DIN EN 61508-5 (VDE 0803-5)

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.

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 integrety 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

Einzelverkauf und Abonnements durch VDE VERLAG GMBH, 10625 Berlin
Einzelverkauf auch durch Beuth Verlag GmbH, 10772 Berlin

Preisgr. 32 K
VDE-Vertr.-Nr. 0803016

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 Abschnittsnummer, 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 61508-3 (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 Gestaltungsleitsätze (ISO 13849-1:2006); Deutsche Fassung EN ISO 13849-1:2008*

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

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN 61508-5

Mai 2010

ICS 35.240.50

Ersatz für EN 61508-5:2001

Deutsche Fassung

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

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

Bilder

Seite

Tabellen

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 integrety 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.

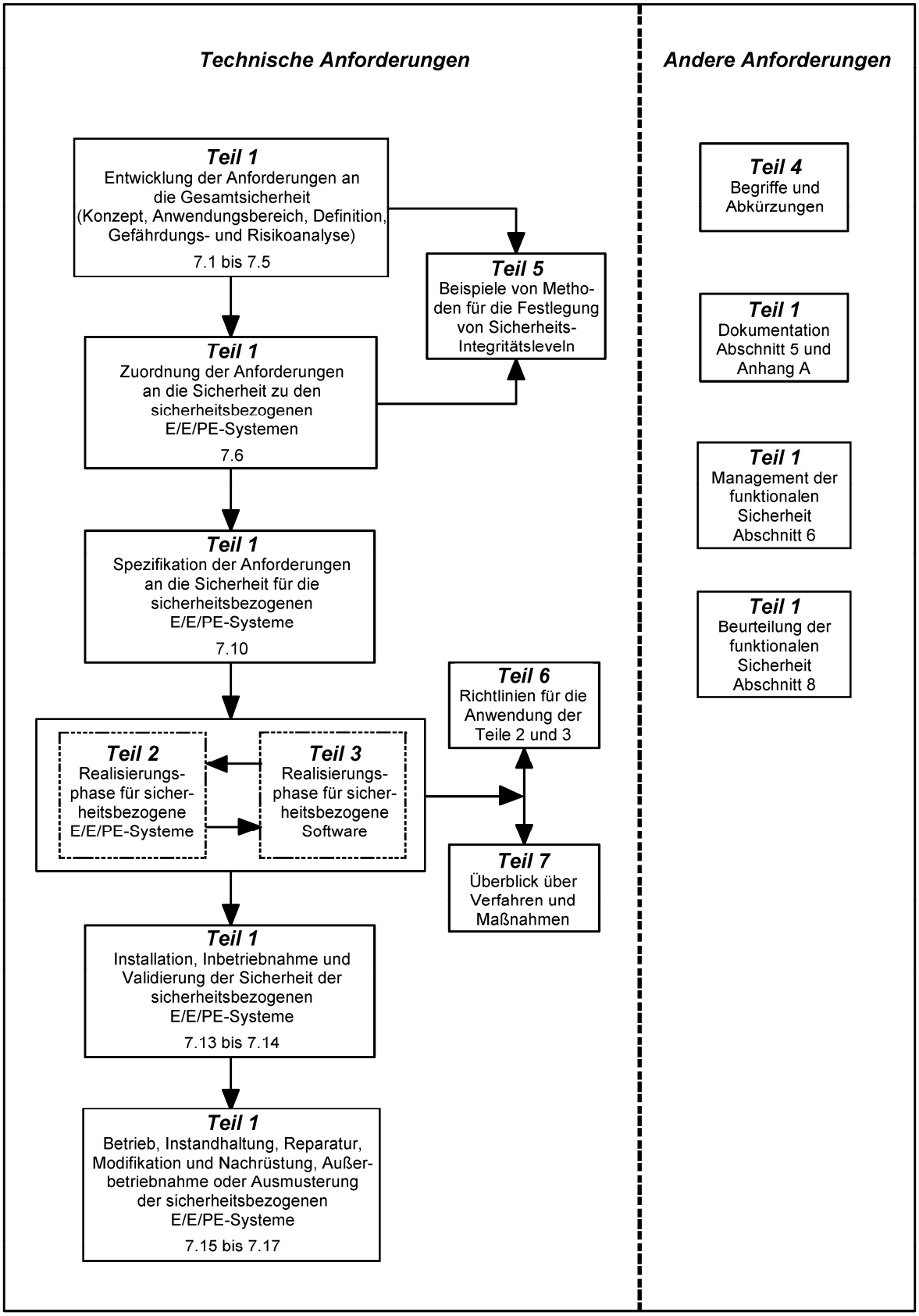


Bild 1 – Gesamtrahmen der Normenreihe IEC 61508

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 10^8 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.

– der systematische Sicherheitsintegrität: derjenige Teil der Sicherheitsintegrität, der sich auf systematische Ausfälle mit gefahrbringender Ausfallart bezieht (siehe IEC 61508-4, 3.5.6). Obwohl die mittlere Ausfallrate für systematische Ausfälle einer Abschätzung zugänglich sein kann, führen die durch Entwurfsfehler und Ausfälle infolge gemeinsamer Ursache resultierenden Ausfalldaten dazu, dass die Verteilung der Ausfälle schwer vorherzusagen ist. Dies führt zu einer zunehmenden Ungewissheit in den Berechnungen der Ausfallwahrscheinlichkeiten für eine bestimmte Situation (zum Beispiel die Ausfallwahrscheinlichkeit einer sicherheitsbezogenen Schutzeinrichtung). Daher muss eine Beurteilung der Auswahl der besten Vorgehensweisen zur Verringerung dieser Ungewissheit erfolgen. Es ist zu beachten, dass es nicht so ist, dass Maßnahmen zur Reduzierung der Wahrscheinlichkeit zufälliger Hardwareausfälle einen gleichartigen Einfluss auf die Wahrscheinlichkeit eines systematischen Ausfalls haben. Methoden, wie zum Beispiel die Verwendung redundanter Kanäle mit identischer Hardware, die sehr wirksam in der Beherrschung zufälliger Hardwareausfälle sind, haben nur einen geringen Nutzen bei der Reduzierung systematischer Ausfälle wie Softwarefehler.

A.5 Betriebsarten und Bestimmung des SIL

Die Betriebsart bezieht sich auf die Art und Weise, wie eine Sicherheitsfunktion verwendet werden soll, mit Bezug auf die Häufigkeit von Anforderungen an sie. Unterschieden wird zwischen Betriebsarten:

– **mit niedriger Anforderungsrate**: wenn die Häufigkeit von Anforderungen während des Betriebs an die Sicherheitsfunktion nicht größer als einmal je Jahr ist; oder

– **mit hoher Anforderungsrate:** wenn die Häufigkeit von Anforderungen während des Betriebs an die Sicherheitsfunktion größer als einmal je Jahr ist; oder

– **mit kontinuierlicher Anforderung:** wenn die Anforderung an die Sicherheitsfunktion kontinuierlich vorhanden ist.

Die IEC 61508-1, Tabellen 2 und 3, zeigen die Ausfallgrenzwerte für jede der Betriebsarten im Zusammenhang mit den vier Sicherheits-Integritätsleveln. Die Betriebsarten werden in den folgenden Abschnitten weiter beschrieben.

A.5.1 Sicherheitsintegrität und Risikominderung für Anwendungen mit niedriger Anforderungsrate

Die erforderliche Sicherheitsintegrität der sicherheitsbezogenen E/E/PE-Systeme und anderen risikomindernden Maßnahmen muss auf einer solchen Stufe sein, dass sichergestellt ist, dass:

– die durchschnittliche Ausfallwahrscheinlichkeit bei Anforderung der sicherheitsbezogenen Systeme ausreichend niedrig ist, um zu verhindern, dass die Häufigkeit des gefährlichen Vorfalls die zum Erreichen des tolerierbaren Risikos geforderte Häufigkeit überschreitet; und/oder

– die sicherheitsbezogenen Systeme die Auswirkungen eines Ausfalls in dem erforderlichen Ausmaß verändern, um das tolerierbare Risiko zu erreichen.

Bild A.1 zeigt die allgemeinen Konzepte der Risikominderung. Im allgemeinen Modell ist angenommen, dass:

– eine EUC und ein Steuerungssystem vorhanden ist;

– zugehörige menschliche Faktoren vorhanden sind;

– die sicherheitsbezogenen Schutzmaßnahmen Folgendes umfassen:
  – sicherheitsbezogene E/E/PE-Systeme;
  – andere risikomindernde Maßnahmen.

ANMERKUNG Bild A.1 ist ein verallgemeinertes Risikomodell zur Darstellung der allgemeinen Prinzipien. Um das Risikomodell für eine bestimmte Anwendung zu entwickeln, ist es notwendig, die spezifische Art und Weise, mit der die notwendige Risikominderung durch die sicherheitsbezogenen E/E/PE-Systeme und/oder anderen risikomindernden Maßnahmen erreicht wird, zu berücksichtigen. Das daraus hervorgehende Risikomodell kann daher von dem in Bild A.1 gezeigten abweichen.

Die in Bild A.1 und A.2 gezeigten unterschiedlichen Risiken sind:

– EUC-Risiko: das Risiko, das für die festgelegten gefährlichen Vorfälle der EUC, des EUC-Leit- oder Steuerungssystems und zugehöriger menschlicher Faktoren besteht; vorgesehene sicherheitsbezogene Schutzmerkmale werden bei der Bestimmung dieses Risikos nicht berücksichtigt (siehe IEC 61508-4, 3.1.9);
– tolerierbares Risiko: das Risiko, das in einem gegebenen Zusammenhang basierend auf den üblichen gesellschaftlichen Wertvorstellungen tragbar ist (siehe IEC 61508-4, 3.1.7);
– Restrisiko: im Zusammenhang mit dieser Norm ist das Restrisiko das Risiko, das für die festgelegten gefährlichen Vorfälle der EUC, des EUC-Leit- oder Steuerungssystems und zugehöriger menschlicher Faktoren verbleibt, jedoch unter Berücksichtigung der sicherheitsbezogenen E/E/PE-Systeme und anderen risikomindernden Maßnahmen (siehe auch IEC 61508-4, 3.1.7).

Das EUC-Risiko ist eine Funktion des zur EUC selbst zugehörigen Risikos, jedoch unter Berücksichtigung der durch das EUC-Leit- oder Steuerungssystem erreichten Risikominderung. Um ungerechtfertigte Anforderungen an die Sicherheitsintegrität des EUC-Leit- oder Steuerungssystems zu verhindern, legt diese Norm Beschränkungen für die Anforderungen, die gestellt werden können, fest (siehe IEC 61508-1, 7.5.2.5).

Die notwendige Risikominderung wird durch eine Kombination aller sicherheitsbezogenen Schutzmerkmale erreicht. Die Risikominderung, die vom Ausgangspunkt des EUC-Risikos aus notwendig ist, um das tolerierbare Risiko zu erreichen, ist in Bild A.1 gezeigt (wichtig für eine Sicherheitsfunktion, die in der Betriebsart mit niedriger Anforderungsrate arbeitet).

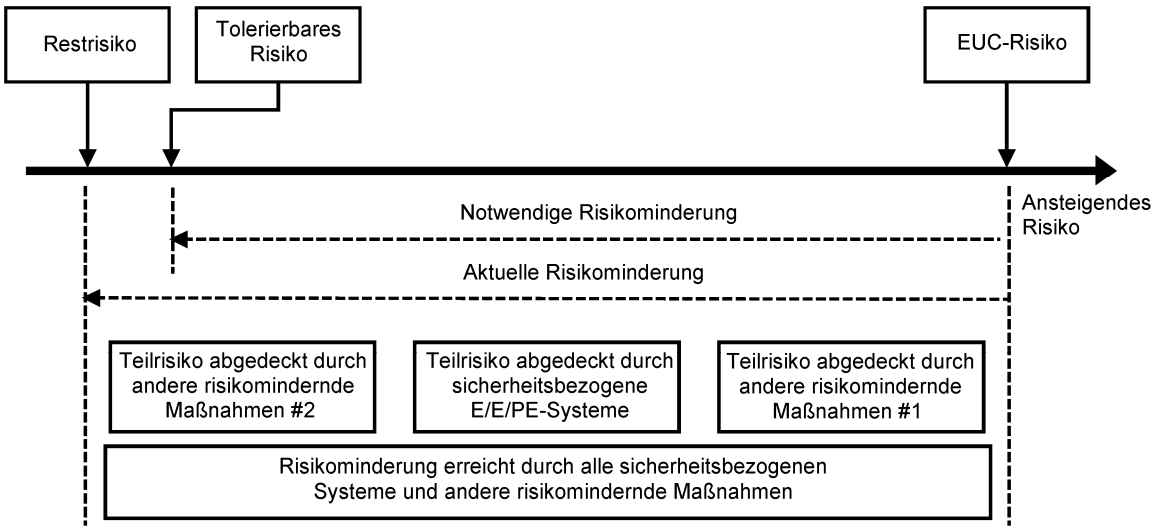


Bild A.1 – Risikominderung – Allgemeine Konzepte (Betriebsart mit niedriger Anforderungsrate)

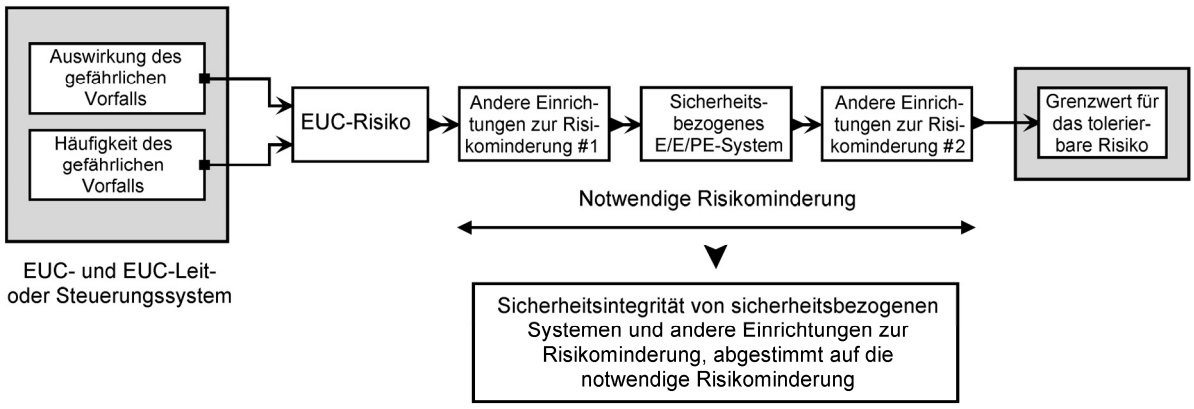


Bild A.2 – Risiko- und Sicherheitsintegritätskonzept

A.5.2 Sicherheitsintegrität für Anwendungen in der Betriebsart mit hoher Anforderungsrate

Die erforderliche Sicherheitsintegrität der sicherheitsbezogenen E/E/PE-Systeme und anderer Maßnahmen zur Risikominderung müssen von einem solchen Niveau sein, das sicherstellt, dass

– die mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung des sicherheitsbezogenen Systems niedrig genug ist, um zu verhindern, dass die Häufigkeit eines gefährlichen Vorfalls die zur Einhaltung des zulässigen Risikos geforderte überschreitet; und/oder
– die mittlere Wahrscheinlichkeit eines Ausfalls des sicherheitsbezogenen Systems je Stunde niedrig genug ist, um zu verhindern, dass die Häufigkeit eines gefährlichen Vorfalls die zur Einhaltung des zulässigen Risikos geforderte überschreitet.

Bild A.3 zeigt die allgemeinen Konzepte für Anwendungen in der Betriebsart mit hoher Anforderungsrate. Das Modell geht davon aus, dass

– eine EUC und ein Steuerungssystem vorhanden sind;
– zugehörige menschliche Faktoren vorhanden sind;
– die sicherheitsbezogenen Schutzmaßnahmen Folgendes umfassen:
  – sicherheitsbezogene E/E/PE-Systeme in einer Betriebsart mit hoher Anforderungsrate;
  – andere risikomindernde Maßnahmen.

