

	DIN EN 61508-6 (VDE 0803-6)	
	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 61508-6 (VDE 0803-6):2003-06 Siehe Anwendungsbeginn 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 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 (IEC 61508-6:2010); German version EN 61508-6:2010 Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3 (CEI 61508-6:2010); Version allemande EN 61508-6:2010 Gesamtumfang 121 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

Anwendungsbeginn

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

Daneben darf DIN EN 61508-6 (VDE 0803-6):2003-06 noch bis 2013-05-01 angewendet werden.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 61508-6 (VDE 0803-6):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 61508-6 (VDE 0803-6):2003-06 wurden folgende Änderungen vorgenommen:

- a) vollständige Überarbeitung des Anhangs B;
- b) vollständige Überarbeitung des Anhangs D.

Frühere Ausgaben

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

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 61025:2001	IEC 61025:2006	DIN EN 61025:2007-08	–
EN 61078:2006	IEC 61078:2006	DIN EN 61078:2006-10	–
EN 61165:2006	IEC 61165:2006	DIN EN 61165:2007-02	–
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 61508-5:2010	IEC 61508-5:2010	DIN EN 61508-5 (VDE 0803-5):2011-02	VDE 0803-5
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
–	IEC 65B/725/CD:2009	E DIN IEC 61131-3:2009-12	–
–	IEC 56/1266/CD:2008	E DIN IEC 62551 (VDE 0050-4):2008-10	VDE 0050-4
–	ISA-TR84.00.02-2002	–	–

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 61025:2007-08, *Fehlzustandsbaumanalyse (IEC 61025:2006); Deutsche Fassung EN 61025:2007*

DIN EN 61078:2006-10, *Techniken für die Analyse der Zuverlässigkeit – Zuverlässigkeitsblockdiagramm und Boole'sche Verfahren*

DIN EN 61165:2007-02, *Anwendung des Markoff-Verfahrens (IEC 61165:2006); Deutsche Fassung EN 61165:2006*

DIN EN 61508-6 (VDE 0803-6):2011-02

DIN EN 61508-1 (VDE 0803-1):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: 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 61508-5 (VDE 0803-5):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 5: Beispiele von Methoden für die Bestimmung von Sicherheits-Integritätsleveln* (IEC 61508-5:2010); Deutsche Fassung EN 61508-5:2010

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*

E DIN IEC 61131-3:2009-12, *Speicherprogrammierbare Steuerungen – Teil 3: Programmiersprachen; Englische Fassung* (IEC 65B/725/CD:2009)

E DIN IEC 62551 (VDE 0050-4):2008-10, *Analysemethoden für Zuverlässigkeit – Petrinetz-Modellierung* (IEC 56/1266/CD:2008)

Funktionale Sicherheit sicherheitsbezogener
elektrischer/elektronischer/programmierbarer elektronischer Systeme –
Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3
(IEC 61508-6:2010)

Functional safety of
electrical/electronic/programmable electronic
safety-related systems –
Part 6: Guidelines on the application of IEC
61508-2 and IEC 61508-3
(IEC 61508-6:2010)

Sécurité fonctionnelle des systèmes
électriques/électroniques/électroniques
programmables relatifs à la sécurité –
Partie 6: Lignes directrices pour l'application de
la CEI 61508-2 et de la CEI 61508-3
(CEI 61508-6:2010)

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

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

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

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

CENELEC

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

Zentralsekretariat: Avenue Marnix 17, B-1000 Brüssel

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

Ref. Nr. EN 61508-6:2010 D

Vorwort

Der Text des Schriftstücks 65A/553/FDIS, zukünftige 2. Ausgabe von IEC 61508-6, 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 61508-6 angenommen.

Diese Europäische Norm ersetzt EN 61508-6:2001.

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 61508-6:2010 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.
[4] IEC 61078:2006	ANMERKUNG	Harmonisiert als EN 61078:2006 (nicht modifiziert).
[5] IEC 61165:2006	ANMERKUNG	Harmonisiert als EN 61165:2006 (nicht modifiziert).
[16] IEC 61131-3:2003	ANMERKUNG	Harmonisiert als EN 61131-3:2003 (nicht modifiziert).
[18] IEC 61025:2006	ANMERKUNG	Harmonisiert als EN 61025:2007 (nicht modifiziert).
[26] IEC 60601 Reihe	ANMERKUNG	Harmonisiert in der Reihe EN 60601 (teilweise modifiziert).
[27] IEC 61508-1:2010	ANMERKUNG	Harmonisiert als EN 61508-1:2010 (nicht modifiziert).
[28] IEC 61508-5:2010	ANMERKUNG	Harmonisiert als EN 61508-5:2010 (nicht modifiziert).
[29] IEC 61508-7:2010	ANMERKUNG	Harmonisiert als EN 61508-7:2010 (nicht modifiziert).

Inhalt

	Seite
Vorwort.....	2
Einleitung	8
1 Anwendungsbereich	10
2 Normative Verweisungen	12
3 Begriffe und Abkürzungen	12
Anhang A (informativ) Anwendung der IEC 61508-2 und der IEC 61508-3.....	13
A.1 Allgemeines	13
A.2 Funktionale Schritte bei der Anwendung der IEC 61508-2	15
A.3 Funktionale Schritte bei der Anwendung der IEC 61508-3	19
Anhang B (informativ) Beispielverfahren für die Bewertung von Ausfallwahrscheinlichkeiten der Hardware	21
B.1 Allgemeines	21
B.2 Betrachtungen zu grundlegenden Wahrscheinlichkeitsberechnungen	22
B.2.1 Einleitung	22
B.2.2 Sicherheitsbezogenes E/E/PE-System mit niedriger Anforderungsrate	22
B.2.3 Sicherheitsbezogenes E/E/PE-System mit hoher Anforderungsrate oder kontinuierlicher Anforderung	23
B.3 Zuverlässigkeitsblockdiagramm-Ansatz mit angenommener konstanter Ausfallrate.....	25
B.3.1 Grundlegende Hypothese.....	25
B.3.2 Mittlere Ausfallwahrscheinlichkeit bei Anforderung (für die Betriebsart mit niedriger Anforderungsrate).....	29
B.3.3 Mittlere Häufigkeit eines gefahrbringenden Ausfalls (für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung)	43
B.4 Boolescher Ansatz.....	52
B.4.1 Allgemeines	52
B.4.2 Modell des Zuverlässigkeitsblockdiagramms	52
B.4.3 Fehlerbaummodell.....	53
B.4.4 PFD-Berechnungen.....	53
B.5 Zustands-/Übergangs-Ansätze.....	58
B.5.1 Allgemeines	58
B.5.2 Markov-Ansatz.....	59
B.5.3 Ansätze basierend auf Petri-Netzen und Monte-Carlo-Simulation.....	67
B.5.4 Andere Ansätze	73
B.6 Behandlung von Unsicherheiten.....	75
B.7 Verweise	76
Anhang C (informativ) Ausgearbeitetes Beispiel für die Berechnung des Diagnosedeckungsgrads und des Anteils sicherer Ausfälle	77
Anhang D (informativ) Eine Methode zur Quantifizierung der Auswirkungen von hardwarebedingten Ausfällen infolge gemeinsamer Ursache in E/E/PE-Systemen	80
D.1 Allgemeines	80

