegen;
- die bestmögliche, unabhängige, industrielle, expertengestützte und wissenschaftliche Unterstützung durch Beratungsinstitutionen.

Bei der Bestimmung der Anforderungen zur Sicherheitsintegrität der sicherheitsbezogenen E/E/PE-Systeme und anderer risikomindernder Maßnahmen sind im Hinblick auf die Erreichung der tolerierbaren Häufigkeit eines gefährlichen Vorfalls die Merkmale der Gefahr der einschlägigen Anwendung zu berücksichtigen. Die tolerierbare Häufigkeit wird von den rechtlichen Anforderungen in dem Land der Anwendung und von den durch Anwender-Organisationen spezifizierten Kriterien abhängen. Fragen, die berücksichtigt werden müssen, werden im Folgenden erörtert und auch, wie sie auf die sicherheitsbezogenen E/E/PE-Systeme anzuwenden sind.

¹⁾ Um das tolerierbare Risiko zu erreichen, ist es erforderlich, die notwendige Risikominderung festzusetzen. Die [Anhänge E](#) und [G](#) dieses Dokuments skizzieren qualitative Methoden. In den Beispielen ist die notwendige Risikominderung durch die Angabe der SIL-Anforderung ausgedrückt und nicht durch einen numerischen Wert.

²⁾ Zum Beispiel, dass der gefährliche Vorfall, der zu einer bestimmten Auswirkung führt, nicht mit einer Häufigkeit von mehr als einmal in 10⁸ Stunden auftreten darf.

A.2.1 Individuelles Risiko

Es werden in der Regel verschiedene Ziele für Beschäftigte und Privatpersonen definiert. Die Zielvorgabe für das individuelle Risiko für die Beschäftigten bezieht sich auf die am höchsten gefährdete Person und kann ausgedrückt werden als das gesamte Risiko je Jahr, das aus allen Tätigkeiten erwächst. Das Ziel ist auf eine hypothetische Person ausgelegt und muss daher den Anteil der Zeit berücksichtigen, den die einzelne Person bei der Arbeit verbringt. Dieses Ziel gilt für alle Risiken der gefährdeten Person und das tolerierbare Risiko für eine einzelne Sicherheitsfunktion muss andere Risiken mit berücksichtigen.

Vertrauen, dass das gesamte Risiko unter ein bestimmtes Ziel reduziert wurde, kann durch eine Reihe von Möglichkeiten erreicht werden. Eine Methode besteht darin, alle Risiken in Betracht zu ziehen und deren Summe für die am stärksten exponierte Person zu bilden. Dies kann beispielsweise in Fällen, in denen eine Person vielen Risiken ausgesetzt und eine frühzeitige Entscheidungen für die Systementwicklung notwendig ist, schwierig werden. Ein alternativer Ansatz besteht darin, einen bestimmten Prozentsatz des gesamten individuellen Ziel-Risikos jeder einzelnen betrachteten Sicherheitsfunktion zuzuordnen. Der zugeordnete Anteil kann in der Regel aus früheren Erfahrungen mit der Art der betrachteten Anlage bestimmt werden.

Das Ziel für eine individuelle Sicherheitsfunktion sollte auch den Konservatismus der verwendeten Methode der Risikoanalyse berücksichtigen. Alle qualitativen Methoden, wie Risikographen, beinhalten einige Bewertungen kritischer Parameter, die zu einem Risiko beitragen. Faktoren, die zu Risiken beitragen, sind die Auswirkung des gefährlichen Vorfalls und seine Häufigkeit. Bei der Festlegung dieser Faktoren kann es nötig sein, eine Reihe von Risikoparametern zu berücksichtigen, wie eine Anfälligkeit für einen gefährlichen Vorfall, die Anzahl der Personen, die möglicherweise durch den gefährlichen Vorfall betroffen sind, die Wahrscheinlichkeit, dass eine Person anwesend ist, wenn der gefährliche Vorfall eintritt (d. h. Aufenthaltsdauer), und die Wahrscheinlichkeit der Vermeidung des gefährlichen Vorfalls.

Qualitative Methoden beinhalten allgemein die Entscheidung, ob ein Parameter sich innerhalb einer bestimmten Bandbreite bewegt. Die Beschreibungen der Kriterien bei der Verwendung dieser Methoden müssen so sein, dass ein hohes Maß an Vertrauen vorliegt, dass das Ziel für die Risiken nicht überschritten wird. Dies kann einen Einstellbereich für Grenzen aller Parameter beinhalten, so dass Anwendungen, deren Parameter die Grenzbedingung einhalten, die spezifizierten Risikokriterien für die Sicherheit erfüllen. Dieses Konzept zur Festlegung der Grenzbereiche ist sehr konservativ, denn es werden nur sehr wenige Anwendungen existieren, bei denen alle Parameter im Worst-Case-Bereich liegen. Wenn Privatpersonen einem Risiko des Ausfalls eines sicherheitsbezogenen E/E/PE-Systems ausgesetzt sind, dann kommt in der Regel ein niedrigeres Ziel zur Anwendung.