Verschiedene Anforderungen an die sicherheitsbezogenen E/E/PE-Systeme können wie folgt auftreten:

– allgemeine Anforderungen durch das EUC;
– Anforderungen durch Ausfälle des EUC-Leit- oder Steuerungssystems;
– Anforderungen durch menschliches Versagen.

Wenn die Gesamtanforderungsrate aus allen Anforderungen an das System mehr als 1 je Jahr überschreitet, dann ist der kritische Faktor die Rate gefahrbringender Ausfälle des sicherheitsbezogen E/E/PE-Systems. Die Restfrequenz der Gefährdung kann die gefährliche Ausfallrate des sicherheitsbezogenen E/E/PE-Systems nie überschreiten. Sie kann niedriger sein, wenn andere Maßnahmen zur Risikominderung die Wahrscheinlichkeit eines Schadens reduzieren.

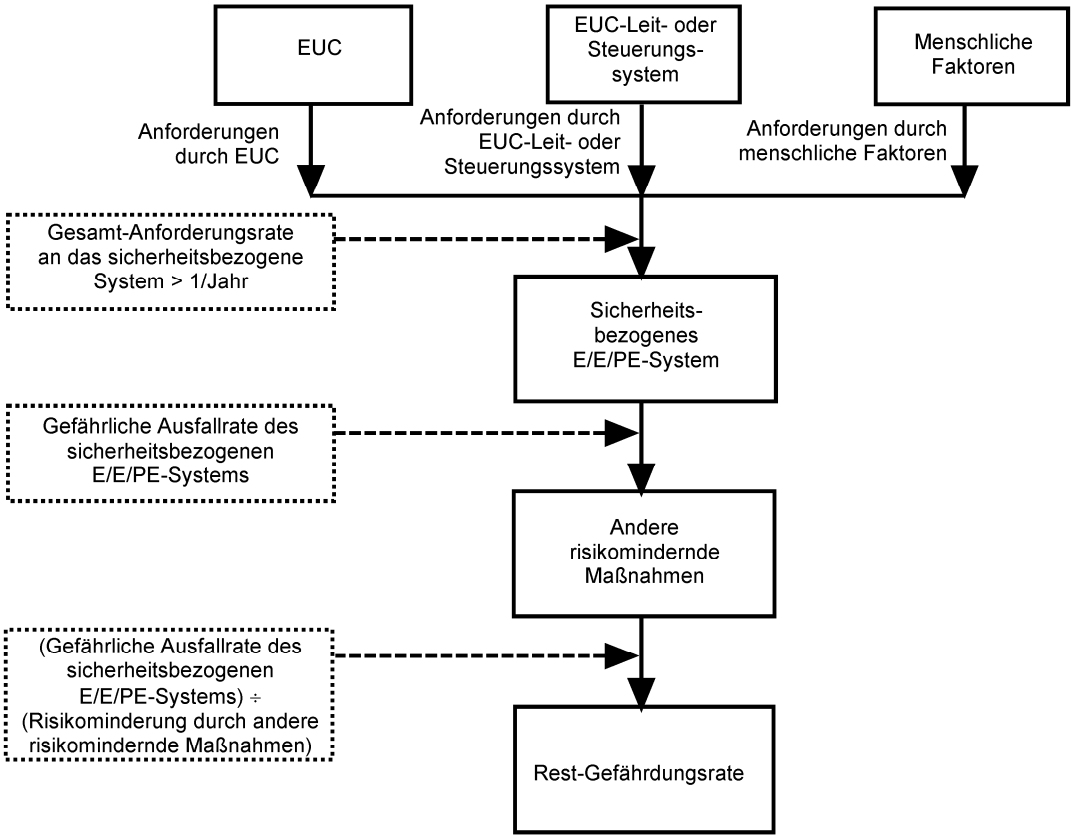


Bild A.3 – Risikodarstellung zu Anwendungen in der Betriebsart mit hoher Anforderungsrate

A.5.3 Sicherheitsintegrität für Anwendungen in der Betriebsart mit kontinuierlicher Anforderung

Die erforderliche Sicherheitsintegrität der sicherheitsbezogenen E/E/PE-Systeme und anderer Maßnahmen zur Risikominderung müssen von einem solchen Niveau sein, das sicherstellt, dass die mittlere Wahrscheinlichkeit eines Ausfalls des sicherheitsbezogenen Systems je Stunde niedrig genug ist, um zu verhindern, dass die Häufigkeit eines gefährlichen Vorfalls die zur Einhaltung des zulässigen Risikos geforderte überschreitet.

Mit einem sicherheitsbezogenen E/E/PE-System in der Betriebsart mit kontinuierlicher Anforderung können andere risikomindernde Maßnahmen die Resthäufigkeit der Gefährdung entsprechend der bereitgestellten Risikominderung mindern. Das Modell ist in Bild A.4 gezeigt.

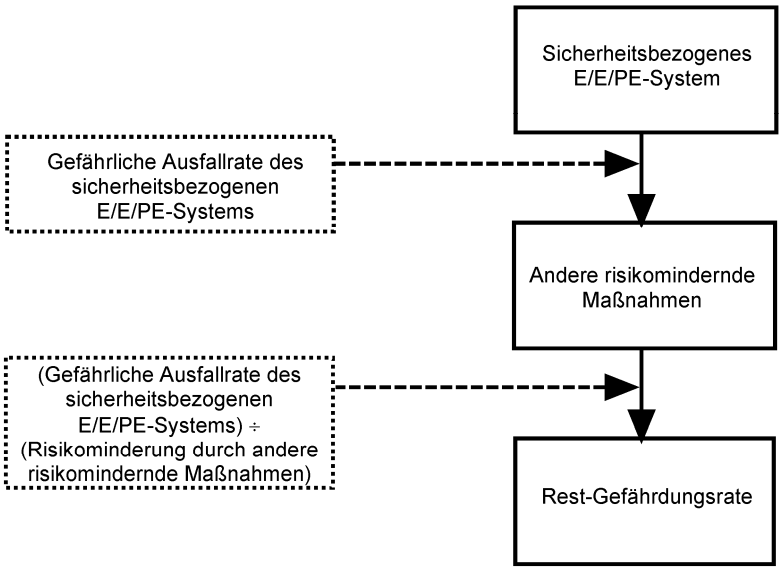


Bild A.4 – Risikodarstellung zu Anwendungen in der Betriebsart mit kontinuierlichen Anforderung

A.5.4 Ausfälle infolge gemeinsamer und abhängiger Ursache

Während der Bestimmung der Sicherheits-Integritätslevel ist es wichtig, Ausfälle infolge gemeinsamer und abhängiger Ursachen zu berücksichtigen. Die oben gezeigten Modelle in den Bildern A.1, A.2, A.3 und A.4 basieren auf der Grundlage, dass jedes Sicherheitssystem für die gleiche Gefährdung völlig unabhängig ist. Es gibt viele Anwendungen, bei denen dies nicht der Fall ist. Beispiele hierfür sind die folgenden:

1) Wenn ein gefahrbringender Ausfall eines Elements in dem EUC-Leit- oder Steuerungssystem dazu führt, dass eine Anforderung an ein sicherheitsbezogenes System erfolgt und das sicherheitsbezogene System ein Element verwendet, das aus dem gleichen Grund ausfällt. Ein Beispiel hierfür wäre, wenn ein Steuerungs- und ein Schutzsystem zwar getrennte Sensoren verwenden, aber eine gemeinsame Ursache zum Ausfall dieser beiden führt (siehe Abbildung A.5).
2) Wenn mehr als ein sicherheitsbezogenes System verwendet wird und innerhalb derer Betriebsmittel gleicher Bauart verwendet sind, so wird jedes sicherheitsbezogene System von Ausfällen infolge gemeinsamer Ursache betroffen. Ein Beispiel wäre, wenn die gleiche Art von Sensor in zwei getrennten Schutzsystemen verwendet wird, die beide Risikominderungen für die gleiche Gefährdung bereitstellen (siehe Abbildung A.6).
3) Wenn mehr als ein Schutzsystem verwendet wird, die Schutzsysteme diversitär sind, aber die Wiederholungsprüfungen für alle Systeme gleichzeitig erfolgen. In solchen Fällen wird die tatsächliche PFD_{avg}, erreicht durch die Kombination mehrerer Systeme, erheblich höher sein als die aufgrund der Multiplikation der PFD_{avg} der einzelnen Systeme erwartete PFD_{avg}.
4) Wenn das gleiche Element als Teil eines Leit- oder Steuerungssystems und eines sicherheitsbezogenen Systems verwendet wird.
5) Wo mehr als ein Schutzsystem verwendet wird und in denen das gleiche einzelne Element als Teil von mehr als einem System verwendet wird.

In solchen Fällen ist die Wirkung der gemeinsamen Ursache/Abhängigkeit in Betracht zu ziehen. Es sollte betrachtet werden, ob die endgültige Anordnung in der Lage ist, die erforderliche systematische Eignung und die erforderliche Wahrscheinlichkeit gefährlicher zufälliger Hardwareausfallraten im Hinblick auf die geforderte gesamte Risikominderung zu erreichen. Die Wirkung von Ausfällen infolge gemeinsamer Ursache ist nur schwer zu bestimmen und benötigt oftmals die Aufstellung spezieller Modelle (z. B. Fehlerbaum- oder Markov-Modelle).

Die Auswirkung einer gemeinsamen Ursache ist in Anwendungen mit hohen Sicherheits-Integritätsleveln wahrscheinlich größer. In einigen Anwendungen kann Diversität erforderlich sein, so dass Auswirkungen infolge gemeinsamer Ursache minimiert werden. Es sollte jedoch darauf hingewiesen werden, dass es mit der

Diversität zu Problemen beim Entwurf, der Instandhaltung und Änderung kommen kann. Die Einführung von Diversität kann aufgrund von Unkenntnis und mangelnder Erfahrung mit diesen zusätzlichen Geräten zu Fehlern führen.

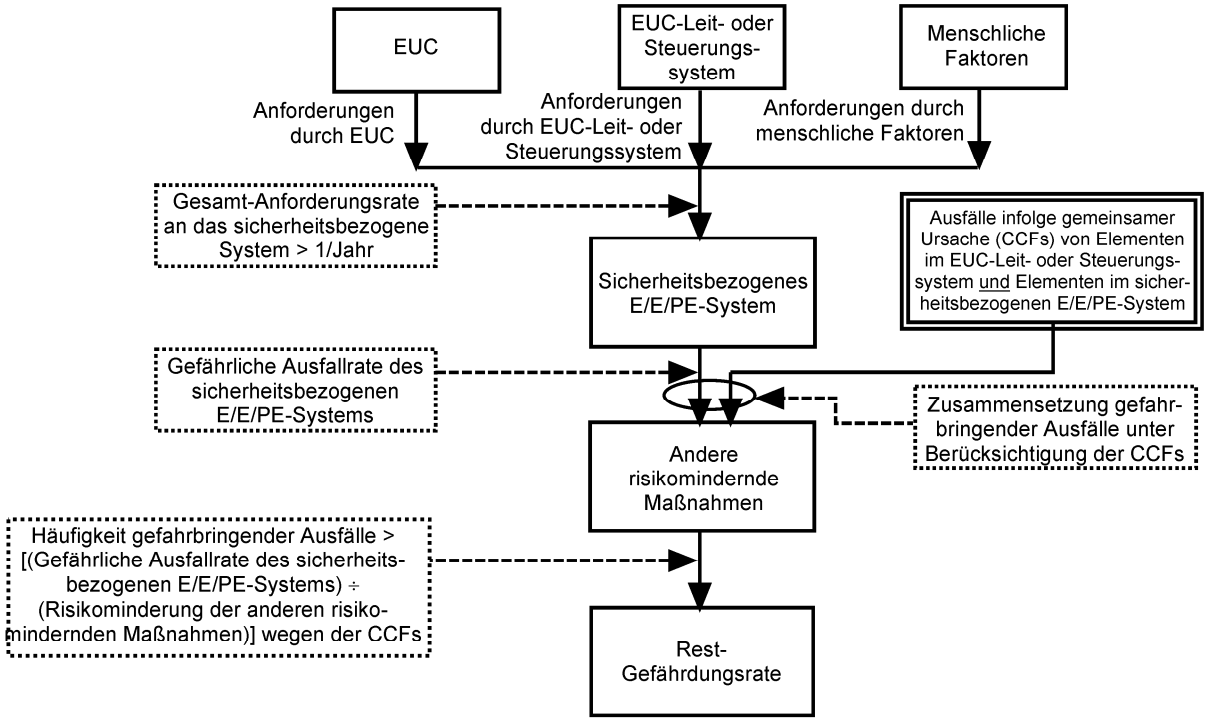


Bild A.5 – Darstellung von Ausfällen infolge gemeinsamer Ursache (CCFs) von Elementen im EUC-Leit- oder Steuerungssystem und Elementen im sicherheitsbezogenen E/E/PE-System

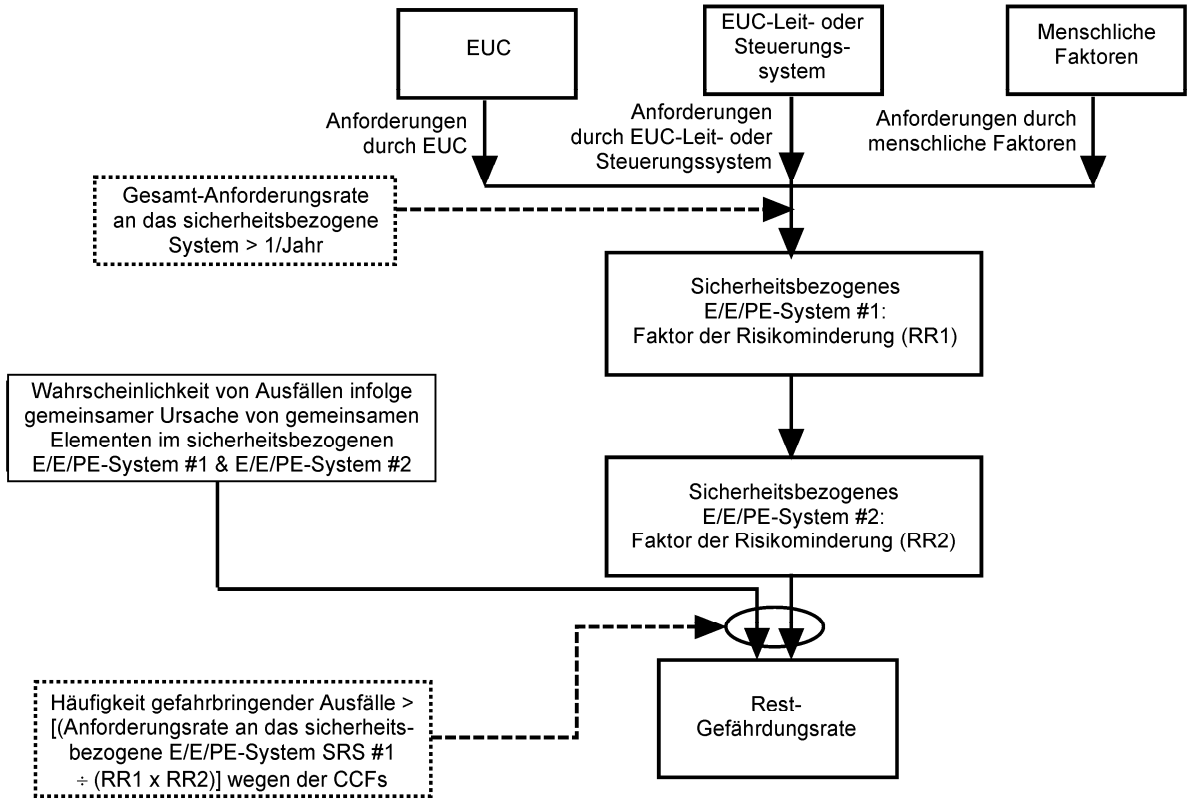


Bild A.6 – Gemeinsame Ursache zwischen zwei sicherheitsbezogenen E/E/PE-Systemen

A.5.5 Sicherheits-Integritätslevel bei Verwendung mehrerer Schutzebenen

Wenn mehrere Schutzebenen verwendet werden, um ein annehmbares Risiko zu erreichen, kann es zu Wechselwirkungen zwischen den Systemen selbst und auch zwischen den Systemen und den Ursachen einer Anforderung kommen. Wie bereits oben in A.5.4 erörtert, gibt es immer wieder Bedenken wegen der Gleichzeitigkeit von Prüfungen und Ausfällen infolge gemeinsamer Ursache, da diese wesentliche Faktoren sein können, wenn die Anforderungen an die Gesamtrisikominderung hoch sind und wenn die Frequenz der Anforderungen gering ist. Die Bewertung der Wechselwirkungen zwischen den Schutzebenen und zwischen den Schutzebenen und den Ursachen der Anforderung kann sehr komplex sein und die Entwicklung eines ganzheitlichen Modells erfordern (z. B. wie in ISO/IEC 31010 beschrieben), das zum Beispiel auf einem Top-down-Ansatz mit der zulässigen Frequenz der Gefährdung als Top-Ereignis beruht. Das Modell kann alle Schutzebenen für die Berechnung der tatsächlichen Risikominderung und alle Ursachen von Anforderungen für die Berechnung der tatsächlichen Häufigkeit von Unfällen beinhalten. Dies ermöglicht die Ermittlung von minimalen Schnittmengen (d. h. Ausfallszenarien), zeigt die Schwachpunkte (d. h. die kleinste minimale Schnittmenge: Einzel-, Doppel-Ausfälle usw.) in der Anordnung der Systeme und eine Systemverbesserung durch Empfindlichkeits-Analyse.