	Seite
D.1.1 Einleitung	80
D.1.2 Kurzübersicht	80
D.1.3 Schutz gegen Ausfälle infolge gemeinsamer Ursache	81
D.1.4 In der Normenreihe IEC 61508 gewählter Ansatz	83
D.2 Anwendungsbereich der Methode	84
D.3 Durch die Methode berücksichtigte Punkte	85
D.4 Verwendung des β -Faktors, um die Wahrscheinlichkeit eines Ausfalls eines sicherheitsbezogenen E/E/PE-Systems durch Ausfälle infolge gemeinsamer Ursache zu berechnen	86
D.5 Schätzung von β unter Verwendung der Tabellen	87
D.6 Beispiele für die Anwendung der β -Faktor-Methode	92
D.7 Binomialverteilte Ausfallrate (Schockmodell) – CCF-Ansatz	93
D.8 Literaturhinweise	95
Anhang E (informativ) Beispiele für die Anwendung der Tabellen zur Sicherheitsintegrität der Software aus IEC 61508-3	96
E.1 Allgemeines	96
E.2 Beispiel für den Sicherheits-Integritätslevel 2	96
E.3 Beispiel für den Sicherheits-Integritätslevel 3	105
Literaturhinweise	114
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	117
Bilder	
Bild 1 – Gesamtrahmen der Normenreihe IEC 61508	11
Bild A.1 – Anwendung der IEC 61508-2	17
Bild A.2 – Anwendung der IEC 61508-2 (Fortsetzung von Bild A.1)	18
Bild A.3 – Anwendung der IEC 61508-3	20
Bild B.1 – Zuverlässigkeitsblockdiagramm einer vollständigen PLT-Schutzeinrichtung	22
Bild B.2 – Beispielkonfiguration für zwei Kanäle mit Sensoren	27
Bild B.3 – Struktur mit Teilsystemen	29
Bild B.4 – Blockschaltbild für 1oo1	31
Bild B.5 – Zuverlässigkeitsblockdiagramm für 1oo1	31
Bild B.6 – Blockschaltbild für 1oo2	32
Bild B.7 – Zuverlässigkeitsblockdiagramm für 1oo2	32
Bild B.8 – Blockschaltbild für 2oo2	32
Bild B.9 – Zuverlässigkeitsblockdiagramm für 2oo2	33
Bild B.10 – Blockschaltbild für 1oo2D	33
Bild B.11 – Zuverlässigkeitsblockdiagramm für 1oo2D	33
Bild B.12 – Blockschaltbild für 2oo3	34
Bild B.13 – Zuverlässigkeitsblockdiagramm für 2oo3	34
Bild B.14 – Architektur eines Beispiels für die Betriebsart mit niedriger Anforderungsrate	40

Bild B.15 – Architektur des Beispiels für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung.....	50
Bild B.16 – Zuverlässigkeitsblockdiagramm einer einfachen vollständigen Schleife mit Sensoren als 2oo3-Logik.....	52
Bild B.17 – Einfacher Fehlerbaum entsprechend dem in Bild B.1 dargestellten Zuverlässigkeitsblockdiagramm	53
Bild B.18 – Gleichartigkeit von Fehlerbaum und Zuverlässigkeitsblockdiagramm	54
Bild B.19 – Augenblickliche Nichtverfügbarkeit $U(t)$ einzelner, periodisch getesteter Komponenten	55
Bild B.20 – Prinzip der Berechnung von PFD_{avg} bei Verwendung von Fehlerbäumen	56
Bild B.21 – Auswirkung von versetzten Tests	57
Bild B.22 – Beispiel eines komplexen Testmusters	58
Bild B.23 – Markov-Graph, der das Verhalten eines Systems mit zwei Komponenten modelliert.....	59
Bild B.24 – Prinzip der Modellierung eines mehrphasigen Markov-Prozesses	60
Bild B.25 – Sägezahnkurve bei mehrphasigem Markov-Ansatz	62
Bild B.26 – Angenähertes Markov-Modell	62
Bild B.27 – Auswirkungen von Ausfällen durch die Anforderung selbst.....	62
Bild B.28 – Modellierung des Einflusses der Testdauer	63
Bild B.29 – Mehrphasiges Markov-Modell mit DD- und DU-Ausfällen	63
Bild B.30 – Logikänderung (2oo3 nach 1oo2) anstelle einer Reparatur des ersten Ausfalls	64
Bild B.31 – Markov-Graphen für die „Zuverlässigkeit“ mit einem absorbierenden Zustand.....	65
Bild B.32 – Markov-Graphen für die „Verfügbarkeit“ ohne absorbierende Zustände	66
Bild B.33 – Petri-Netz für die Modellierung einer einzelnen periodisch getesteten Komponente	68
Bild B.34 – Petri-Netze zur Modellierung von Ausfällen infolge gemeinsamer Ursache und Reparaturressourcen.....	71
Bild B.35 – Verwendung von Zuverlässigkeitsblockdiagrammen zur Aufstellung von Petri-Netzen und Auxiliary-Petri-Netzen für die PFD - und PFH -Berechnungen	71
Bild B.36 – Einfaches Petri-Netz für eine einzelne Komponente mit entdeckten Ausfällen und Reparaturen.....	72
Bild B.37 – Beispiel einer funktionalen und dysfunktionalen Modellierung mit einer formalen Sprache	74
Bild B.38 – Prinzip der Fortpflanzung von Unsicherheiten	75
Bild D.1 – Beziehung zwischen Ausfällen infolge gemeinsamer Ursache und Ausfällen einzelner Kanäle.....	83
Bild D.2 – Umsetzung des Schockmodells anhand von Fehlerbäumen.....	94
Tabellen	
Tabelle B.1 – In diesem Anhang verwendete Benennungen und ihre zugehörigen Parameterbereiche	27
Tabelle B.2 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für ein Wiederholungsprüfungsintervall von sechs Monaten und eine mittlere Dauer bis zur Wiederherstellung von 8 h.....	36
Tabelle B.3 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für ein Wiederholungsprüfungsintervall von einem Jahr und eine mittlere Dauer bis zur Wiederherstellung von 8 h.....	37