A.2.2 Gesellschaftliche Risiken

Diese entstehen, wenn mehrere Todesfälle durch einzelne Vorfälle zu erwarten sind. Solche Vorfälle werden gesellschaftlich genannt, weil sie geeignet sind, eine sozialpolitische Reaktion auszulösen. Es kann bedeutende öffentliche und organisatorische Abneigung gegen die hohe Auswirkung dieses Vorfalls geben und dies muss in einigen Fällen berücksichtigt werden. Das Kriterium für ein gesellschaftliches Risiko wird oft als eine maximale kumulierte Häufigkeit für tödliche Verletzungen einer bestimmten Anzahl von Personen ausgedrückt. Das Kriterium wird in der Regel in Form einer oder mehrerer Linien auf einem F/N-Diagramm dargestellt, wobei F die kumulative Häufigkeit von Gefahren und N die Anzahl der Todesfälle ist, die sich aus den Gefährdungen ergeben. Die Beziehung ist in der Regel eine gerade Linie, wenn diese auf einer logarithmischen Skala gezeichnet wird. Die Steigung der Linie wird davon abhängen, in welchem Umfang Organisationen Risiken mit höheren Auswirkungen scheuen. Die Anforderung wird sein, dass die kumulierte Häufigkeit für eine bestimmte Zahl von Todesfällen niedriger ist als die kumulierte Häufigkeit in dem F/N-Diagramm (siehe Verweis [7] in den Literaturhinweisen).

A.2.3 Kontinuierliche Verbesserung

Die Grundsätze zur Verringerung des Risikos auf einen Wert so niedrig wie vernünftigerweise möglich werden im [Anhang C](#) vorgestellt.

A.2.4 Risikoprofil

Bei der Entscheidung, Risikokriterien für eine bestimmte Gefährdung anzuwenden, kann es notwendig werden, ein Risikoprofil über die gesamte Laufzeit der Anlage in Betracht zu ziehen. Das Restrisiko wird von niedrig, nach einer Wiederholungsprüfung oder nach Durchführung einer Reparatur, bis zu einem Maximum, kurz vor einer Wiederholungsprüfung, variieren. Dies sollte unter Umständen von Organisationen in Betracht gezogen werden, die die Risikokriterien spezifizieren, die anzuwenden sind. Wenn Intervalle für Wiederholungsprüfungen von Bedeutung sind, dann kann es angemessen sein, die maximale Wahrscheinlichkeit einer Gefährdung, die vor einer Wiederholungsprüfung akzeptiert werden kann, zu spezifizieren. Oder die PFD(t) oder PFH(t) ist niedriger als die obere SIL-Grenze für mehr als einen bestimmten Prozentsatz der Zeit (z. B. 90 %).

A.3 Die Rolle der sicherheitsbezogenen E/E/PE-Systeme

Sicherheitsbezogene E/E/PE-Systeme tragen dazu bei, die für das Erreichen des tolerierbaren Risikos notwendige Risikominderung herbeizuführen.

Ein sicherheitsbezogenes System

- beinhaltet sowohl die geforderten Sicherheitsfunktionen, die notwendig sind, einen sicheren Zustand für die EUC-Einrichtung zu erreichen oder einen sicheren Zustand für die EUC-Einrichtung aufrechtzuerhalten; und
- ist dazu vorgesehen, selbständig oder mit anderen sicherheitsbezogenen E/E/PE-Systemen oder anderen risikomindernden Maßnahmen die notwendige Sicherheitsintegrität für die geforderten Sicherheitsfunktionen zu erreichen (IEC 61508-4, 3.5.1).

ANMERKUNG 1 Der erste Teil der Definition gibt an, dass das sicherheitsbezogene System die Sicherheitsfunktionen ausführen muss, die in der Spezifikation der Anforderungen an die Sicherheitsfunktionen festgelegt werden. Zum Beispiel könnte die Spezifikation der Anforderungen an die Sicherheitsfunktionen festlegen, dass bei Erreichen der Temperatur x das Ventil y öffnen muss, um eine Wasserzufuhr in einen Behälter zu ermöglichen.

ANMERKUNG 2 Der zweite Teil der Definition gibt an, dass das sicherheitsbezogene System die Sicherheitsfunktionen mit einem der Anwendung angemessenen Grad an Gewissheit ausführen muss, um das tolerierbare Risiko zu erreichen.

Eine Person kann ein integraler Bestandteil eines sicherheitsbezogenen E/E/PE-Systems sein. Eine Person könnte zum Beispiel von einer Anzeigetafel Informationen über den Zustand der EUC entgegennehmen und eine auf diesen Informationen beruhende sicherheitsgerichtete Handlung ausführen.

Sicherheitsbezogene E/E/PE-Systeme können in einer Betriebsart mit niedriger Anforderungsrate oder in einer Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung betrieben werden (siehe IEC 61508-4, 3.5.16).

A.4 Sicherheitsintegrität

Sicherheitsintegrität ist definiert als die „Wahrscheinlichkeit eines sicherheitsbezogenen Systems, die geforderten Sicherheitsfunktionen unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraumes zufriedenstellend auszuführen“ (IEC 61508-4, 3.5.4). Die Sicherheitsintegrität bezieht sich auf die Leistungsfähigkeit der sicherheitsbezogenen Systeme, die Sicherheitsfunktionen auszuführen (die auszuführenden Sicherheitsfunktionen sind in der Spezifikation der Anforderungen an die Sicherheitsfunktionen festgelegt).

Die Sicherheitsintegrität setzt sich aus den folgenden beiden Elementen zusammen:

- der Sicherheitsintegrität der Hardware; derjenige Teil der Sicherheitsintegrität, der sich auf zufällige Hardwareausfälle mit gefahrbringender Ausfallart bezieht (siehe IEC 61508-4, 3.5.7). Das Erreichen der festgelegten Stufe der Sicherheitsintegrität der Hardware kann mit einer vernünftigen Genauigkeit abgeschätzt werden. Die Anforderungen können daher unter Verwendung der üblichen Regeln für die Kombination von Wahrscheinlichkeiten zwischen den Teilsystemen aufgeteilt werden. Zum Erreichen einer angemessenen Sicherheitsintegrität der Hardware kann die Anwendung redundanter Architekturen notwendig sein.