A.6 Risiko und Sicherheitsintegrität

Es ist wichtig, dass die Unterscheidung zwischen Risiko und Sicherheitsintegrität vollständig erkannt wird. Das Risiko ist ein Maß für die Wahrscheinlichkeit und die Auswirkung eines bestimmten auftretenden gefährlichen Vorfalls. Es kann für unterschiedliche Situationen ausgewertet werden (EUC-Risiko, notwendige Risikominderung, um das tolerierbare Risiko zu erreichen, tatsächliches Risiko (siehe Bild A.1)). Das tolerierbare Risiko wird bestimmt unter Berücksichtigung des in A.2 beschriebenen Sachverhalts. Die Sicherheitsintegrität bezieht sich nur auf die sicherheitsbezogenen E/E/PE-Systeme und andere risikomindernde Maßnahmen und ist ein Maß für die Wahrscheinlichkeit dieser Systeme/Einrichtungen, die notwendige Risikominderung in Bezug auf die festgelegten Sicherheitsfunktionen zufriedenstellend zu erreichen. Sobald das tolerierbare Risiko festgelegt und die notwendige Risikominderung bestimmt worden ist, können die Anforderungen zur Sicherheitsintegrität der sicherheitsbezogenen Systeme zugeordnet werden (siehe IEC 61508-1, 7.4, 7.5 und 7.6).

ANMERKUNG Die Zuordnung ist notwendigerweise iterativ, um den Entwurf so zu optimieren, dass die verschiedenen Anforderungen erfüllt werden.

A.7 Sicherheits-Integritätslevel und systematische Eignung

Um den weiten Bereich der notwendigen Risikominderungen, den sicherheitsbezogene Systeme erreichen müssen, abzudecken, ist es nützlich, über eine Anzahl von Sicherheits-Integritätsleveln zur Erfüllung der Anforderungen der Sicherheitsintegrität der Sicherheitsfunktionen, die den sicherheitsbezogenen Systemen zugewiesen sind, zu verfügen. Die systematische Eignung der Software wird als Grundlage für die Spezifikation der Anforderungen zur Sicherheitsintegrität von Sicherheitsfunktionen, die teilweise durch die sicherheitsbezogene Software realisiert wird, verwendet. Die Spezifikation der Anforderungen an die Sicherheitsintegrität sollte den Sicherheits-Integritätslevel für die sicherheitsbezogenen E/E/PE-Systeme bestimmen.

In dieser Norm sind vier Sicherheits-Integritätslevel festgelegt, wobei der Sicherheits-Integritätslevel 4 die höchste und der Sicherheits-Integritätslevel 1 die niedrigste Stufe ist.

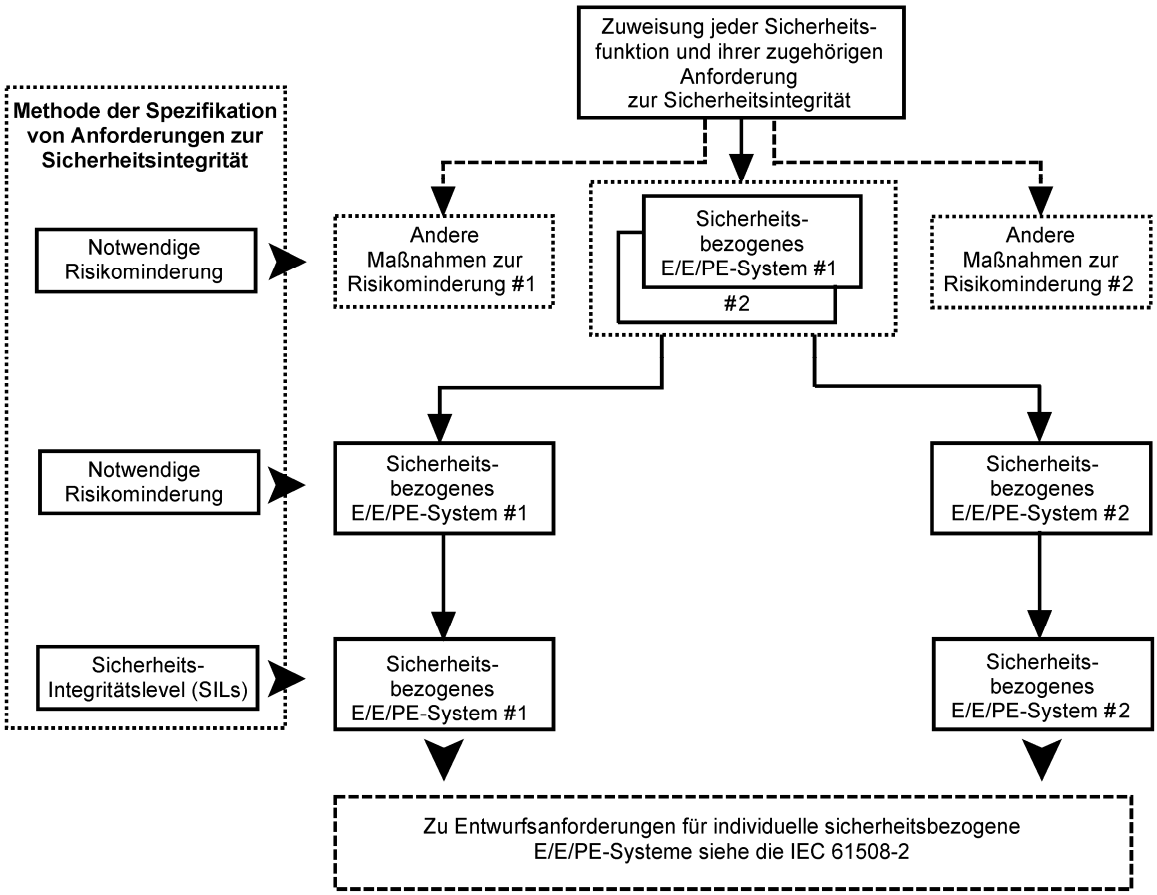
Die Versagens- und Ausfallgrenzwerte für die vier Sicherheits-Integritätslevel sind in IEC 61508-1, Tabellen 2 und 3, angegeben. Zwei Parameter sind angegeben, einer für sicherheitsbezogene Systeme, die in einer Betriebsart mit niedriger Anforderungsrate betrieben werden, und einer für sicherheitsbezogene Systeme, die in einer Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung betrieben werden.

ANMERKUNG Für sicherheitsbezogene Systeme, die in einer Betriebsart mit niedriger Anforderungsrate betrieben werden, ist das interessierende Maß für die Sicherheitsintegrität die Ausfallwahrscheinlichkeit, die entworfene Funktion auf Anforderung nicht auszuführen. Für sicherheitsbezogene Systeme, die in einer Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung betrieben werden, ist das interessierende Maß für die Sicherheitsintegrität die mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde (siehe IEC 61508-4, 3.5.16 und 3.5.17).

A.8 Zuordnung von Sicherheitsanforderungen

Die Zuordnung von Sicherheitsanforderungen (sowohl der Sicherheitsfunktionen als auch der Anforderungen zur Sicherheitsintegrität) zu den sicherheitsbezogenen E/E/PE-Systemen, sicherheitsbezogenen Systemen anderer Technologie und externen Einrichtungen zur Risikominderung wird in Bild A.7 dargestellt (dies ist identisch zu IEC 61508-1, Bild 6). Die Anforderungen an die Phase der Zuordnung der Sicherheitsanforderungen sind in IEC 61508-1, 7.6, enthalten.

Die Methoden für die Zuordnung der Anforderungen zur Sicherheitsintegrität zu den sicherheitsbezogenen E/E/PE-Systemen, sicherheitsbezogenen Systemen anderer Technologie und andere Maßnahmen zur Risikominderung hängen zuallererst davon ab, ob die notwendige Risikominderung in einer numerischen oder qualitativen Art und Weise festgelegt ist. Diese Methoden werden als quantitative bzw. qualitative Methoden bezeichnet (siehe Anhänge C, D, E, F und G).



ANMERKUNG 1 Anforderungen an die Sicherheitsintegrität sind jeder Sicherheitsfunktion vor der Zuweisung zugeordnet (siehe IEC 61508-1, 7.5.2.3 und 7.5.2.4).

ANMERKUNG 2 Eine Sicherheitsfunktion kann mehr als einem sicherheitsbezogenen System zugeordnet werden.

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

A.9 Systeme zur Schadensbegrenzung

Systeme zur Schadensbegrenzung greifen im Falle des vollständigen oder teilweisen Ausfalls anderer sicherheitsbezogener Systeme wie z. B. E/E/PE-Sicherheitssysteme ein. Das Ziel ist eher die Verringerung der Auswirkungen im Zusammenhang mit einem gefährlichen Vorfall als dessen Häufigkeit. Beispiele für Systeme zur Schadensbegrenzung sind Feuer- und Gas-Systeme (Erkennung von Feuer/Gas- und nachgeord-

nete Maßnahmen, um das Feuer zu löschen (z. B. durch Wasserflutung)) und Airbag-Systeme in einem Automobil).

Bei der Bestimmung der Anforderungen der Sicherheitsintegrität sollte berücksichtigt werden, dass bei der Entscheidung über die Schwere der Auswirkungen nur die erhöhten Auswirkungen zu berücksichtigen sind. Das bedeutet die Bestimmung der Zunahme der Schwere der Auswirkungen, wenn die Funktion nicht arbeitet, gegenüber wenn diese wie vorgesehen arbeitet. Dies kann erfolgen, indem zunächst die Konsequenzen betrachtet werden, wenn das System nicht wie vorgesehen funktioniert, und dann, welchen Unterschied es ausmacht, wenn die Systeme zur Schadensbegrenzung ordnungsgemäß arbeiten. Bei der Berücksichtigung der Auswirkungen, wenn das System nicht wie vorgesehen funktioniert, wird sich in der Regel eine Reihe von Ergebnissen mit unterschiedlichen Wahrscheinlichkeiten ergeben. Die Ereignisbaumanalyse (en: event tree analysis, ETA) kann ein nützliches Instrument hierzu sein.

ANMERKUNG Die Anleitung zur Bestimmung des Sicherheits-Integritätslevels für Feuer-, Gas- und Notabschaltungs-Systeme ist im Anhang B der ISO-10418 enthalten.

Anhang B
(informativ)

Auswahl von Methoden zur Bestimmung der Anforderungen an den Sicherheits-Integritätslevel

B.1 Allgemeines

Dieser Anhang enthält eine Reihe von Verfahren, die zur Bestimmung des Sicherheits-Integritätslevels verwendet werden können. Keines der Verfahren eignet sich für alle Anwendungen und die Benutzer werden daher das am besten geeignete auswählen. Bei der Auswahl der am besten geeigneten Verfahren sollten die folgenden Faktoren berücksichtigt werden:

1) Die Risiko-Akzeptanzkriterien, die zu erfüllen sind. Einige der Verfahren werden nicht geeignet sein, wenn es erforderlich ist, nachzuweisen, dass das Risiko so weit wie vernünftigerweise möglich reduziert wurde.
2) Die Betriebsart der Sicherheitsfunktion. Einige Verfahren sind nur für die Betriebsart mit niedriger Anforderungsrate geeignet.
3) Das Wissen und die Erfahrung der Personen, die die SIL-Bestimmung durchführen, und der traditionelle Ansatz in ihrem Bereich.
4) Das geforderte Vertrauen, dass das sich ergebende Restrisiko die spezifizierten Kriterien der Anwender-Organisation erfüllt. Einige der Methoden können bei quantifizierten Zielen angewendet werden, einige Ansätze sind aber nur qualitativ.
5) Es kann mehr als eine Methode verwendet werden. Eine Methode kann für eine Vorauswahl verwendet werden, gefolgt von einem anderen strengeren Ansatz, wenn die Vorauswahl die Notwendigkeit eines hohen Sicherheits-Integritätslevels zeigt.
6) Die Schwere der Auswirkungen. Strengere Methoden können ausgewählt werden, wenn die Auswirkungen mehrere Todesopfer beinhalten.
7) Ob gemeinsame Ursachen zwischen den sicherheitsbezogenen E/E/PE-Systemen oder zwischen dem sicherheitsbezogenen E/E/PE-System und den Ursachen der Anforderungen bestehen.

Unabhängig von der angewandten Methode sollten alle gemachten Annahmen für das zukünftige Management der Sicherheit aufgezeichnet werden. Alle Entscheidungen sollten aufgezeichnet werden, damit die SIL-Beurteilung verifiziert und einer unabhängigen Beurteilung der funktionalen Sicherheit unterzogen werden kann.

B.2 Die ALARP-Methode

Die ALARP-Prinzipien können als eigenständige Methode oder zusammen mit anderen Methoden verwendet werden, um die SIL-Anforderungen für eine Sicherheitsfunktion zu bestimmen. Sie kann in einer qualitativen oder quantitativen Art verwendet werden. Bei Verwendung in qualitativer Art werden die SIL-Anforderungen für eine spezifizierte Sicherheitsfunktion so lange erhöht, bis sich die Häufigkeit des Auftretens so reduziert, dass die Bedingungen, die der Risikoklasse II oder III zugeordnet sind, erfüllt werden. Bei Verwendung in einer quantitativen Art werden die Häufigkeiten und Auswirkungen numerisch spezifiziert und die SIL-Anforderungen erhöht, bis gezeigt werden kann, dass die zusätzlichen Finanzmittel und Betriebskosten für die Umsetzung eines höheren SILs die Bedingungen, die der Risikoklasse II oder III zugeordnet sind, erreicht würden (siehe Bild C.1).

Bei Anwendung der ALARP-Methode wird die Grenze zwischen dem nicht annehmbaren Bereich und dem ALARP-Bereich betrachtet.

B.3 Quantitative Methode der SIL-Bestimmung

Die quantitative Methode ist in Anhang D beschrieben. Sie kann zusammen mit der ALARP-Methode in Anhang C verwendet werden.

Die quantitative Methode kann sowohl für einfache als auch komplexe Anwendungen verwendet werden. Bei komplexen Anwendungen können Fehlerbäume konstruiert werden, um das Gefährdungsmodell darzustellen. Das oberste Ereignis wird in der Regel ein oder mehrere Todesopfer sein und es wird eine Logik entworfen, um die Ursachen der Anforderungen und Ausfälle der sicherheitsbezogenen E/E/PE-Systeme darzustellen, die zu dem obersten Ereignis führen. Es stehen Softwarewerkzeuge zur Verfügung, um gemeinsame Ursachen zu modellieren, wenn die gleiche Art von Ausrüstung für die Steuerungs- und Schutzfunktionen verwendet wird. In einigen komplexen Anwendungen kann ein einzelnes Ausfallereignis an mehr als einer Stelle im Fehlerbaum auftreten. Dies erfordert die Durchführung einer Boolschen Reduzierung. Die Werkzeuge unterstützen auch die Empfindlichkeitsanalyse, um die beherrschenden Einflussfaktoren auf die Häufigkeit des obersten Ereignisses zu zeigen. Der SIL kann durch die Bestimmung der erforderlichen Risikominderung, um das tolerierbare Risikokriterium zu erreichen, erhalten werden.