Tabelle B.4 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für ein Wiederholungsprüfungsintervall von zwei Jahren und eine mittlere Dauer bis zur Wiederherstellung von 8 h	38
Tabelle B.5 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für ein Wiederholungsprüfungsintervall von zehn Jahren und eine mittlere Dauer bis zur Wiederherstellung von 8 h	39
Tabelle B.6 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für das Sensor-Teilsystem in dem Beispiel für die Betriebsart mit niedriger Anforderungsrate (ein Jahr Wiederholungsprüfungsintervall und 8 h <i>MTTR</i>)	40
Tabelle B.7 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für das Logik-Teilsystem in dem Beispiel für die Betriebsart mit niedriger Anforderungsrate (ein Jahr Wiederholungsprüfungsintervall und 8 h <i>MTTR</i>)	41
Tabelle B.8 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für das Stellglied-Teilsystem in dem Beispiel für die Betriebsart mit niedriger Anforderungsrate (ein Jahr Wiederholungsprüfungsintervall und 8 h <i>MTTR</i>)	41
Tabelle B.9 – Beispiel für eine unvollständige Wiederholungsprüfung.....	43
Tabelle B.10 – Mittlere Häufigkeit eines gefahrbringenden Ausfalls (in der Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung) für ein Wiederholungsprüfungsintervall von einem Monat und eine mittlere Dauer bis zur Wiederherstellung von 8 h.....	46
Tabelle B.11 – Mittlere Häufigkeit eines gefahrbringenden Ausfalls (in der Betriebsart mit hoher oder Anforderungsrate kontinuierlicher Anforderung) für ein Wiederholungsprüfungsintervall von drei Monaten und eine mittlere Dauer bis zur Wiederherstellung von 8 h.....	47
Tabelle B.12 – Mittlere Häufigkeit eines gefahrbringenden Ausfalls (in der Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung) für ein Wiederholungsprüfungsintervall von sechs Monaten und eine mittlere Dauer bis zur Wiederherstellung von 8 h	48
Tabelle B.13 – Mittlere Häufigkeit eines gefahrbringenden Ausfalls (in der Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung) für ein Wiederholungsprüfungsintervall von einem Jahr und eine mittlere Dauer bis zur Wiederherstellung von 8 h	49
Tabelle B.14 – Mittlere Häufigkeit eines gefahrbringenden Ausfalls für das Sensor-Teilsystem in dem Beispiel für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung (sechs Monate Wiederholungsprüfungsintervall und 8 h <i>MTTR</i>)	50
Tabelle B.15 – Mittlere Häufigkeit eines gefahrbringenden Ausfalls für das Logik-Teilsystem in dem Beispiel für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung (sechs Monate Wiederholungsprüfungsintervall und 8 h <i>MTTR</i>)	51
Tabelle B.16 – Mittlere Häufigkeit eines gefahrbringenden Ausfalls für das Stellglied-Teilsystem in dem Beispiel für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung (sechs Monate Wiederholungsprüfungsintervall und 8 h <i>MTTR</i>)	51
Tabelle C.1 – Beispielberechnung für den Diagnosedeckungsgrad und den Anteil sicherer Ausfälle.....	78
Tabelle C.2 – Diagnosedeckungsgrad und Wirksamkeit für verschiedene Teilsysteme	79
Tabelle D.1 – Bewertung programmierbarer Elektronik oder Sensoren/Stellglieder	88
Tabelle D.2 – Werte für Z – programmierbare Elektronik	90
Tabelle D.3 – Werte für Z – Sensoren oder Stellglieder	90
Tabelle D.4 – Berechnung von β_{nt} oder $\beta_{\text{D int}}$	91
Tabelle D.5 – Berechnung von β für Redundanzsysteme größer als 1002	91
Tabelle D.6 – Beispielwerte für programmierbare Elektroniken	93
Tabelle E.1 – Spezifikation der Anforderungen an die Sicherheit der Software.....	97
Tabelle E.2 – Softwareentwurf und Softwareentwicklung – Entwurf der Softwarearchitektur	98

Tabelle E.3 – Softwareentwurf und Softwareentwicklung – Werkzeuge und Programmiersprache	99
Tabelle E.4 – Softwareentwurf und Softwareentwicklung – Detaillierter Entwurf.....	100
Tabelle E.5 – Softwareentwurf und Softwareentwicklung – Test der Softwaremodule und Integration.....	101
Tabelle E.6 – Integration der programmierbaren Elektronik (Hardware und Software)	101
Tabelle E.7 – Softwareaspekte bezüglich der Validierung der Sicherheit des Systems	102
Tabelle E.8 – Softwaremodifikation	103
Tabelle E.9 – Softwareverifikation	104
Tabelle E.10 – Beurteilung der funktionalen Sicherheit.....	104
Tabelle E.11 – Spezifikation der Anforderungen an die Sicherheit der Software.....	106
Tabelle E.12 – Softwareentwurf und Softwareentwicklung – Entwurf der Softwarearchitektur.....	106
Tabelle E.13 – Softwareentwurf und Softwareentwicklung – Werkzeuge und Programmiersprache	108
Tabelle E.14 – Softwareentwurf und Softwareentwicklung – Detaillierter Entwurf.....	108
Tabelle E.15 – Softwareentwurf und Softwareentwicklung – Test der Softwaremodule und Integration.....	109
Tabelle E.16 – Integration der programmierbaren Elektronik (Hardware und Software)	110
Tabelle E.17 – Softwareaspekte bezüglich der Validierung der Sicherheit des Systems	110
Tabelle E.18 – Modifikation	111
Tabelle E.19 – Softwareverifikation	112
Tabelle E.20 – Beurteilung der funktionalen Sicherheit.....	112

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.

1 Anwendungsbereich

1.1 Dieser Teil der IEC 61508 enthält Informationen und Hinweise zu IEC 61508-2 und IEC 61508-3.

- **Anhang A** liefert einen kurzen Überblick über die Anforderungen der IEC 61508-2 und der IEC 61508-3 und zeigt die funktionalen Schritte zu ihrer Anwendung.
- **Anhang B** zeigt ein Beispiel für die Anwendung der Verfahren zur Berechnung der Wahrscheinlichkeiten von Hardwareausfällen und sollte in Verbindung mit IEC 61508-2, 7.4.3 und Anhang C, und Anhang D gelesen werden.
- **Anhang C** zeigt ein ausgearbeitetes Beispiel für die Berechnung des Diagnosedeckungsgrads und sollte in Verbindung mit IEC 61508-2, Anhang C, gelesen werden.
- **Anhang D** zeigt eine Methode zur Quantifizierung der Auswirkungen von hardwarebezogenen Ausfällen infolge gemeinsamer Ursache auf die Ausfallwahrscheinlichkeit.
- **Anhang E** zeigt für die Sicherheits-Integritätslevel 2 und 3 ausgearbeitete Beispiele für die Anwendung der Tabellen zur Sicherheitsintegrität der Software nach IEC 61508-3, Anhang A.

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 Gesamtrahmen für die Normenreihe IEC 61508 und zeigt die Rolle, welche IEC 61508-6 beim Erreichen der funktionalen Sicherheit für sicherheitsbezogene E/E/PE-Systeme spielt.