Die Methode ist für Sicherheitsfunktionen in der Betriebsart mit kontinuierlicher/hoher und der Betriebsart mit niedriger Anforderungsrate geeignet. Diese Methode ergibt in der Regel geringe SILs, da das Risikomodell speziell für jede Anwendung und deren numerische Werte entworfen worden ist, um jeweils einen Risikofaktor darzustellen, statt der numerischen Bereiche, die in kalibrierten Risikographen verwendet werden. Quantitative Methoden erfordern jedoch die Aufstellung eines speziellen Modells für jeden gefährlichen Vorfall. Die Modellierung erfordert Geschick, Werkzeuge und Kenntnisse über die Anwendung und kann erhebliche Zeit zur Entwicklung und zur Überprüfung erfordern.

Die Methode erleichtert den Nachweis, dass das Risiko so weit wie vernünftigerweise möglich reduziert worden ist. Dies kann durch Berücksichtigung von Möglichkeiten für eine weitere Risikominderung, der Integration von zusätzlichen Einrichtungen in das Fehlerbaum-Modell und schließlich der Bestimmung der Verringerung des Risikos und den Vergleich mit den Kosten für diese Variante erreicht werden.

B.4 Die Risikograph-Methode

Die qualitative Methode des Risikographen ist in Anhang E beschrieben. Die Methode ermöglicht es, den Sicherheits-Integritätslevel aufgrund der Kenntnis der Risikofaktoren, die mit dem EUC-Leit- oder Steuerungssystem verbunden sind, zu bestimmen. Es wird eine Reihe von Parametern eingeführt, die zusammen die Art der Gefährdungssituation beschreiben, wenn die sicherheitsbezogenen Systeme versagen oder nicht zur Verfügung stehen. Aus vier Sätzen wird je ein Parameter gewählt, und die ausgewählten Parameter werden dann kombiniert, um so den der Sicherheitsfunktion zugeordneten Sicherheits-Integritätslevel zu bestimmen. Die Methode wird ausführlich im Maschinenbau, siehe ISO 14121-2 und ISO 13849-1, Anhang A, verwendet.

Die Methode kann qualitativ sein, in diesem Fall ist die Auswahl der Parameter subjektiv und erfordert ein erhebliches Urteilsvermögen. Das Restrisiko kann nicht durch die Kenntnis der Werte der Parameter berechnet werden. Die Methode ist so nicht geeignet, wenn eine Organisation fordert, das Restrisiko auf einen bestimmten quantitativen Wert zu reduzieren.

Die Beschreibung der Parameter kann numerische Werte beinhalten, die sich durch die Kalibrierung des Risikographen gegen numerische, tolerierte Risikokriterien herleiten. Das Restrisiko lässt sich aus den numerischen Werten, die für jeden der Parameter verwendet wurden, berechnen. Diese Methode ist geeignet, wenn eine Organisation Vertrauen darin fordert, dass das Restrisiko auf einen bestimmten quantitativen Wert reduziert worden ist. Die Erfahrung hat gezeigt, dass die Verwendung der Methode eines kalibrierten Risikographen zu hohen Sicherheits-Integritätslevel führen kann. Dies liegt daran, dass die Kalibrierung in der Regel mit verwendeten Worst-Case-Werten der einzelnen Parameter durchgeführt wird. Jeder Parameter hat den Bereich einer Dekade, so dass für Anwendungen, bei denen alle Parameter Durchschnittswerte sind, der SIL eine Dekade höher sein wird als das notwendige tolerierbare Risiko. Das Verfahren wird umfangreich im Prozess- und im Offshore-Sektor eingesetzt.

Die Risikograph-Methode berücksichtigt nicht, wenn eine gemeinsame Ursache die Anforderung auslöst und gleichzeitig zum Ausfall des sicherheitsbezogenen E/E/PE-System führt oder gemeinsame Ursachen in mehreren Schutzebenen.

B.5 Analyse der Schutzebenen (en: Layer of Protection Analysis (LOPA))

Die grundlegende Methode ist in einer Reihe von Büchern beschrieben und das Verfahren kann in einer Reihe von verschiedenen Formen verwendet werden. Eine Technik, die für die SIL-Bestimmung verwendet werden kann, ist im Anhang F beschrieben.

Das Verfahren ist quantitativ und der Anwender hat die zulässigen Häufigkeiten für jede Auswirkung und jeden Schweregrad festzulegen. Es erfolgt eine numerische Gutschrift für die Schutzebenen, die die Häufigkeit der individuellen Ursachen für Anforderungen reduzieren. Nicht alle Schutzebenen sind für alle Ursachen von Anforderungen zuständig, so dass das Verfahren für komplexere Anwendungen verwendet werden kann. Die den Schutzebenen zugeordneten numerischen Werte können auf die nächste signifikante Zahl oder den nächsten signifikanten Dekadebereich aufgerundet werden. Wenn numerische Werte von Schutzebenen auf die nächste signifikante Zahl gerundet werden, ergibt das Verfahren im Durchschnitt geringere Anforderungen an die Risikominderung und niedrigere SIL-Werte als kalibrierte Risikographen.

Da bestimmten Auswirkungs-Schweregraden numerische Ziele zugeordnet sind, kann der Anwender darauf vertrauen, dass das Restrisiko die Unternehmenskriterien erfüllt.

Die beschriebene Methode ist nicht geeignet für Funktionen, die in der Betriebsart mit kontinuierlicher Anforderung betrieben werden, und berücksichtigt nicht, wenn eine gemeinsame Ursache die Anforderung auslöst und gleichzeitig zum Ausfall des sicherheitsbezogenen E/E/PE-System führt. Die Methode kann jedoch angepasst werden und eignet sich dann für solche Fälle.

B.6 Matrix des Ausmaßes des gefährlichen Vorfalls

Die Methode der Bestimmung des Ausmaßes des gefährlichen Vorfalls in einer Matrix wird in Anhang G beschrieben. Eine inhärente Annahme ist die, dass, wenn eine Schutzebene hinzugefügt wird, eine Größenordnung der Risikominderung erreicht wird. Eine weitere Annahme ist die, dass die Schutzebenen unabhängig von der Ursache der Anforderung und unabhängig voneinander sind. Die Methode wird beschrieben als nicht geeignet für Funktionen, die in der Betriebsart mit kontinuierlicher Anforderung betrieben werden. Diese Methode kann qualitativ sein, in diesem Fall ist die Auswahl der Risikofaktoren subjektiv und erfordert erhebliche Beurteilungen. Das Restrisiko kann nicht aus der Kenntnis der ausgewählten Risikofaktoren berechnet werden. Die Methode wird nicht geeignet sein, wenn eine Organisation Vertrauen darin fordert, dass das Restrisiko auf einen bestimmten quantitativen Wert reduziert wird.

Anhang C
(informativ)

Konzepte für ALARP und tolerierbares Risiko

C.1 Allgemeines

Dieser Anhang berücksichtigt einen bestimmten Ansatz zur Erreichung eines tolerierbaren Risikos. Er ist nicht als eine endgültige Beschreibung der Methode vorgesehen, sondern zur Erläuterung der allgemeinen Prinzipien. Das Konzept beinhaltet einen Prozess der kontinuierlichen Verbesserung, wobei alle Möglichkeiten, die das Risiko reduzieren, betrachtet werden in Bezug auf Kosten und Nutzen. Diejenigen, die beabsichtigen, die in diesem Anhang aufgeführten Methoden anzuwenden, sollten das angegebene Quellenmaterial zu Rate ziehen (siehe Verweis [7] in den Literaturhinweisen).

C.2 ALARP-Modell

C.2.1 Einleitung

Der Abschnitt C.2 gibt einen Überblick über die Hauptprüfungen, die bei der Regulierung industrieller Risiken verwendet werden, und gibt an, dass es sich darum handelt festzustellen, ob:

a) das Risiko so groß ist, dass es insgesamt abgelehnt werden muss; oder

b) das Risiko so klein ist oder so weit verringert worden ist, dass es unbedeutend ist; oder

c) das Risiko zwischen den beiden oben in a) und b) genannten Zuständen liegt, und dass es auf die niedrigste Stufe, die praktikabel ist, verringert worden ist unter Berücksichtigung des aus der Akzeptanz folgenden Nutzens und der Kosten jeder weiteren Minderung.

Im Hinblick auf c) erfordert das ALARP-Prinzip, dass jedes Risiko so weit wie vernünftigerweise möglich gemindert wird oder bis zu einer Stufe, die so niedrig wie vernünftigerweise möglich ist (ALARP = as low as reasonably practicable = so niedrig wie vernünftigerweise möglich). Wenn ein Risiko zwischen die beiden Extreme fällt (d. h. zwischen den nicht annehmbaren Bereich und den weithin annehmbaren Bereich) und das ALARP-Prinzip angewendet worden ist, ist das resultierende Risiko das für die betreffende Anwendung tolerierbare Risiko. Diese Vorgehensweise mit drei Bereichen ist in Bild C.1 gezeigt.

Oberhalb einer bestimmten Stufe wird das Risiko als nicht tolerierbar betrachtet und kann unter keinem üblichen Umstand gerechtfertigt werden.

Unterhalb dieser Ebene gibt es einen tolerierbaren Bereich, in dem eine Tätigkeit erlaubt ist, vorausgesetzt, dass die zugehörigen Risiken so weit wie vernünftigerweise möglich gemindert worden sind. „Tolerierbar“ unterscheidet sich hier von „annehmbar“: Es zeigt die Bereitwilligkeit an, mit einem Risiko eines bestimmten Nutzens wegen zu leben mit der gleichzeitigen Erwartung, es zu beobachten und zu vermindern, sobald dies möglich ist. Hier ist eine Nutzenbeurteilung erforderlich, entweder explizit oder implizit, um die Kosten und die Notwendigkeit für weitere Sicherheitsmaßnahmen abzuwägen. Je höher das Risiko, desto mehr Aufwand kann erwartet werden, um dieses zu verringern. An der Grenze der Tolerierbarkeit würde Aufwand in großem Missverhältnis zum Nutzen gerechtfertigt werden. Hier wird das Risiko beträchtlich und Recht und Billigkeit verlangen selbst für eine unbedeutende Minderung einen beträchtlichen Aufwand.

Wo Risiken weniger bedeutsam sind, wird proportional weniger Aufwand benötigt, um diese zu mindern, und am unteren Ende des tolerierbaren Bereiches ist eine Abwägung zwischen Kosten und Nutzen ausreichend.

Unterhalb des tolerierbaren Bereiches ist der weithin annehmbare Bereich, in dem Risiken im Vergleich zum täglichen Risiko, das wir alle erfahren, klein sind. Während in dem weithin annehmbaren Bereich keine weitere Arbeit notwendig ist, um ALARP darzulegen, ist andererseits Wachsamkeit notwendig, um sicherzustellen, dass das Risiko auf dieser Stufe verbleibt.

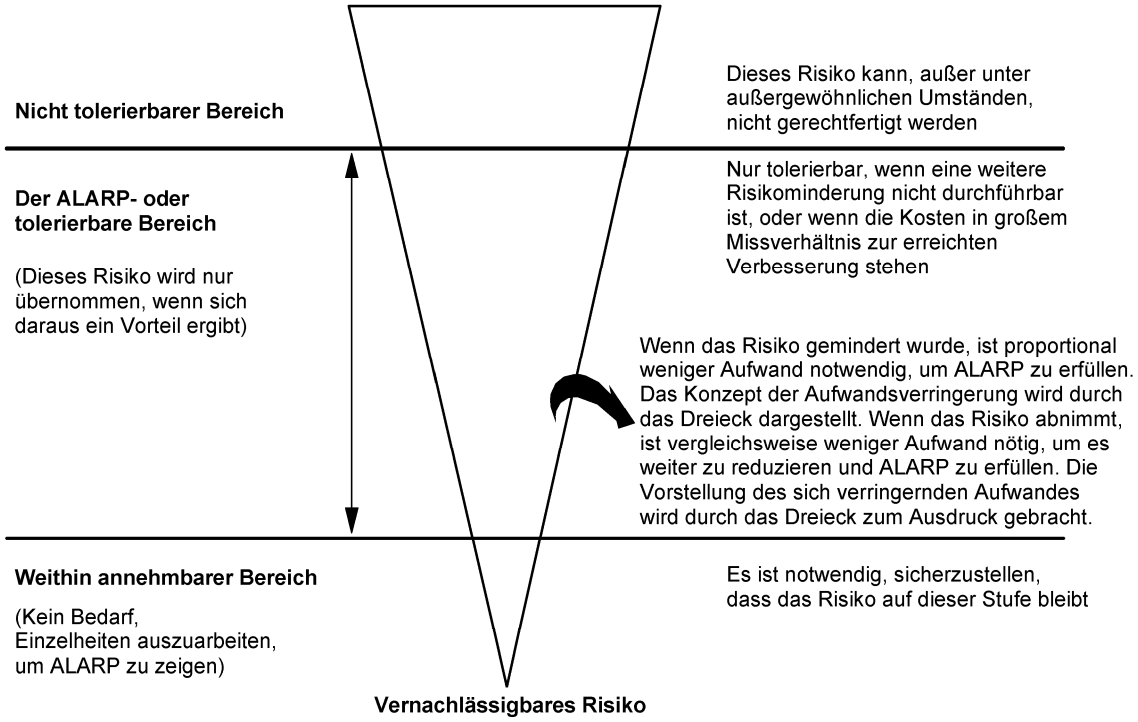


Bild C.1 – Tolerierbares Risiko und ALARP

Das ALARP-Konzept kann benutzt werden, wenn qualitative oder quantitative Risikogrenzwerte verwendet werden. C.2.2 zeigt eine Methode für quantitative Risikogrenzwerte. (Anhang D und F zeigen quantitative Methoden und die Anhänge E und G zeigen qualitative Methoden für die Festlegung der notwendigen Risikominderung für eine bestimmte Gefährdung. Die aufgezeigten Methoden könnten in der Entscheidungsfindung das ALARP-Konzept mit einbeziehen.)

ANMERKUNG Für weitere Informationen zu ALARP siehe Verweis [7] der Literaturhinweise.

C.2.2 Grenzwert für das tolerierbare Risiko

Eine Möglichkeit, wie ein Grenzwert für das tolerierbare Risiko erreicht werden kann, ist es, eine Anzahl von Auswirkungen zu bestimmen und ihnen tolerierbare Häufigkeiten zuzuweisen. Dieses Zusammenbringen der Auswirkungen mit den tolerierbaren Häufigkeiten erfolgt durch Diskussion und Übereinkommen zwischen den beteiligten Parteien (z. B. den Behörden, die Sicherheitsregeln erstellen, und denjenigen, die das Risiko verursachen, und denjenigen, die dem Risiko ausgesetzt sind).

Unter Berücksichtigung von ALARP-Konzepten kann das Zusammenbringen einer Auswirkung mit einer tolerierbaren Häufigkeit durch Risikoklassen erfolgen. Tabelle C.1 ist ein Beispiel, das vier Risikoklassen (I, II, III, IV) für eine Anzahl von Auswirkungen und Häufigkeiten enthält. Unter Verwendung des ALARP-Konzeptes interpretiert Tabelle C.2 jede Risikoklasse. Das bedeutet, dass die Beschreibung jeder Risikoklasse auf Bild C.1 basiert. Die Risiken in diesen Risikoklassen sind die Risiken, die vorhanden sind, wenn die Maßnahmen zur Risikominderung durchgeführt worden sind. Im Hinblick auf Bild C.1 sind die Risikoklassen wie folgt festgelegt:

– Risikoklasse I ist im nicht tolerierbaren Bereich;
– Risikoklassen II und III sind im ALARP-Bereich; die Risikoklasse II ist gerade noch im ALARP-Bereich;
– Risikoklasse IV ist im weithin annehmbaren Bereich.

Für jede bestimmte Situation oder jeden bestimmten Bereich vergleichbarer Industrien würde eine Tabelle, ähnlich zu Tabelle C.1, unter Berücksichtigung eines weiten Bereiches gesellschaftlicher, politischer und wirtschaftlicher Faktoren entwickelt werden. Jede Auswirkung würde mit einer Häufigkeit zusammengebracht und die Tabelle mit Risikoklassen ausgefüllt werden. Zum Beispiel könnte „häufig“ in Tabelle C.1 ein Ereignis bezeichnen, das wahrscheinlich dauernd eintritt, was als Häufigkeit von mehr als 10 Ereignissen je Jahr be-

zeichnet werden könnte. Eine kritische Auswirkung könnte der Tod einer Person und/oder mehrfache schwerwiegende Verletzungen oder eine schwerwiegende Berufskrankheiten sein.

Tabelle C.1 – Beispiel für die Risikoklassifizierung von Unfällen

Häufigkeit	Auswirkung			
	katastrophal	kritisch	begrenzt	Geringfügig
häufig	I	I	I	II
wahrscheinlich	I	I	II	III
gelegentlich	I	II	III	III
gering	II	III	III	IV
unwahrscheinlich	III	III	IV	IV
nicht glaubhaft	IV	IV	IV	IV

ANMERKUNG 1 Die tatsächlichen Risikoklassen I, II, III, IV sind vom Einsatzgebiet abhängig und ebenfalls davon, was die aktuellen Häufigkeiten „häufig“, „wahrscheinlich“ usw. bedeuten. Daher sollte diese Tabelle eher als Beispiel gesehen werden, wie eine solche Tabelle ausgefüllt werden könnte, und weniger als Festlegung für die zukünftige Verwendung.

ANMERKUNG 2 Die Bestimmung des Sicherheits-Integritätslevels aus den Häufigkeiten dieser Tabelle wird in Anhang D darstellt.

Tabelle C.2 – Interpretation der Risikoklassen

Risikoklasse	Interpretation
Klasse I	nicht tolerierbares Risiko
Klasse II	unerwünschtes Risiko, das nur tolerierbar ist, wenn eine Risikominderung nicht durchführbar ist oder die Kosten der Minderung unverhältnismäßig hoch im Vergleich zur erzielten Verbesserung sind
Klasse III	tolerierbares Risiko, wenn die Kosten einer Risikominderung die erreichbare Verbesserung übersteigen
Klasse IV	vernachlässigbares Risiko

Anhang D
(informativ)

Festlegung der Sicherheits-Integritätslevel – Eine quantitative Methode

D.1 Allgemeines

Dieser Anhang skizziert, wie die Sicherheits-Integritätslevel bei Verwendung einer quantitativen Methode festgelegt werden können, und zeigt auf, wie die in Tabellen, zum Beispiel Tabelle D.1, enthaltenen Informationen verwendet werden können. Eine quantitative Methode ist von besonderem Wert, wenn:

– das tolerierbare Risiko in einer numerischen Art und Weise zu bestimmen ist (z. B. dass eine bestimmte Auswirkung nicht mit einer Häufigkeit größer als einmal in 10^4 Jahren auftreten sollte);

– numerische Grenzwerte für die Sicherheits-Integritätslevel der sicherheitsbezogenen Systeme bestimmt worden sind. Derartige Grenzwerte sind in dieser Norm festgelegt worden (siehe IEC 61508-1, Tabellen 2 und 3).

Dieser Anhang ist nicht als endgültige Beschreibung der Methode, sondern zur Erläuterung der allgemeinen Prinzipien vorgesehen. Er ist insbesondere anwendbar, wenn das Risikomodell dem in den Bildern A.1 und A.2 gezeigten entspricht.

D.2 Allgemeine Methode

Das für die Darstellung der allgemeinen Prinzipien verwendete Modell wird in Bild A.1 gezeigt. Die wesentlichen Schritte der Methode sind die folgenden und für jede durch das sicherheitsbezogene E/E/PE-System realisierte Sicherheitsfunktion erforderlich:

– Bestimmung des tolerierbaren Risikos aus einer Tabelle ähnlich der Tabelle C.1;

– Bestimmung des EUC-Risikos;

– Bestimmung der notwendigen Risikominderung, um das tolerierbare Risiko zu erreichen;

– Zuordnung der notwendigen Risikominderung zu den sicherheitsbezogenen E/E/PE-Systemen, sicherheitsbezogenen Systemen anderer Technologien und anderen Maßnahmen zur Risikominderung (siehe IEC 61508-1, 7.6) [NA1)].

Tabelle C.1 enthält Risikohäufigkeiten und ermöglicht die Festlegung eines numerischen Grenzwertes (F_t) für das tolerierbare Risiko.

Die Häufigkeit, die mit dem Risiko, das für die EUC einschließlich des EUC-Leit- oder Steuerungssystems und menschlicher Faktoren ohne jede Schutzmaßnahme existiert (das EUC-Risiko), zusammenhängt, kann unter Anwendung quantitativer Risikobeurteilungsmethoden abgeschätzt werden. Diese Häufigkeit (F_{np}), mit der ein gefährlicher Vorfall ohne vorhandene Schutzeigenschaften auftreten könnte, ist einer von zwei Bestandteilen des EUC-Risikos; der andere Bestandteil ist die Auswirkung des gefährlichen Vorfalls. F_{np} kann bestimmt werden durch:

– Analyse der Ausfallraten in vergleichbaren Situationen;

– Daten aus relevanten Datenbanken;

– Berechnung unter Anwendung angemessener Vorhersagemethoden.

Diese Norm macht Einschränkungen bezüglich der minimalen Ausfallraten, die für das EUC-Leit- oder Steuerungssystem geltend gemacht werden können (siehe IEC 61508-1, 7.5.2.5). Falls geltend gemacht wird, dass das EUC-Leit- oder Steuerungssystem eine geringere Ausfallrate als diese minimalen Ausfallraten hat, muss

---

[NA1)] Nationale Fußnote: Die sicherheitsbezogenen Systeme anderer Technologien und andere Maßnahmen zur Risikominderung bilden zusammen die „anderen risikominderden Maßnahmen“.

das EUC-Leit- oder Steuerungssystem als sicherheitsbezogenes System betrachtet werden und allen Anforderungen an sicherheitsbezogene Systeme in dieser Norm unterworfen werden.

D.3 Beispielrechnung

Bild D.1 liefert ein Beispiel, wie der Grenzwert der Sicherheitsintegrität für eine einzelne sicherheitsbezogene Schutzeinrichtung berechnet wird. In diesem Fall ist:

$$PFD_{avg} \leq F_t / F_{np}$$

Dabei ist

PFD_{avg} die mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung des sicherheitsbezogenen Schutzsystems ist, das ist der Ausfallgrenzwert für das sicherheitsbezogene Schutzsystem in der Betriebsart mit niedriger Anforderungsrate (siehe IEC 61508-1, Tabelle 2, und IEC 61508-4, 3.5.12);

F_t die Häufigkeit der tolerierbaren Gefährdung ist;

F_{np} die Anforderungsrate der sicherheitsbezogenen Schutzeinrichtung ist.

Ebenfalls in Bild D.1:

– C ist die Auswirkung des gefährlichen Vorfalls;

– F_p ist die Häufigkeit des Risikos bei Vorhandensein der Schutzeigenschaften.

Es ist ersichtlich, dass die Bestimmung von F_{np} für die EUC wegen ihrer Beziehung zu PFD_{avg} und damit zum Sicherheits-Integritätslevel des sicherheitsbezogenen Schutzsystems wichtig ist.

Die erforderlichen Schritte zur Erzielung des Sicherheits-Integritätslevels (wenn die Auswirkung C konstant bleibt) werden unten (wie in Bild D.1) für die Situation angegeben, in der die gesamte notwendige Risikominderung durch eine einzelne sicherheitsbezogene Schutzeinrichtung erreicht wird, welche die Gefährdungsrate mindestens von F_{np} auf F_t verringern muss:

– Bestimmung der Häufigkeit des EUC-Risikos ohne das Vorhandensein irgendwelcher Schutzeigenschaften (F_{np});

– Bestimmung der Auswirkung C ohne das Vorhandensein irgendwelcher Schutzeigenschaften;

– Bestimmung, ob für die Häufigkeit (F_{np}) und die Auswirkung (C) eine tolerierbare Stufe des Risikos erreicht worden ist, unter Verwendung der Tabelle C.1. Wenn durch die Verwendung der Tabelle C.1 diese Bestimmung zu der Risikoklasse I führt, ist eine weitere Risikominderung erforderlich. Die Risikoklassen IV oder III entsprechen tolerierbaren Risiken. Die Risikoklasse II erfordert weitere Untersuchungen;

ANMERKUNG Tabelle C.1 wird zur Überprüfung verwendet, ob weitere Maßnahmen zur Risikominderung notwendig sind, da es möglich sein könnte, ein tolerierbares Risiko ohne zusätzliche Schutzeigenschaften zu erreichen.

– Festlegung der Wahrscheinlichkeit eines Ausfalls bei Anforderung für die sicherheitsbezogene Schutzeinrichtung PFD_{avg}, um die minimal erforderliche Risikominderung (ΔR) zu erreichen. Für eine konstante Auswirkung ergibt dies für die beschriebene spezielle Situation $PFD_{avg} = (F_t / F_{np}) = \Delta R$;

– Für $PFD_{avg} = (F_t / F_{np})$ kann der Sicherheits-Integritätslevel der IEC 61508-1, Tabelle 2, entnommen werden (z. B. für $PFD_{avg} = 10^{-2} – 10^{-3}$ ist der Sicherheits-Integritätslevel = 2).

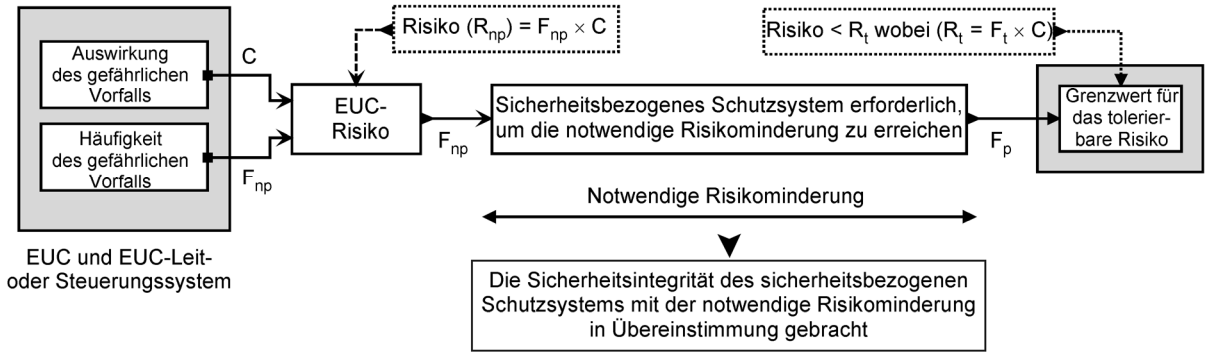


Bild D.1 – Zuordnung der Sicherheitsintegrität – Beispiel für eine sicherheitsbezogene Schutzeinrichtung

Anhang E
(informativ)

Bestimmung der Sicherheits-Integritätslevel – Risikograph-Methoden

E.1 Allgemeines

Dieser Anhang beschreibt die Risikograph-Methode, die es ermöglicht, den Sicherheits-Integritätslevel eines sicherheitsbezogenen Systems aus der Kenntnis der Risikofaktoren, die mit der EUC und dem EUC-Leit- oder Steuerungssystem zusammenhängen, zu bestimmen. Die Vorgehensweise ist insbesondere anwendbar, wenn das Risikomodell dem in den Bildern A.1 und A.2 gezeigten entspricht. Die Methode kann auf einer qualitativen oder quantitativen Basis verwendet werden.

Bei Anwendung dieser Methode wird zur Vereinfachung der Angelegenheit eine Anzahl von Parametern eingeführt, die gemeinsam den Charakter der Gefährdungssituation beschreiben, wenn sicherheitsbezogene Systeme versagen oder nicht vorhanden sind. Ein Parameter wird aus je einem von vier Parametersätzen ausgewählt, und die ausgewählten Parameter werden dann kombiniert, um den Sicherheits-Integritätslevel, der den Sicherheitsfunktionen zugeordnet wird, festzulegen. Diese Parameter:

– erlauben es, eine sinnvolle Abstufung des Risikos durchzuführen, und
– enthalten die Schlüsselfaktoren der Risikobeurteilung.

Dieser Anhang ist nicht als eine endgültige Beschreibung der Methode, sondern zur Erläuterung der allgemeinen Prinzipien vorgesehen.

E.2 Aufbau des Risikographen

Das nachfolgende vereinfachte Verfahren basiert auf folgender Gleichung:

$$R = (f) \text{ eines bestimmten } (C)$$

Dabei ist

R das Risiko ohne sicherheitsbezogenes System ist;

f die Häufigkeit des gefährlichen Vorfalls ohne sicherheitsbezogenes System ist;

C die Auswirkung des gefährlichen Vorfalls ist (die Auswirkungen könnten auf den Schaden, der mit Gesundheit und Sicherheit oder mit Umweltschäden einhergeht, bezogen werden).

Die Häufigkeit des gefährlichen Vorfalls *f* setzt sich in diesem Fall aus drei beeinflussenden Faktoren zusammen:

– der Häufigkeit und Aufenthaltsdauer im Gefahrenbereich;
– der Möglichkeit, den gefährlichen Vorfall zu vermeiden;
– der Wahrscheinlichkeit des Auftretens des gefährlichen Vorfalls ohne das Vorhandensein irgendeines sicherheitsbezogenen Systems (jedoch mit anderen Einrichtungen zur Risikominderung) – dieses wird als die „Wahrscheinlichkeit eines unerwünschten Ereignisses“ bezeichnet.

Dies führt zu den folgenden vier Risikoparametern:

– Auswirkung des gefährlichen Vorfalls (*C*);
– Häufigkeit und Aufenthaltsdauer im Gefahrenbereich (*F*);
– Möglichkeit, den gefährlichen Vorfall zu vermeiden (*P*);
– Wahrscheinlichkeit des unerwünschten Ereignisses (*W*).

Die Risikoparameter können auf einer qualitativen Grundlage wie in Tabelle E.1 oder auf einer quantitativen wie in Tabelle E.2 festgelegt werden. Zur Festlegung der numerischen Werte im Zusammenhang mit jedem Parameter der Tabelle E.2 ist eine Kalibrierung erforderlich.

E.3 Kalibrierung

Die Ziele der Kalibrierung sind wie folgt:

– die Beschreibung aller Parameter in einer Weise, die es dem SIL-Bewertungs-Team ermöglicht, auf der Grundlage der Merkmale der Anwendung eine objektive Entscheidung zu treffen;

– die Sicherstellung, dass die SIL-Auswahl für eine Anwendung im Einklang mit den firmeninternen Risikokriterien steht und Berücksichtigung der Risiken aus anderen Quellen;

– es zu ermöglichen, den Prozess der Parameterauswahl zu verifizieren.

Die Kalibrierung des Risikographen ist das Verfahren der Zuordnung von numerischen Werten zu den Parametern des Risikographen. Dies bildet die Grundlage für die Beurteilung des vorhandenen Prozessrisikos und erlaubt die Bestimmung der erforderlichen Integrität der betrachteten sicherheitstechnischen Funktion. Jedem der Parameter wird eine Reihe von Werten zugeordnet, in Kombination angewandt ergeben sie eine abgestufte Bewertung des Risikos, das ohne die jeweilige Sicherheitsfunktion vorhanden ist. So wird ein Maß für den Grad des Vertrauens, das in die Sicherheitsfunktion zu setzen ist, bestimmt. Der Risikograph stellt Beziehungen zwischen einzelnen Kombinationen von Risikoparametern und den Sicherheits-Integritätsleveln her. Die Beziehung zwischen den Kombinationen der Risikoparameter und den Sicherheits-Integritätsleveln wird durch die Berücksichtigung des für bestimmte Gefährdungen tolerierbaren Risikos erreicht.