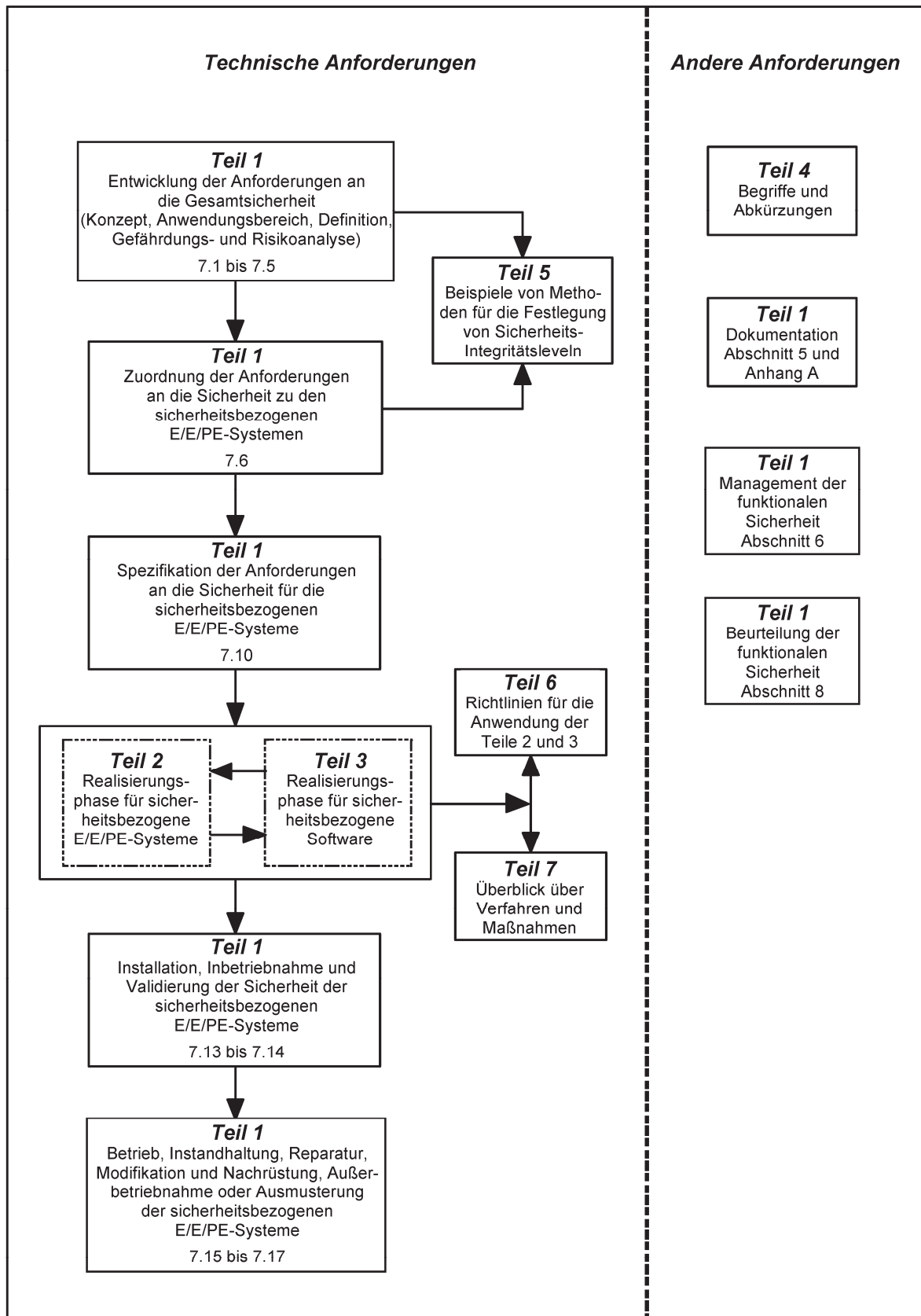


Bild 1 – Gesamtrahmen der Normenreihe IEC 61508

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 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

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

3 Begriffe und Abkürzungen

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

Anhang A (informativ)

Anwendung der IEC 61508-2 und der IEC 61508-3

A.1 Allgemeines

Maschinen, Prozessanlagen und andere Betriebsmittel können im Fall einer Fehlfunktion (z. B. aufgrund von Ausfällen elektrischer, elektronischer und/oder programmierbarer elektronischer Geräte) durch gefährliche Vorfälle wie Feuer, Explosion, Überdosis von Strahlung oder in eine Maschine eingeschlossen werden Risiken für Personen und die Umwelt darstellen. Ausfälle können entweder durch physikalische Fehler im Gerät (die z. B. zufällige Hardwareausfälle verursachen), durch systematische Fehler (z. B. kann menschliches Versagen bei der Spezifikation oder beim Entwurf systematische Ausfälle bei einer besonderen Kombination von Eingaben verursachen) oder durch Umgebungsbedingungen entstehen.

IEC 61508-1 liefert mit einem risikobasierten Ansatz den Gesamtrahmen zur Vermeidung und/oder Beherrschung von Ausfällen in elektromechanischen, elektronischen oder programmierbaren elektronischen Geräten.

Das Hauptziel ist es, sicherzustellen, dass die Anlage und die Betriebsmittel sicher automatisiert werden können. Ein zentrales Ziel dieser Norm ist die Verhinderung von Folgendem:

- Ausfälle von Steuerungssystemen, die andere Vorfälle auslösen, die wiederum zu Gefahren (z. B. Brand, Freisetzen giftiger Stoffe, Wiederanlauf einer Maschine usw.) führen können; und
- unerkannte Ausfälle in Schutzsystemen (z. B. in einem Notabschaltsystem), die die Systeme für den Fall eines notwendigen Sicherheitseingriffs unverfügbar machen.

IEC 61508-1 fordert, dass eine Gefährdungs- und Risikoanalyse auf Prozess-/Maschinenebene durchgeführt wird, um den für die Risikokriterien der Anwendung notwendigen Betrag der Risikominderung zu bestimmen. Das Risiko basiert auf der Beurteilung sowohl der Auswirkung (oder Schwere) als auch der Häufigkeit (oder Wahrscheinlichkeit) des gefährlichen Vorfalls.

IEC 61508-1 fordert weiterhin, dass der durch die Risikoanalyse festgestellte Betrag der Risikominderung zur Feststellung verwendet wird, ob ein oder mehrere sicherheitsbezogene Systeme¹⁾ notwendig sind und für welche Sicherheitsfunktionen (jede mit einer spezifizierten Sicherheitsintegrität)²⁾ diese gebraucht werden.

IEC 61508-2 und IEC 61508-3 nehmen die Sicherheitsfunktionen und Anforderungen an die Sicherheitsintegrität auf, die jedem System durch die Anwendung der IEC 61508-1 zugeordnet worden sind und das als sicherheitsbezogenes E/E/PE-System bezeichnet wird, und legen die Anforderungen an die Tätigkeiten im Sicherheitslebenszyklus fest, die:

- während der Spezifikation, des Entwurfs und der Modifikation der Hardware und Software angewendet werden müssen; und

¹⁾ Systeme, die für die funktionale Sicherheit notwendig sind und ein oder mehrere elektrische (elektromechanische), elektronische oder programmierbare elektronische (E/E/PE) Geräte beinhalten, werden als sicherheitsbezogenes E/E/PE-Systeme bezeichnet und schließen alle Betriebsmittel ein, die zur Ausführung der erforderlichen Sicherheitsfunktion (siehe IEC 61508-4, 3.5.1) notwendig sind.

²⁾ Die Sicherheitsintegrität ist als eine von vier diskreten Stufen festgelegt. Der Sicherheits-Integritätslevel 4 ist der höchste und Sicherheits-Integritätslevel 1 der niedrigste (siehe IEC 61508-4, 3.5.4 und 3.5.8).

- sich auf Mittel zur Verhinderung und/oder Beherrschung zufälliger Hardware- und systematischer Ausfälle (dem Sicherheitslebenszyklus des E/E/PE-Systems und dem Software-Sicherheitslebenszyklus)³⁾ konzentrieren.

IEC 61508-2 und IEC 61508-3 geben keine Anleitung, welcher Sicherheits-Integritätslevel für ein gegebenes erforderliches tolerierbares Risiko angemessen ist. Diese Entscheidung hängt von vielen Faktoren ab, einschließlich der Art der Anwendung, dem Maß, in dem andere Systeme Sicherheitsfunktionen ausführen, und von gesellschaftlichen und wirtschaftlichen Gegebenheiten (siehe IEC 61508-1 und IEC 61508-5).

Die Anforderungen der IEC 61508-2 und der IEC 61508-3 beinhalten:

- die Anwendung von Maßnahmen und Verfahren⁴⁾, abgestuft gegen den Sicherheits-Integritätslevel, zur Vermeidung systematischer Ausfälle⁵⁾ durch vorbeugende Methoden, und
- die Beherrschung systematischer Ausfälle (einschließlich Softwarefehler) und zufälliger Hardwareausfälle durch Entwurfsmerkmale wie Fehleraufdeckung, Redundanz und Architekturmerkmale (z. B. Diversität).

In IEC 61508-2 beruht die Zusicherung, dass das Ziel der Sicherheitsintegrität für gefahrbringende zufällige Hardwareausfälle erreicht worden ist, auf:

- den Anforderungen zur Hardwarefehlertoleranz (siehe IEC 61508-2, Tabellen 2 und 3), und
- dem Diagnosedeckungsgrad und der Häufigkeit von Wiederholungsprüfungen von Teilsystemen und Bauteilen, indem eine Zuverlässigkeitsanalyse unter Verwendung angemessener Daten ausgeführt wird.

Sowohl in IEC 61508-2 als auch in IEC 61508-3 wird die Gewissheit, dass das Ziel der Sicherheitsintegrität für systematische Ausfälle erreicht worden ist, erzielt durch:

- die korrekte Anwendung von Sicherheitsmanagementverfahren,
- den Einsatz fachkundigen Personals,
- die Durchführung der im Sicherheitslebenszyklus festgelegten Tätigkeiten einschließlich der festgelegten Verfahren und Maßnahmen⁶⁾, und
- eine unabhängige Beurteilung der funktionalen Sicherheit⁷⁾.

Das Gesamtziel ist es, sicherzustellen, dass entsprechend dem Sicherheits-Integritätslevel verbliebene systematische Fehler keinen Ausfall des sicherheitsbezogenen E/E/PE-Systems verursachen.

³⁾ Um den Anforderungen dieser Norm eine eindeutige Struktur zu geben, wurde die Entscheidung getroffen, die Anforderungen unter Verwendung eines Modells des Entwicklungsprozesses zu ordnen, in dem die Stufen in einer definierten Reihenfolge mit geringer Iteration (manchmal auch Wasserfallmodell genannt) aufeinanderfolgen. Es sei jedoch hervorgehoben, dass jeder Ansatz für einen Lebenszyklus verwendet werden kann, vorausgesetzt, dass eine Aussage zur Gleichwertigkeit im Sicherheitsplan für das Projekt gemacht worden ist (siehe IEC 61508-1, Abschnitt 7).

⁴⁾ Die für jeden Sicherheits-Integritätslevel geforderten Verfahren und Maßnahmen sind in den Tabellen der Anhänge A und B von IEC 61508-2 und IEC 61508-3 aufgelistet.

⁵⁾ Systematische Ausfälle können gewöhnlich nicht quantifiziert werden. Ursachen hierfür sind u. a.: Spezifikations- und Entwurfsfehler in Hardware und Software, Ausfälle aufgrund der Umgebungsbedingungen (z. B. Temperatur) und betriebsbedingte Fehler (z. B. eine schlechte Schnittstelle).

⁶⁾ Andere als in dieser Norm festgelegte Maßnahmen sind ebenfalls annehmbar, wenn sie während der Planung der Sicherheit schriftlich begründet werden (siehe IEC 61508-1, Abschnitt 6).

⁷⁾ Eine unabhängige Beurteilung bedeutet nicht unbedingt eine Beurteilung durch Dritte (siehe IEC 61508-1, Abschnitt 8).

IEC 61508-2 ist entwickelt worden, um Anforderungen zum Erreichen der Sicherheitsintegrität der Hardware⁸⁾ des sicherheitsbezogenen E/E/PE-Systems einschließlich Sensoren und Stellgliedern zur Verfügung zu stellen. Verfahren und Maßnahmen werden sowohl gegen zufällige als auch gegen systematische Hardwareausfälle gefordert. Diese beinhalten, wie oben dargelegt, eine angemessene Kombination von Maßnahmen zur Vermeidung von Fehlern und zur Beherrschung von Ausfällen. Wird ein Bedieneringriff für die funktionale Sicherheit benötigt, werden Anforderungen an die Bedienerschnittstelle gestellt. In IEC 61508-2 werden ebenfalls auf Software und Hardware basierende Diagnosetestverfahren und Maßnahmen (zum Beispiel Diversität) zur Aufdeckung zufälliger Hardwareausfälle festgelegt.

IEC 61508-3 ist entwickelt worden, um Anforderungen zum Erreichen der Sicherheitsintegrität der Software, und zwar sowohl der Embedded-Software (einschließlich Dienste für Fehlererkennung durch Diagnose) als auch der Anwendungssoftware, zur Verfügung zu stellen. IEC 61508-3 fordert eine Kombination von Ansätzen zur Fehlervermeidung (Qualitätssicherung) und Fehlertoleranz (Softwarearchitektur), da es keinen bekannten Weg zum Nachweis der Fehlerfreiheit in einigermaßen komplexer sicherheitsbezogener Software, besonders der Freiheit von Spezifikations- und Entwurfsfehlern, gibt. IEC 61508-3 fordert die Anwendung von Software-Entwurfsprinzipien wie Top-Down-Entwurf, Modularität, Verifikation jeder Phase des Entwicklungslebenszyklus, verifizierte Softwaremodule und Software-Modulbibliotheken und verständliche Dokumentation, um die Verifikation und Validierung zu erleichtern. Die verschiedenen Stufen der Software erfordern verschiedene Stufen an Zusicherung, dass diese und ähnliche Prinzipien richtig angewendet worden sind.

Der Softwareentwickler darf, muss aber nicht, unabhängig von der Organisation sein, die die gesamte Entwicklung des E/E/PE-Systems durchführt. In jedem Fall ist eine enge Zusammenarbeit notwendig, insbesondere bei der Entwicklung der Architektur der programmierbaren Elektronik, wo die Abwägungen zwischen Hardware- und Softwarearchitektur im Hinblick auf die Auswirkungen auf die Sicherheit (siehe IEC 61508-2, Bild 4) durchgeführt werden müssen.

A.2 Funktionale Schritte bei der Anwendung der IEC 61508-2

Die funktionalen Schritte zur Anwendung der IEC 61508-2 werden in den [Bildern A.1](#) und [A.2](#) gezeigt. Die funktionalen Schritte zur Anwendung der IEC 61508-3 werden in [Bild A.3](#) dargestellt.

Die funktionalen Schritte der IEC 61508-2 (siehe [Bilder A.1](#) und [A.2](#)) sind wie folgt:

- a) Erhalt der Zuordnung der Anforderungen an die Sicherheit (siehe IEC 61508-1). Angemessene Aktualisierung der Planung der Sicherheit während der Entwicklung des sicherheitsbezogenen E/E/PE-Systems.
- b) Bestimmung der Anforderungen an sicherheitsbezogene E/E/PE-Systeme, einschließlich der Anforderungen an die Sicherheitsintegrität für jede Sicherheitsfunktion (siehe IEC 61508-2, 7.2). Zuweisung der Anforderungen an die Software und Übergabe an die Softwarelieferanten und/oder Entwickler zum Zwecke der Anwendung der IEC 61508-3.

ANMERKUNG 1 An dieser Stelle ist es notwendig, die Möglichkeit gleichzeitiger Ausfälle im EUC-Leit- und Steuersystem und sicherheitsbezogenen E/E/PE-System(en) zu berücksichtigen (siehe IEC 61508-5, A.5.4). Diese können aus Bauteilausfällen infolge gemeinsamer Ursache, zum Beispiel gleichartigen Umgebungseinflüssen, herrühren. Bei ungenügender Berücksichtigung kann das Vorhandensein solcher Ausfälle zu einem höheren als dem erwarteten Restrisiko führen.

- c) Start der Phase für die Planung der Validierung der Sicherheit des sicherheitsbezogenen E/E/PE-Systems (siehe IEC 61508-2, 7.3).
- d) Spezifikation der Architektur (Konfiguration) für das sicherheitsbezogene E/E/PE-Logik-Teilsystem, die Sensoren und Stellglieder. Überprüfung der Hardware- und Softwarearchitektur und der sicherheitstechnischen Auswirkungen der Abwägungen zwischen Hardware und Software (siehe IEC 61508-2, Bild 4) mit dem Softwarelieferanten/Entwickler. Falls notwendig, Wiederholung dieses Schrittes.
- e) Entwicklung eines Modells für die Hardwarearchitektur des sicherheitsbezogenen E/E/PE-Systems. Entwicklung dieses Modell durch getrennten Test jeder Sicherheitsfunktion und Bestimmung jedes Teilsystems (Bauteils), das zur Ausführung dieser Funktion verwendet wird.