Bei der Betrachtung der Kalibrierung des Risikographen ist es wichtig, die Anforderungen in Bezug auf das Risiko, die sowohl aus den Erwartungen der Eigentümer als auch den Anforderungen der Behörden herrühren, in Betracht zu ziehen. Die Risiken für das Leben können in einer Reihe von Möglichkeiten, wie in A.2 und Anhang C beschrieben, betrachtet werden.

Falls es notwendig ist, die Häufigkeit eines einzelnen Todesfalls auf ein bestimmtes Maximum zu reduzieren, dann kann nicht davon ausgegangen werden, dass die gesamte Risikominderung einem einzigen sicherheitsbezogenen E/E/PE-System übertragen werden kann. Die exponierten Personen sind einem breiten Spektrum von Risiken ausgesetzt, die sich aus anderen Quellen (z. B. Sturz-, Brand- und Explosionsgefahren) ergeben. Bei der Kalibrierung sind die Zahl der Gefährdungen, denen einzelne Personen ausgesetzt sind, und die gesamte Zeit der Gefährdungsdauer zu berücksichtigen.

Bei der Betrachtung des erforderlichen Ausmaßes der Risikominderung kann eine Organisation Kriterien in Bezug auf die zusätzlichen Kosten für die Verhinderung eines Todesfalls haben. Dies kann durch Division der jährlichen Kosten der für ein höheres Maß an Integrität erforderlichen zusätzliche Hardware- und Ingenieurleistung durch die zusätzliche Risikominderung berechnet werden. Eine weitere Ebene der Integrität ist gerechtfertigt, wenn die zusätzlichen Kosten für die Vermeidung eines Todesfalls geringer sind als ein bestimmter Betrag.

Die oben genannten Fragen sind zu berücksichtigen, bevor die Parameterwerte festgelegt werden können. Die meisten der Parameter sind einem Wertebereich zugeordnet (z. B. wenn die erwartete Anforderungsrate für einen bestimmten Prozess zwischen einem Dekadenbereich je Jahr liegt, dann kann W3 verwendet werden). In gleicher Weise würde für Anforderungen im unteren Dekadenbereich W2 gelten und für Anforderungen im nächstunteren Dekadenbereich W1. Die Zuweisung der einzelnen Parameter zu einem bestimmten Bereich unterstützt das Team bei der Auswahl des Parameterwerts für eine bestimmte Anwendung. Um den Risikographen zu kalibrieren, werden den Parametern Werte oder Wertebereiche zugewiesen. Das jeder Parameterkombinationen zugeordnete Risiko wird dann gegenüber den definierten Risikokriterien beurteilt. Die Parameterbeschreibungen werden dann angepasst, so dass für alle Kombinationen aller Parameterwerte die definierten Risikokriterien erreicht werden. In der Beispielkalibrierung der Tabelle E.2 wird ein Faktor „D“ eingeführt, um den Bereich der Anforderungsraten im Zusammenhang mit jedem W-Faktor so anzupassen, dass ein tolerierbares Risiko erreicht wird. In einigen Fällen sollten Bereiche, die anderen Risikofaktoren zugeordnet sind, angepasst werden, um den Parameterwerten in der Breite der zu berücksichtigen Anwendungen gerecht zu werden. Die Kalibrierung ist ein iterativer Prozess und wird solange fortgesetzt, bis die spezifizierten Risikoakzeptanzkriterien für alle Kombinationen von Parameterwerten erfüllt sind.

Die Kalibrierung ist nicht bei jeder SIL-Bestimmung für eine spezielle Anwendung erneut durchzuführen. Diese Arbeit ist in der Regel für Organisationen für ähnliche Gefährdungen nur einmal notwendig. Anpassungen können für bestimmte Projekte notwendig werden, wenn sich die ursprünglichen Annahmen, die während der Kalibrierung gemacht wurden, als für diese ungültig herausstellen sollten.

Wo Parameterzuweisungen getroffen werden, sollten Informationen zur Verfügung stehen, wie diese Werte hergeleitet wurden.

Es ist wichtig, dass dieser Prozess der Kalibrierung mit einer höheren Ebene innerhalb der Organisation, die die Verantwortung für die Sicherheit trägt, abgestimmt wird. Die getroffenen Entscheidungen bestimmen die erreichte Gesamtsicherheit.

In der Regel wird es für einen Risikographen schwierig sein, die Möglichkeit abhängiger Ausfälle zwischen den Quellen einer Anforderung und der verwendeten Ausrüstung des sicherheitsbezogenen E/E/PE-Systems zu berücksichtigen. Dies kann daher zu einer Überschätzung der Wirksamkeit des sicherheitsbezogenen E/E/PE-Systems führen. Wenn Risikographen kalibriert werden, um höhere Anforderungsraten als einmal je Jahr zu beinhalten, können die SIL-Anforderungen, die sich aus der Verwendung des Risikographen ergeben, höher als notwendig sein, und es wird die Verwendung anderer Verfahren empfohlen.

E.4 Mögliche andere Risikoparameter

Die oben festgelegten Risikoparameter werden als ausreichend allgemeingültig betrachtet, um einen weiten Anwendungsbereich abzudecken. Es können jedoch Anwendungen existieren, die Aspekte enthalten, die die Einführung zusätzlicher Risikoparameter erforderlich machen, zum Beispiel die Verwendung neuer Technologien in dem EUC-Leit- oder Steuerungssystem. Der Zweck zusätzlicher Parameter wäre eine genauere Einschätzung der notwendigen Risikominderung (siehe Bild A.1).

E.5 Anwendung des Risikographen – Allgemeines Schema

Die Kombination der oben beschriebenen Risikoparameter ermöglicht es, einen Risikographen wie in Bild E.1 zu entwickeln. Bezogen auf Bild E.1 gilt:

$$C_A < C_B < C_C < C_D;\ F_A < F_B;\ P_A < P_B;\ W_1 < W_2 < W_3.$$

Erklärung des Risikographen:

– Die Verwendung der Risikoparameter C, F und P führt zu einer Anzahl von Ergebnissen X_1, X_2, X_3... X_n (die genaue Anzahl hängt von dem vom Risikographen abzudeckenden besonderen Anwendungsgebiet ab). Bild E.1 zeigt die Situation ohne zusätzliche Wichtung für ernsthaftere Auswirkungen. Jedes Einzelergebnis ist auf eine von drei Skalen abgebildet (W_1, W_2 und W_3). Jeder Punkt dieser Skalen ist ein Anhaltspunkt für die erforderliche Sicherheitsintegrität, die durch das betrachtete sicherheitsbezogene E/E/PE-System erreicht werden muss. In der Praxis gibt es Situationen, in denen für bestimmte Auswirkungen ein einzelnes sicherheitsbezogenes E/E/PE-System nicht ausreicht, um die notwendige Risikominderung zu gewährleisten.

– Die Abbildung auf W_1, W_2 oder W_3 lässt einen Beitrag anderer Maßnahmen zur Risikominderung zu. Die Verschiebung der Skalen für W_1, W_2 oder W_3 erlaubt es, drei unterschiedliche Stufen zur Risikominderung durch andere Maßnahmen zu berücksichtigen. Das bedeutet, dass die Skala W_3 für einen kleinsten Beitrag durch andere Maßnahmen zur Risikominderung steht (d. h., die höchste Wahrscheinlichkeit, dass das unerwünschte Ereignisses stattfindet), die Skala W_2 für einen mittleren Beitrag und die Skala W_1 für einen höchsten Beitrag. Für ein bestimmtes Zwischenergebnis des Risikographen (d. h. X_1, X_2... oder X_6) und für ein bestimmtes Maß von W (d. h. W_1, W_2 oder W_3) gibt das Endergebnis des Risikographen den Sicherheits-Integritätslevel des sicherheitsbezogenen E/E/PE-Systems (d. h. 1, 2, 3 oder 4) an und ist ein Maß für die geforderte Risikominderung durch dieses System. Zusammen mit den Risikominderungen anderer Maßnahmen, die durch den Mechanismus der W-Skalen berücksichtigt werden (z. B. durch sicherheitsbezogene Systeme anderer Technologie und andere Maßnahmen zur Risikominderung), liefert diese Risikominderung die für die bestimmte Situation notwendige Risikominderung.

Es kann notwendig sein, die in Bild E.1 aufgezeigten Parameter (C_A, C_B, C_C, C_D, F_A, F_B, P_A, P_B, W_1, W_2, W_3) und ihre Gewichtungen für jede bestimmte Situation oder jeden bestimmten Bereich vergleichbarer Industrien

genau festzulegen. Außerdem kann es notwendig sein, diese in anwendungsbezogenen Internationalen Normen festzulegen.

E.6 Beispiel eines Risikographen

Ein Beispiel der Anwendung des Risikographen, das auf den Beispieldaten in Tabelle E.1 beruht, ist in Bild E.2 dargestellt. Die Verwendung der Risikoparameter *C*, *F* und *P* führt zu einem von acht Ergebnissen. Jedes einzelne Ergebnis ist auf eine von drei Skalen abgebildet (W_1, W_2 und W_3). Jeder Punkt auf diesen Skalen (a, b, c, d, e, f, g und h) ist ein Anhaltspunkt für die notwendige Risikominderung, die durch das sicherheitsbezogene System erreicht werden muss.

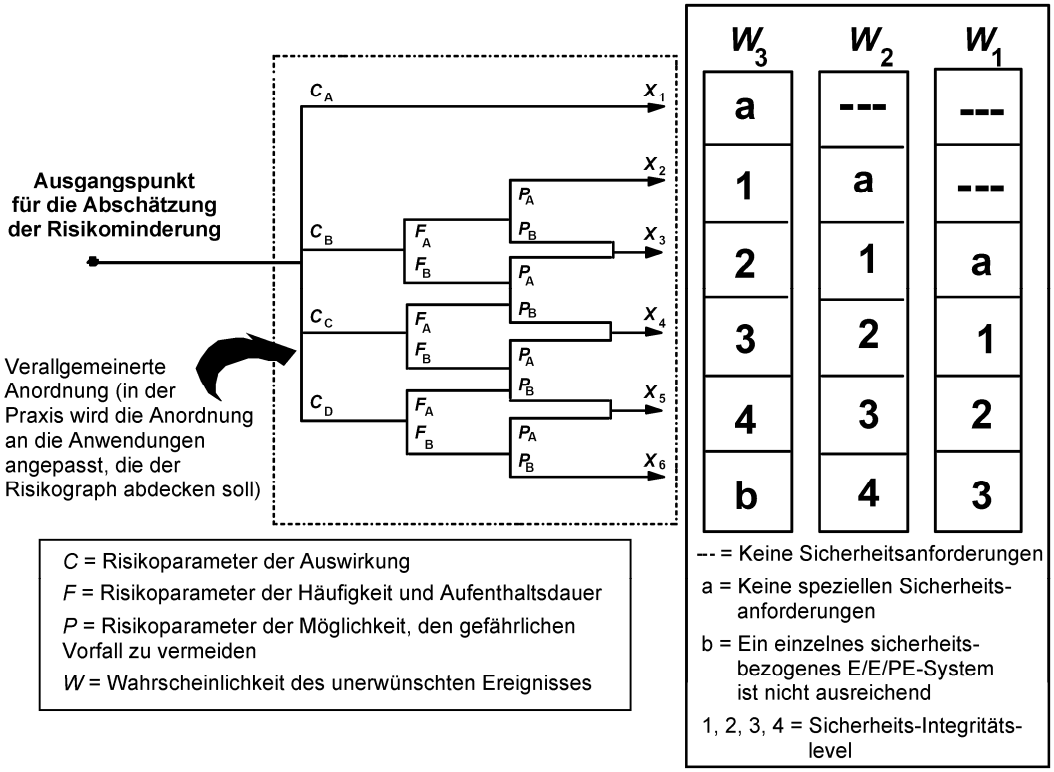
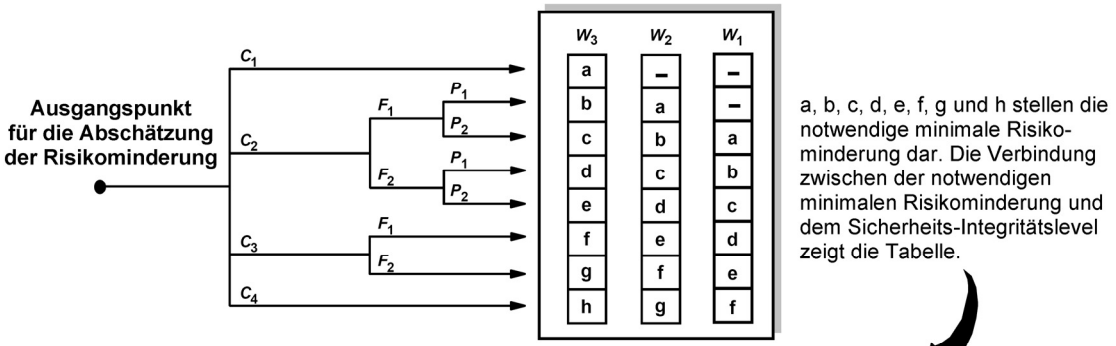


Bild E.1 – Risikograph: Allgemeine Darstellung



C = Risikoparameter der Auswirkung

F = Risikoparameter der Häufigkeit und Aufenthaltsdauer

P = Risikoparameter der Möglichkeit, den gefährlichen Vorfall zu vermeiden

W = Wahrscheinlichkeit des unerwünschten Ereignisses

a, b, c ... h = Abschätzung der notwendigen Risikominderung für die sicherheitsbezogenen Systeme

Notwendige minimale Risikominderung	Sicherheits-Integritätslevel
–	Keine Sicherheitsanforderungen
a	Keine speziellen Sicherheitsanforderungen
b, c	1
d	2
e, f	3
g	4
h	Ein sicherheitsbezogenes E/E/PE-System ist nicht ausreichend

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

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

Risikoparameter		Klassifizierung	Erläuterungen
Auswirkung (*C*)	C_1	Geringe Verletzung	1 Das Klassifizierungssystem ist entwickelt worden, um Verletzungen und Tod von Personen zu berücksichtigen. Für Umwelt- und Materialschäden müssten andere Klassifizierungsverfahren entwickelt werden
	C_2	Schwere irreversible Verletzung einer oder mehrerer Personen; Tod einer Person	2 Bei der Interpretation von C_1, C_2, C_3 und C_4 müssen die Auswirkungen des Unfalls und normale Heilungsprozesse betrachtet werden
	C_3	Tod mehrerer Personen	
	C_4	Tod sehr vieler Personen	
Häufigkeit und Aufenthaltsdauer im gefährlichen Bereich (*F*)	F_1	Seltener bis häufiger Aufenthalt im gefährlichen Bereich	3 Siehe Anmerkung 1 oben
	F_2	Häufiger bis dauernder Aufenthalt im gefährlichen Bereich	
Möglichkeit, den gefährlichen Vorfall zu vermeiden (*P*)	P_1	Möglich unter bestimmten Bedingungen	4 Dieser Parameter zieht in Betracht – Betrieb eines Prozesses (überwacht (d. h. bedient durch ausgebildete oder nicht ausgebildete Personen) oder nicht überwacht); – Geschwindigkeit der Entwicklung des gefährlichen Vorfalls (z. B. plötzlich, schnell, langsam); – Leichtigkeit der Erkennung der Gefahr (z. B. unmittelbar erkennbar, durch technische Maßnahmen aufgedeckt, ohne technische Maßnahmen aufgedeckt); – Vermeidung des gefährlichen Vorfalls (z. B. Fluchtwege möglich, nicht möglich oder unter bestimmten Bedingungen möglich); – aktuelle Sicherheitserfahrung (diese Erfahrung kann von identischen oder ähnlichen EUC oder ähnlichen EUC herrühren, oder kann nicht vorhanden sein).
	P_2	Beinahe unmöglich	
Wahrscheinlichkeit des unerwünschten Ereignisses (*W*)	W_1	Eine sehr geringe Wahrscheinlichkeit, dass die unerwünschten Ereignisse auftreten, und nur wenige unerwünschte Ereignisse sind wahrscheinlich	5 Der Faktor „*W*“ dient zur Bestimmung der Häufigkeit des unerwünschten Ereignisses, ohne die Berücksichtigung jeglicher sicherheitsbezogener Systeme (E/E/PE oder andere Technologie), aber unter Berücksichtigung jeder anderen Maßnahme zur Risikominderung 6 Wenn wenig oder gar keine Erfahrungen mit der EUC oder einem ähnlichen EUC oder EUC-Leit- oder Steuerungssystem bestehen, kann die Bestimmung des Faktors „*W*“ durch Berechnung erfolgen. In solchen Fällen muss eine „Worst Case“-Vorhersage gemacht werden
	W_2	Eine geringe Wahrscheinlichkeit, dass die unerwünschten Ereignisse auftreten, und wenige unerwünschte Ereignisse sind wahrscheinlich	
	W_3	Eine relativ hohe Wahrscheinlichkeit, dass die unerwünschten Ereignisse auftreten, und häufige unerwünschte Ereignisse sind wahrscheinlich	