⁸⁾ Einschließlich fest eingebauter Software oder softwareähnlicher Objekte (auch Firmware genannt), wie z. B. anwendungsspezifische integrierte Schaltkreise.

- f) Festlegung der Systemparameter für jedes der Teilsysteme (Bauteile), die in dem sicherheitsbezogenen E/E/PE-System verwendet werden. Für jedes Teilsystem (Elemente) wird Folgendes bestimmt:
- das Intervall für die Wiederholungsprüfung für Ausfälle, die nicht automatisch aufgedeckt werden;
 - die mittlere Dauer bis zur Wiederherstellung;
 - der Diagnosedeckungsgrad (siehe IEC 61508-2, Anhang C);
 - die Ausfallwahrscheinlichkeit;
 - die Einschränkungen hinsichtlich der Architektur für Route 1_H, siehe IEC 61508-2, 7.4.4.2 und Anhang C, und für Route 2_H, siehe IEC 61508-2, 7.4.4.3.
- g) Bildung eines Zuverlässigkeitsmodells für jede Sicherheitsfunktion, die das sicherheitsbezogene E/E/PE-System ausführen muss.

ANMERKUNG 2 Ein Zuverlässigkeitsmodell ist eine mathematische Formel, die die Beziehung zwischen der Zuverlässigkeit und den betreffenden Parametern der Einrichtung und der Einsatzbedingungen zeigt.

- h) Berechnung einer Zuverlässigkeitsvoraussage für jede Sicherheitsfunktion unter Verwendung eines angemessenen Verfahrens. Vergleich des Ergebnisses mit dem oben in b) festgelegten Ausfallgrenzwert und den Anforderungen der Route 1_H (siehe IEC 61508-2, 7.4.4.2) oder Route 2_H (siehe IEC 61508-2, 7.4.4.3). Falls die vorausgesagte Zuverlässigkeit den Ausfallgrenzwert nicht erfüllt und/oder nicht den Anforderungen von Route 1_H oder Route 2_H entspricht, dann wird Folgendes geändert:
- wenn möglich, einen oder mehrere der Teilsystem-Parameter (zurückgehen zu f) oben); und/oder
 - die Hardwarearchitektur (zurückgehen zu d) oben).

ANMERKUNG 3 Eine Anzahl von Methoden zur Modellierung steht zur Verfügung, und der Analytiker sollte wählen, welche die geeignetste ist (siehe [Anhang B](#) für Hinweise zu einigen Methoden, die verwendet werden können).

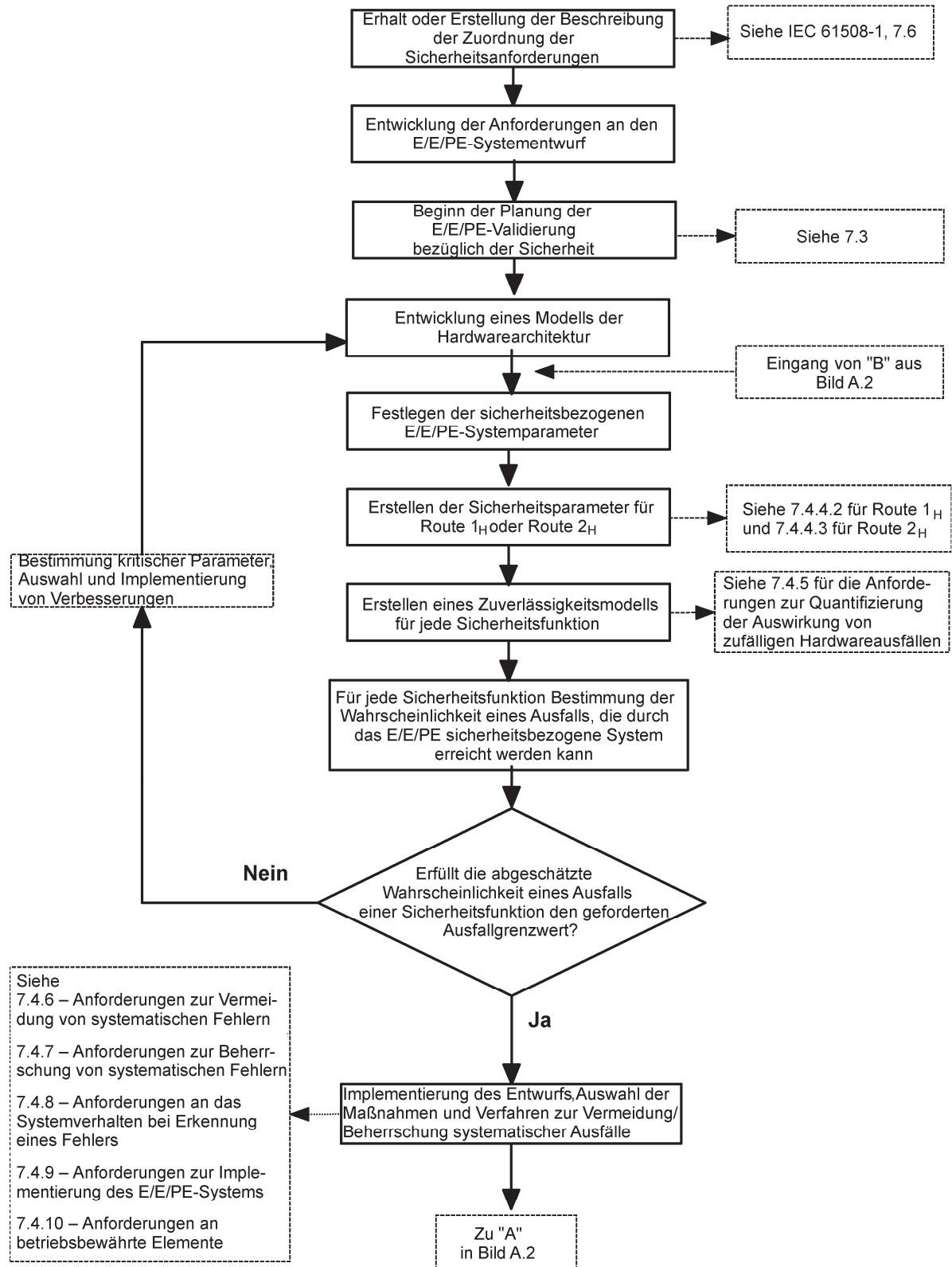
- i) Implementierung des Entwurfs des sicherheitsbezogenen E/E/PE-Systems. Auswahl von Maßnahmen und Verfahren, um systematische Hardwareausfälle, Ausfälle durch Umwelteinflüsse und Bedienfehler (siehe IEC 61508-2, Anhang A) zu beherrschen.
- j) Integration der verifizierten Software (siehe IEC 61508-3) in die Zielhardware (siehe IEC 61508-2, 7.5 und IEC 61508-2, Anhang B) und parallel dazu die Entwicklung der Verfahren, denen Anwender und Instandhaltungspersonal beim Betrieb des Systems zu folgen haben (siehe IEC 61508-2, 7.6 und Anhang B). Berücksichtigung der Softwareaspekte (siehe [A.3 f\)](#)).
- k) Validierung des E/E/PE-Systems (siehe IEC 61508-2, 7.7 und IEC 61508-2, Anhang B) zusammen mit dem Softwareentwickler (siehe IEC 61508-3, 7.7).
- l) Übergabe der Hardware und der Ergebnisse der Validierung der Sicherheit des sicherheitsbezogenen E/E/PE-Systems an die Systemingenieure für die weitere Integration in das Gesamtsystem.
- m) Falls eine Instandhaltung/Modifikation des sicherheitsbezogenen E/E/PE-Systems während der Betriebszeit notwendig wird, erneute Anwendung der IEC 61508-2, sofern angebracht (siehe IEC 61508-2, 7.8).

Einige Tätigkeiten finden im gesamten Sicherheitslebenszyklus des sicherheitsbezogenen E/E/PE-Systems statt. Darunter sind die Verifikation (siehe IEC 61508-2, 7.9) und die Beurteilung der funktionalen Sicherheit (siehe IEC 61508-1, Abschnitt 8).

Durch Anwendung der obigen Schritte werden sicherheitsrelevante Verfahren und Maßnahmen für das sicherheitsbezogene E/E/PE-System im Hinblick auf den erforderlichen Sicherheits-Integritätslevel ausgewählt. Zur Hilfestellung bei dieser Auswahl sind Tabellen mit der Einordnung der verschiedenen Verfahren/Maßnahmen unter die vier Sicherheits-Integritätslevel (siehe IEC 61508-2, Anhang B) formuliert worden. In den Tabellen wird für jedes Verfahren und jede Maßnahme auf eine Kurzbeschreibung mit Literaturhinweisen verwiesen (siehe IEC 61508-7, Anhänge A und B).

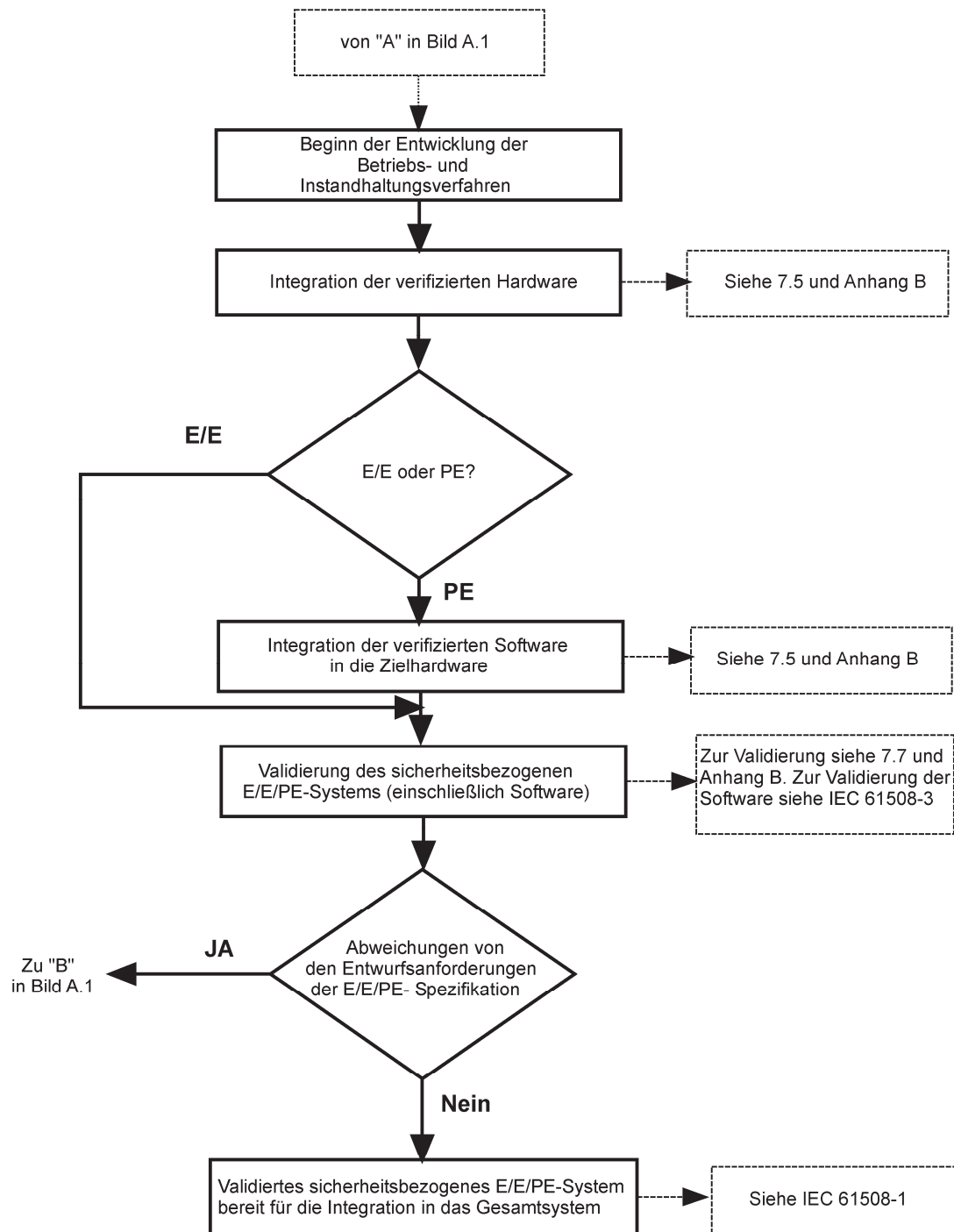
[Anhang B](#) stellt ein mögliches Verfahren zur Berechnung der Wahrscheinlichkeiten von Hardwareausfällen für sicherheitsbezogene E/E/PE-Systeme vor.

ANMERKUNG 4 Andere als in der Norm festgelegte Maßnahmen sind bei der Anwendung dieser Schritte ebenfalls annehmbar, wenn sie während der Planung der Sicherheit schriftlich begründet werden (siehe IEC 61508-1, Abschnitt 6).



ANMERKUNG Für sicherheitsbezogene PE-Systeme werden die Tätigkeiten für die Software gleichzeitig durchgeführt. (siehe Bild A.3).

Bild A.1 – Anwendung der IEC 61508-2



ANMERKUNG Für sicherheitsbezogene PE-Systeme werden die Tätigkeiten für die Software gleichzeitig durchgeführt. (siehe Bild A.3).

Bild A.2 – Anwendung der IEC 61508-2 (Fortsetzung von Bild A.1)

A.3 Funktionale Schritte bei der Anwendung der IEC 61508-3

Die funktionalen Schritte für die IEC 61508-3 (siehe [Bild A.3](#)) sind wie folgt:

- a) Erhalt der Anforderungen an die sicherheitsbezogenen E/E/PE-Systeme und der zutreffenden Teile der Planung der Sicherheit (siehe IEC 61508-2, 7.3). Angemessene Aktualisierung der Planung der Sicherheit während der Softwareentwicklung.