Tabelle E.2 – Beispiel einer Kalibrierung des allgemeinen Risikographen

Risikoparameter		Klassifizierung	Kommentar
Auswirkung (*C*) Anzahl der Todesopfer Lässt sich aus der mittleren Anzahl der anwesenden Personen berechnen, die bei Aufenthalt im Gefahrenbereich einer Gefährdung ausgesetzt sind, multipliziert mit dem Grad ihrer Verletzbarkeit durch die betreffende Gefahr. Aufgrund der Art der Gefährdung können folgende Faktoren für die Verletzbarkeit verwendet werden: V = 0,01 bei kleiner Emission brennbarer/toxischer Stoffe V = 0,1 bei großer Emission brennbarer/toxischer Stoffe V = 0,5 wie oben, bei gleichzeitig hoher Wahrscheinlichkeit einer Zündung oder bei stark toxischen Stoffen V = 1 Bersten oder Explosion	C_A C_B C_C C_D	Geringe Verletzung Bereich 0,01 bis 0,1 Bereich > 0,1 bis 1,0 Bereich > 1,0	1 Diese Klassifizierung wurde für Verletzungen und Todesfälle entwickelt. 2 Bei der Interpretation der Kategorien C_A, C_B, C_C und C_D sind die Unfallfolgen und ein normaler Heilungsprozess zu berücksichtigen.
Aufenthaltswahrscheinlichkeit (*F*) Diese berechnet sich aus dem Anteil der Zeit, in dem sich Personal während der normalen Arbeitszeit im gefährdeten Bereich aufhält ANMERKUNG 1 Sollte die Aufenthaltsdauer im gefährdeten Bereich von der Schicht abhängen, ist jeweils das Maximum anzusetzen. ANMERKUNG 2 Die Kategorie FA darf nur verwendet werden, wenn gezeigt werden kann, dass die Anforderungsrate zufällig ist und nicht mit einer höheren Besetzung durch Personal zusammenhängt. Letzteres ist im Allgemeinen der Fall beim Anfahren der Anlage oder bei der Störungssuche.	F_A F_B	Seltener bis etwas öfterer Aufenthalt in der gefährdeten Zone. Aufenthaltswahrschein-lichkeit < 0,1 Häufiger bis andauernder Aufenthalt in der gefährdeten Zone	3 Siehe oben Kommentar 1
Wahrscheinlichkeit (*P*), mit der das gefährliche Ereignis vermieden werden kann, auch wenn die Schutzeinrichtungen versagen.	P_A P_B	Trifft zu, wenn alle Bedingungen in Spalte 4 erfüllt werden. Trifft zu, wenn nicht alle Bedingungen in Spalte 4 erfüllt werden.	4 P_A sollte nur verwendet werden, wenn folgende Aussagen zutreffen: – Einrichtungen sind vorhanden, die beim Ausfall des sicherheitsbezogenen E/E/PE-Systems den Bediener alarmieren; – unabhängige Einrichtungen zum Abfahren sind vorhanden, so dass die Gefährdung vermieden werden kann, oder es existieren Einrichtungen, mit deren Hilfe alle Personen in einen sicheren Bereich fliehen können; – die Zeit, die nach Alarmierung des Operateurs bis zum Eintreten der Gefährdung verstreicht, übersteigt eine Stunde oder reicht sicher für die erforderlichen Tätigkeiten aus.

Tabelle E.2 *(fortgesetzt)*

Risikoparameter		Klassifizierung	Kommentar
Anforderungsrate (W): Anzahl gefährlicher Ereignisse je Jahr bei Abwesenheit des SIS Zur Bestimmung der Anforderungsrate werden alle Ausfallursachen betrachtet, die zu einer bestimmten Gefährdung führen können. Dabei können Betriebseinrichtungen in begrenztem Umfang in die Berechnung einbezogen werden. Im Falle dass Betriebseinrichtungen oder deren Instandhaltung nicht der IEC 61511 entsprechen, ist deren Leistungsfähigkeit geringer als nach SIL 1 anzusetzen.	W_1	Anforderungsrate weniger als 0,1 D je Jahr	5 Der Zweck des Faktors W besteht in der Abschätzung, wie häufig eine Gefährdung ohne Einrichtung eines sicherheitsbezogenen E/E/PE-Systems stattfinden würde. Bei einer sehr hohen Anforderungsrate muss das SIL auf eine andere Weise festgelegt oder der Risikograph neu kalibriert werden. Es sollte angemerkt werden, dass der Risikograph für Anwendungen in der Betriebsart mit kontinuierlicher Anforderung möglicherweise nicht die beste Methode ist (siehe IEC 61508-4, 3.5.16).
	W_2	Anforderungsrate zwischen 0,1 D und D je Jahr	6 D ist ein Kalibrierfaktor, dessen Wert so bestimmt werden sollte, dass der Risikograph zu einem für die dem Risiko ausgesetzten Personen tolerierbaren Restrisiko führt, unter Berücksichtigung weiterer Risiken, denen sie ausgesetzt sind, und von unternehmenseigenen Kriterien.
	W_3	Anforderungsrate zwischen D und 10 D je Jahr Für Anforderungsraten über 10 D je Jahr ist eine höhere Integrität erforderlich.	

ANMERKUNG Dieses Beispiel zeigt die Anwendung der Prinzipien auf den Entwurf eines Risikographen. Risikographen für bestimmte Anwendungen und besondere Gefährdungen müssen mit den Beteiligten unter Berücksichtigung des tolerierbaren Risikos abgestimmt werden, siehe Abschnitte E.1 bis E.6.

Anhang F
(informativ)

Semi-quantitative Methode, die eine Analyse der Schutzebenen (LOPA) verwendet

F.1 Allgemeines

F.1.1 Beschreibung

Dieser Anhang beschreibt eine Methode, die Analyse der Schutzebenen (LOPA, en: layer of protection analysis) genannt wird. Er ist nicht als eine endgültige Beschreibung der Methode, sondern zur Erläuterung der allgemeinen Prinzipien vorgesehen

F.1.2 Hinweise

Dieser Anhang stützt sich auf eine Methode, die im Detail in einer AIChE-Veröffentlichung beschrieben ist (siehe [8] in den Literaturhinweisen). Sie zeigt viele Möglichkeiten zur Anwendung des LOPA-Verfahrens.

In einem Ansatz werden alle relevanten Parameter zur nächsthöheren Zehner-Potenz aufgerundet (z. B. wird eine Wahrscheinlichkeit von $5 \cdot 10^{-2}$ auf 10^{-1} aufgerundet). Dies ist ein sehr konservativer Ansatz und kann zu deutlich höheren SILs führen. Unsicherheiten von Daten jedoch sollten durch Rundung aller Parameterwerte auf die nächst höhere signifikante Zahl (z. B. sollte $5{,}4 \cdot 10^{-2}$ gerundet werden auf $6 \cdot 10^{-2}$) berücksichtigt werden

F.1.3 Beschreibung der Methode

LOPA analysiert Gefährdungen, um festzustellen, ob Sicherheitsfunktionen erforderlich sind, und wenn ja, für jede den erforderlichen SIL . Um die LOPA-Methode anwenden zu können, ist eine Anpassung an die Risiko-Akzeptanzkriterien notwendig. Das Verfahren beginnt mit den Daten, die bei der Identifikation der Gefährdungen ermittelt worden sind, und berücksichtigt jede ermittelte Gefährdung durch Dokumentation der auslösenden Ursachen und der Schutzebenen, die diese vermeiden oder den damit verbundenen Schaden begrenzen sollen. Der Gesamtbetrag der Risikominderung kann dann bestimmt und die Notwendigkeit einer weiteren Risikominderung analysiert werden. Wenn eine zusätzliche Risikominderung erforderlich ist und wenn diese in Form eines sicherheitsbezogenen E/E/PE-Systems erfolgt, ermöglicht die LOPA-Methode die Bestimmung des geeigneten SIL. Für jede Gefährdung wird ein geeigneter SIL zur Verringerung der Risiken auf ein tolerierbares Niveau bestimmt. Die nachfolgende Tabelle F.1 zeigt ein typisches LOPA-Format.

F.2 Schadensereignis

Unter Verwendung der Tabelle F.1 wird jede Beschreibung eines Schadensereignisses (Auswirkung), bestimmt durch die Identifikation der Gefährdung, in Tabelle F.1, Spalte 1, eingetragen.

F.3 Schweregrad

Der Schweregrad des Ereignisses wird in Tabelle F.1, Spalte 2, eingetragen. Der Schweregrad wird aus einer Tabelle abgeleitet, die allgemeine Auswirkungsstufen beschreibt, z. B. gering, ernst, katastrophal, mit bestimmten Bereichen der Auswirkung und der maximalen Häufigkeit für jeden Schweregrad. Als Ergebnis legt diese Tabelle Anwender-Toleranzkriterien fest. Es werden Informationen benötigt, die es erlauben, zu Ereignissen mit Auswirkungen für Sicherheit und Umwelt den Schweregrad und die maximale Häufigkeit zu bestimmen.

F.4 Auslösende Ursache

Alle auslösenden Ursachen des Schadensereignisses werden in Tabelle F.1, Spalte 3, eingetragen. Schadensereignisse können viele auslösende Ursachen haben und alle sollten aufgeführt werden.

F.5 Eintrittswahrscheinlichkeit

Die Wahrscheinlichkeitswerte jeder der in Tabelle F.1, Spalte 3, eingetragenen auslösenden Ursachen werden in Ereignissen je Jahr in Tabelle F.1, Spalte 4, eingegeben.

Die Eintrittswahrscheinlichkeit kann durch allgemeine Daten der Ausfallraten der Ausrüstung und der Kenntnis der Intervalle der Wiederholungsprüfungen berechnet werden, oder durch Aufzeichnungen über die Einrichtung. Eine geringe Eintrittswahrscheinlichkeit sollte nur verwendet werden, wenn es ausreichende statistische Grundlagen für die Daten gibt.

Tabelle F.1 – LOPA-Dokumentationsblatt

a)	1	2	3	4	5			6	7	8	9	10	11
					Schutzebenen (PLs)								
	Beschreibung des Schadensereignisses F.2	Schweregrad F.3	Auslösende Ursache F.4	Eintrittswahrscheinlichkeit F.5	Allgemeiner Entwurf F.6.1	Steuerungssystem F.6.2	Alarme, usw. F.6.3	Zusätzliche Schadensbegrenzungsmaßnahmen, beschränkter Zugang F.7	Zusätzliche Schadensbegrenzungsmaßnahmen F.8	Vorläufige Wahrscheinlichkeit für das Ereignis F.9	PFD_{avg} erforderlich für das E/E/PES (und SIL) F.10	Tolerierbare Wahrscheinlichkeit des Ereignisses mit Schadensbegrenzung F.11	Anmerkungen
1	Überdrehzahl des Rotors führt zum Bruch des Gehäuses	Verlust des Lebens von Personen, die sich in der Nähe des Gehäuses befinden, Todesfälle überschreiten nicht 2	Geschwindigkeitsregelung ausgefallen	0,1	1	1	1	0,1	0,1	10^{-3}	$5 \cdot 10^{-3}$ (SIL 2 mit einer minimalen PFD_{avg} von $5 \cdot 10^{-3}$)	10^{-5}	
			Lastabwurf	1	1	0,1	1	0,1	0,1	10^{-3}			
			Ausfall der Kupplung	0,1	1	0,1	1	0,1	0,1	10^{-4}			
						0,1 Vertrauen an das Steuerungssystem		Aufenthaltsdauer begrenzt, 90 % der Zeit keine Personen anwesend	Todesfall tritt nur ein, wenn Personen von Bruchstücken getroffen werden	Gesamt $2{,}1 \cdot 10^{-3}$		Tolerierbare Häufigkeit, sofern nicht mehr als 5 Todesfälle	

Tabelle F.1 *(fortgesetzt)*

[a]	1	2	3	4	5	6	7	8	9	10	11
					Schutzebenen (PLs)						
2	Wiederholung des obigen Falls zu Umweltrisiken										
3				Fortsetzung bei Bedarf							
.											
.											
N											

ANMERKUNG 1 Der Schweregrad kann eingeteilt werden in C = (katastrophal, en:catastrophic), E = (ausgedehnt, en: extensive), S = (ernsthaft, en: serious) oder M = (gering, en: minor). Die tolerierbare Wahrscheinlichkeit des Ereignisses mit Schadensbegrenzung hängt ab vom Schweregrad.

ANMERKUNG 2 Die Einheiten in den Spalten 3, 8 und 10 sind Ereignisse je Jahr.

ANMERKUNG 3 Die Einheiten in den Spalten 4 – 7 und 9 sind dimensionslos. Die Zahlenwerte zwischen 0 und 1 sind Faktoren, mit denen die Wahrscheinlichkeit multipliziert werden kann, um die Schadensbegrenzung der zugehörigen Schutzebene darzustellen. So bedeutet 1 keinen mindernden Effekt und 0,1 ist der Faktor der Risikominderung um 10.

[a] Für die angegebenen Spalten- und Zeilennummern sind weitere Beschreibungen in Anhang F enthalten.

F.6 Schutzebenen (PLs)

F.6.1 Allgemeines

Jede Schutzebene besteht aus einer Gruppe von Einrichtungen und/oder organisatorischen Maßnahmen, die von anderen Schichten unabhängig funktionieren.

Die Eigenschaften des Entwurfs zur Verringerung der Wahrscheinlichkeit eines Schadensereignisses, für das bereits eine auslösende Ursache aufgetreten ist, werden zuerst in die Tabelle F.1, Spalte 5, geschrieben.

Die Schutzebenen sollten folgende wichtigen Merkmale aufweisen:

– konkret sein: Eine Schutzebene ist darauf ausgelegt, vor einem bestimmten, möglicherweise gefährlichen Ereignis zu schützen oder dessen Auswirkungen zu begrenzen (z. B. eine Durchgehreaktion, Entweichen giftiger Stoffe, Produktaustritt oder Feuer). Mehrere Ursachen können zu demselben gefährlichen Ereignis führen, und deshalb können mehrere Ereignisszenarien ein Eingreifen der Schutzebene auslösen.

– Wirksamkeit: Ein Schutzebene muss allein in der Lage sein, das Auftreten des Ereignisses zu verhindern, wenn alle anderen Maßnahmen vollständig versagt haben.

– Unabhängigkeit: Eine Schutzebene ist unabhängig von den anderen Schutzebenen im Zusammenhang mit dem festgestellten gefährlichen Vorfall.

– Zuverlässigkeit: Es ist davon auszugehen, dass eine Schutzebene das tun wird, wofür sie ausgelegt wurde, dadurch, dass während der Planung sowohl zufällige als auch systematische Fehler berücksichtigt wurden.

– Prüfbarkeit: Eine Schutzebene ist dafür ausgelegt, eine regelmäßige Validierung ihrer Schutzfunktionen zu erleichtern. Wiederholungsprüfungen und die Instandhaltung des Sicherheitssystems sind erforderlich.

F.6.2 Leit- oder Steuerungssystem

Der nächste Punkt in der Tabelle F.1, Spalte 5, ist das EUC-Leit- oder Steuerungssystem. Wenn eine Steuerungsfunktion das Auftreten eines Schadensereignisses verhindert, wenn die auslösende Ursache auftritt, dann wird das Vertrauen auf der Grundlage ihrer PFD_{avg} in Anspruch genommen. Es sollte kein Vertrauen für eine Steuerungsfunktion geltend gemacht werden, wenn ihr Ausfall zu einer Anforderung an das sicherheitsbezogene E/E/PE-System führen würde. Es sollte auch darauf hingewiesen werden, dass die für eine Steuerungsfunktion beanspruchte PFD_{avg} auf das Minimum von 0,1 begrenzt werden sollte, wenn die Steuerungsfunktion nicht als Sicherheitssystem entworfen wurde und als solches betrieben wird.

F.6.3 Alarme

Der letzte Punkt in der Tabelle F.1, Spalte 5, nimmt das Vertrauen in Alarme, die den Bediener zum Eingreifen veranlassen, in Anspruch. Vertrauen in Alarme sollte nur unter folgenden Umständen geltend gemacht werden:

– Die verwendete Hardware- und Software ist getrennt und unabhängig von der des Steuerungssystems (z. B. sollten Eingangskarten und Prozessoren nicht gemeinsam verwendet werden).

– Der Alarm wird mit einer hohen Priorität in einer ständig besetzten Stelle angezeigt. Vertrauen in einen Alarm sollte die folgenden Aspekte berücksichtigen:

  – Die Wirksamkeit eines Alarms hängt von der Komplexität der Aufgabe ab, die durchgeführt werden soll, falls der Alarm auftritt, und den anderen Aufgaben, die zur gleichen Zeit durchgeführt werden müssen.

  – Das Vertrauen sollte auf ein Mindestmaß der PFD_{avg} von 0,1 beschränkt werden.

  – Der Bediener benötigt genügend Zeit und unabhängige Einrichtungen, um die Gefährdung zu beenden. Normalerweise sollte kein Vertrauen geltend gemacht werden, wenn die Zeit zwischen dem Alarm und der Gefährdung nicht mehr als 20 Minuten beträgt.

F.7 und F.8 Zusätzliche Schadensbegrenzungsmaßnahmen

Schadensbegrenzungsebenen sind üblicherweise mechanischer oder bautechnischer Art oder können in Form einer Verfahrensanweisung vorliegen. Beispiele beinhalten:

– Zugangsbeschränkungen;
– Reduzierung der Wahrscheinlichkeit einer Entzündung;
– alle anderen Faktoren, die die Verletzbarkeit von Personen, die einer Gefährdung aussetzt sind, verringern.

Schadensbegrenzungsebenen können die Schwere der Auswirkungen des Schadensereignisses mildern, aber nicht verhindern, dass das Ereignis auftritt. Beispiele sind:

– Flutungssysteme im Fall eines Brandes;
– Gasalarme;
– Evakuierungsmaßnahmen, die zu einer Verringerung der Wahrscheinlichkeit führen, dass Personen einem sich entwickelnden Ereignis ausgesetzt sind.

Bei der Schadensbegrenzung kann die anteilige Aufenthaltsdauer der am stärksten exponierten Personen in der Gefahrenzone berücksichtigt werden. Diese sollte durch die Festlegung der Anzahl der Stunden in der Gefahrenzone je Jahr, geteilt durch 8760 h, bestimmt werden.

Die angemessene PFD_{avg} oder gleichwertiges sollte für alle Schadensbegrenzungsebenen bestimmt und in Tabelle F.1, Spalte 6 und 7, eingetragen werden.

F.9 Vorläufige Wahrscheinlichkeit für das Ereignis

Die vorläufige Wahrscheinlichkeit für das Ereignis wird durch die Multiplikation der folgenden Faktoren berechnet und das Ergebnis als Häufigkeit je Jahr in die Spalte 8 der Tabelle F.1 eingetragen:

– die Verletzbarkeit der am stärksten exponierten Person;
– die Eintrittswahrscheinlichkeit (Spalte 4);
– die PFD_{avg} der Schutzebenen und Schadensbegrenzungsebenen (Spalten 5, 6 und 7).

Die gesamte vorläufige Ereignishäufigkeit sollte durch Addition der vorläufigen Ereignishäufigkeiten jeder Ursache berechnet werden.

Die gesamte vorläufige Ereignishäufigkeit sollte mit der tolerierbaren Risikohäufigkeit für den damit verbundenen Schweregrad verglichen werden. Wenn die gesamte vorläufige Ereignishäufigkeit über der tolerierbaren Risikohäufigkeit liegt, ist eine Risikominderung erforderlich. Lösungen durch sichere Konstruktion sollten in Erwägung gezogen werden, bevor zusätzliche Schutzebenen in Form von sicherheitsbezogenen E/E/PE-Systemen zum Einsatz kommen.

Wenn die Zahlen der vorläufigen Wahrscheinlichkeit für das Ereignis nicht unter das maximale Häufigkeitskriterium reduziert werden können, wird ein sicherheitsbezogenes E/E/PE-System erforderlich.

F.10 Sicherheits-Integritätslevel (SILs)

Wenn eine Sicherheitsfunktion erforderlich ist, kann der erforderliche SIL wie folgt bestimmt werden:

– Zur Bestimmung der erforderlichen PFD_{avg} wird die maximale Häufigkeit des damit verbundenen Schweregrads durch den Gesamtwert der vorläufigen Wahrscheinlichkeit für das Ereignis dividiert.
– Der numerische Grenzwert der PFD_{avg} kann dann in der Spezifikation der Sicherheitsanforderungen zusammen mit dem zugehörigen SIL verwendet werden. Der zugehörige SIL kann aus IEC 61508-1, Tabelle 2, entnommen werden.
– Wenn der numerische Wert der PFD_{avg} nicht in der Prozess-Anforderungsspezifikation angegeben werden soll, sondern nur der erforderliche SIL, dann sollte dieser einen Level höher sein, so dass eine angemessene Risikominderung mit allen Werten der PFD_{avg} im Zusammenhang mit dem angegebenen SIL erreicht werden kann.

Wenn die für das tolerierbare Risiko erforderliche PFD_{avg} größer oder gleich 0,1 ist, dann wird die Funktion der Einstufung „Keine besonderen Anforderungen an die Sicherheitsintegrität“ zugeordnet.

F.11 Tolerierbare Wahrscheinlichkeit des Ereignisses mit Schadensbegrenzung

Die tolerierbare Wahrscheinlichkeit des Ereignisses mit Schadensbegrenzung wird von dem Schweregrad der Auswirkungen abhängen. Dies wird von den verabschiedeten akzeptierten Risikokriterien abhängen (siehe A.2 für tolerierbare Risikokriterien).

Anhang G
(informativ)

Festlegung der Sicherheits-Integritätslevel – Eine qualitative Vorgehensweise – Matrix des Ausmaßes des gefährlichen Vorfalls

G.1 Allgemeines

Die in Anhang D beschriebene numerische Methode kann nicht angewendet werden, wenn das Risiko (oder dessen Anteil „Häufigkeit“) nicht quantifiziert werden kann. Dieser Anhang beschreibt die qualitative Methode „Matrix des Ausmaßes des gefährlichen Vorfalls“, die es ermöglicht, die Festlegung des Sicherheits-Integritätslevels eines sicherheitsbezogenen E/E/PE-Systems aus den Kenntnissen über die Risikofaktoren, die mit der EUC und dem EUC-Leit- oder Steuerungssystem verbunden sind, zu bestimmen. Diese Methode ist insbesondere anwendbar, wenn das Risikomodell demjenigen der Bilder A.1 und A.2 entspricht.

Das in diesem Anhang beschriebene Schema nimmt an, dass jedes sicherheitsbezogene System und jede andere Maßnahme zur Risikominderung unabhängig ist.

Dieser Anhang ist nicht als eine endgültige Beschreibung der Methode vorgesehen, sondern zur Erläuterung der allgemeinen Prinzipien, wie solch eine Matrix von denjenigen entwickelt werden kann, die ausreichende Kenntnis von den in Betracht zu ziehenden Parametern haben. Diejenigen, die beabsichtigen, die in diesem Anhang aufgeführten Methoden anzuwenden, sollten das angegebene Quellenmaterial zu Rate ziehen.

ANMERKUNG Für weitere Informationen zur Matrix des gefährlichen Vorfalls siehe [4] in den Literaturhinweisen.

G.2 Matrix des Ausmaßes des gefährlichen Vorfalls

Die folgenden Anforderungen untermauern die Matrix und jede ist für die Gültigkeit der Methode notwendig:

a) die sicherheitsbezogenen E/E/PE-Systeme und andere Maßnahmen zur Risikominderung sind unabhängig;

b) jedes sicherheitsbezogene System (E/E/PE und andere Technologien) und andere Maßnahmen zur Risikominderung werden als Schutzebenen betrachtet, die, wie in Bild A.1 gezeigt, selbst einen Anteil zur Risikominderung beisteuern;

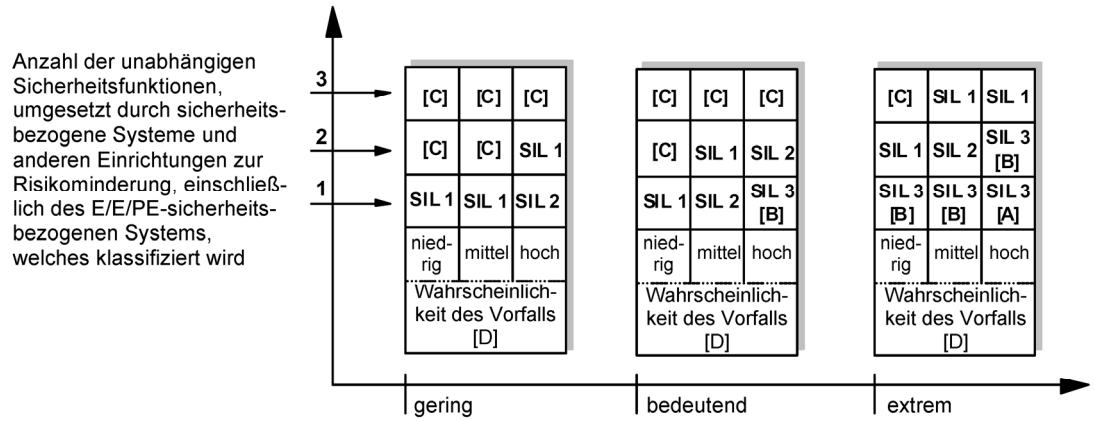
ANMERKUNG 1 Diese Annahme ist nur gültig, falls regelmäßige Nachweisprüfungen der Schutzebenen durchgeführt werden.

c) wenn eine Schutzebene (siehe b) oben) hinzugefügt wird, dann wird eine Verbesserung der Sicherheitsintegrität um eine Größenordnung erreicht;

ANMERKUNG 2 Diese Annahme ist nur gültig, falls die sicherheitsbezogenen Systeme und die anderen Maßnahmen zur Risikominderung einen angemessenen Grad der Unabhängigkeit aufweisen.

d) nur ein sicherheitsbezogenes E/E/PE-System wird verwendet (aber dies kann in Verbindung mit einem sicherheitsbezogenen System anderer Technologie und/oder anderen Maßnahmen zur Risikominderung auftreten), für das diese Vorgehensweise den notwendigen Sicherheits-Integritätslevel bestimmt;

e) die obigen Betrachtungen führen zur „Matrix des Ausmaßes des gefährlichen Vorfalls“, die in Bild G.1 gezeigt wird. Es sollte beachtet werden, dass diese Matrix mit Beispieldaten ausgefüllt wurde, um die allgemeinen Prinzipien aufzuzeigen. Für jede besondere Situation oder jeden bestimmten Bereich vergleichbarer Industrien kann eine Matrix ähnlich derjenigen in Bild G.1 entwickelt und, im Hinblick auf ein tolerierbares Risikokriterium, das auf die jeweilige Situation anwendbar ist, kalibriert werden.



[A] Ein SIL 3 sicherheitsbezogenes E/E/PE-System liefert in dieser Stufe keine ausreichende Risikominderung. Zusätzliche Maßnahmen zur Risikominderung sind erforderlich.

[B] Ein SIL 3 sicherheitsbezogenes E/E/PE-System könnte in dieser Stufe keine ausreichende Risikominderung liefern. Eine Gefährdungs- und Risikoanalyse ist erforderlich, um festzustellen, ob zusätzliche Maßnahmen zu Risikominderung erforderlich sind.

[C] Ein unabhängiges sicherheitsbezogenes E/E/PE-System ist wahrscheinlich nicht erforderlich.

[D] Die Wahrscheinlichkeit des Ereignisses ist die Wahrscheinlichkeit für das Auftreten des gefährlichen Vorfalls, ohne jegliches sicherheitsbezogenes System oder jegliche externe Einrichtung zur Risikominderung.

[E] Die Wahrscheinlichkeit des Vorfalls und die Gesamtanzahl unabhängiger Schutzschichten sind in Bezug zu ihrer spezifischen Anwendung definiert.

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

Literaturhinweise

[1] IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*

ANMERKUNG Harmonisiert in der Reihe EN 61511 (nicht modifiziert).

[2] IEC 62061, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

ANMERKUNG Harmonisiert als EN 62061.

[3] IEC 61800-5-2, *Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional*

ANMERKUNG Harmonisiert als EN 61800-5-2.

[4] ANSI/ISA S84:1996, *Application of safety Instrumented Systems for the Process Industries*

[5] Health and Safety Executive (UK) *publication, ISBN 011 886368 1, Tolerability of risk from nuclear power stations,* <www.hse.gov.uk/nuclear/tolerability.pdf>

[6] The Motor Industry Research Association, 1994, ISBN 09524156 0 7, *Development guidelines for vehicle based software*

[7] Health and Safety Executive (UK) publication, ISBN 0 7176 2151 0, *Reducing Risks, Protecting People*, <www.hse.gov.uk/risk/theory/r2p2.pdf>

[8] CCPS ISBN 0-8169-0811-7, *Layer of Protection Analysis – Simplified Process Risk Assessment*

[9] ISO/IEC 31010, *Risk management – Risk assessment techniques*[3)]

ANMERKUNG Harmonisiert als EN 31010.

[10] ISO 10418:2003, *Petroleum and natural gas industries – Offshore production installations – Basic surface process safety systems*

ANMERKUNG Harmonisiert als EN 10418:2003 (nicht modifiziert).

[11] ISO/TR 14121-2*, Safety of machinery – Risk assessment – Part 2: Practical guidance and examples of methods*

[12] ISO 13849-1:2006, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

ANMERKUNG Harmonisiert als EN ISO 13849-1:2006 (nicht modifiziert).

[13] IEC 60601 (all parts), *Medical electrical equipment*

ANMERKUNG Harmonisiert in der Reihe EN 60601 (teilweise modifiziert).

[14] IEC 61508-2, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

ANMERKUNG Harmonisiert als EN 61508-2.

[15] IEC 61508-3, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

ANMERKUNG Harmonisiert als EN 61508-3.

3) Zu veröffentlichen.

[16] IEC 61508-6, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

ANMERKUNG Harmonisiert als EN 61508-6.

[17] IEC 61508-7, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*

ANMERKUNG Harmonisiert als EN 61508-7.

[18] IEC 61511-1, *Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements*

ANMERKUNG Harmonisiert als EN 61511-1.

Anhang ZA
(normativ)

Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen

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).

ANMERKUNG Wenn internationale Publikationen durch gemeinsame Abänderungen geändert wurden, durch (mod) angegeben, gelten die entsprechenden EN/HD.

Publikation	Jahr	Titel	EN/HD	Jahr
IEC 61508-1	2010	Functional safety of electrical/electronic/ programmable electronic safety-related systems – Part 1: General requirements	EN 61508-1	2010
IEC 61508-4	2010	Functional safety of electrical/electronic/ programmable electronic safety-related systems – Part 4: Definitions and abbreviations	EN 61508-4	2010