ANMERKUNG 1 Frühere Lebenszyklusphasen haben bereits:

- die erforderlichen Sicherheitsfunktionen und ihre Sicherheits-Integritätslevel festgelegt (siehe IEC 61508-1, 7.4 und 7.5),
 - die Sicherheitsfunktionen sicherheitsbezogenen E/E/PE-Systemen zugewiesen (siehe IEC 61508-1, 7.6) und
 - Funktionen der Software innerhalb jedes sicherheitsbezogenen E/E/PE-Systems zugewiesen (siehe IEC 61508-2, 7.2).
- b) Bestimmung der Softwarearchitektur für alle Sicherheitsfunktionen, die der Software zugewiesen worden sind (siehe IEC 61508-3, 7.4 und IEC 61508-3, Anhang A).
 - c) Überprüfung der Software und Hardwarearchitektur und der sicherheitstechnischen Auswirkungen der Abwägungen zwischen Software und Hardware (siehe IEC 61508-2, Bild 4) mit dem Lieferanten/Entwickler des sicherheitsbezogenen E/E/PE-Systems. Falls notwendig, Wiederholung dieses Schrittes.
 - d) Beginn der Planung für die Verifikation und Validierung der Sicherheit der Software (siehe IEC 61508-3, 7.3 und 7.9).
 - e) Entwurf, Entwicklung und Verifizieren/Testen der Software gemäß:
 - der Planung der Sicherheit der Software;
 - dem Software-Sicherheits-Integritätslevel; und
 - dem Software-Sicherheitslebenszyklus.
 - f) Vervollständigen der abschließenden Tätigkeiten der Softwareverifikation und Integration der verifizierten Software in die Zielhardware (siehe IEC 61508-3, 7.5) und parallel dazu Entwicklung der Softwareaspekte der Verfahren, denen Anwender und Instandhaltungspersonal beim Betrieb des Systems zu folgen haben (siehe IEC 61508-3, 7.6 und A.2 k)).
 - g) Validierung der Software in den integrierten sicherheitsbezogenen E/E/PE-Systemen (siehe IEC 61508-3, 7.7) zusammen mit dem Hardwareentwickler (siehe IEC 61508-2, 7.7).
 - h) Übergabe der Ergebnisse der Validierung der Sicherheit der Software an die Systemingenieure für die weitere Integration in das Gesamtsystem.
 - i) Falls eine Modifikation der Software des sicherheitsbezogenen E/E/PE-Systems während der Betriebszeit notwendig wird, erneute Anwendung dieser Phase der IEC 61508-3 in angemessener Weise (siehe IEC 61508-3, 7.8).

Einige Tätigkeiten finden im gesamten Software-Sicherheitslebenszyklus statt. Darunter sind die Verifikation (siehe IEC 61508-3, 7.9) und die Beurteilung der funktionalen Sicherheit (siehe IEC 61508-3, Abschnitt 8).

Durch Anwendung der obigen Schritte werden sicherheitsrelevante Verfahren und Maßnahmen für die Software im Hinblick auf den erforderlichen Sicherheits-Integritätslevel ausgewählt. Zur Hilfestellung bei dieser Auswahl sind Tabellen mit der Einordnung der verschiedenen Verfahren/Maßnahmen unter die vier Sicherheits-Integritätslevel (siehe IEC 61508-3, Anhang A) formuliert worden. In den Tabellen wird für jedes Verfahren und jede Maßnahme auf eine Kurzbeschreibung mit Literaturhinweisen verwiesen (siehe IEC 61508-7, Anhang C).

Ausgearbeitete Beispiele für die Anwendung der Tabellen zur Sicherheitsintegrität werden in [Anhang E](#) gegeben, und IEC 61508-7 beinhaltet einen probabilistischen Ansatz für die Bestimmung der Sicherheitsintegrität von bereits entwickelter Software (siehe IEC 61508-7, Anhang D).

ANMERKUNG 2 Andere als in dieser Norm festgelegte Maßnahmen sind bei der Anwendung dieser Schritte ebenfalls annehmbar, wenn sie während der Planung der Sicherheit schriftlich begründet werden (siehe IEC 61508-1, Abschnitt 6).

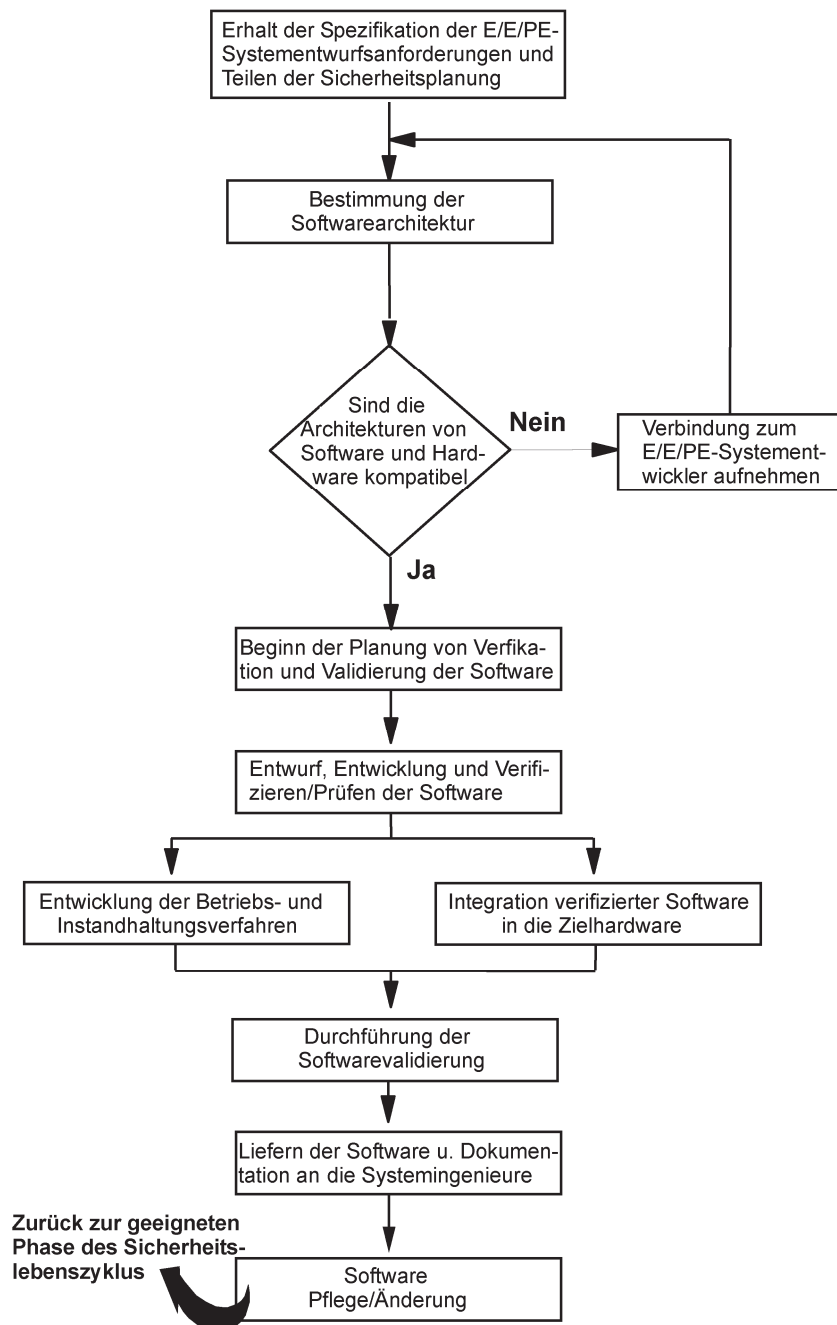


Bild A.3 – Anwendung der IEC 61508-3

Anhang B (informativ)

Beispielverfahren für die Bewertung von Ausfallwahrscheinlichkeiten der Hardware

B.1 Allgemeines

Dieser Anhang stellt mögliche Verfahren für die Berechnung der Ausfallwahrscheinlichkeiten der Hardware von nach IEC 61508-1, IEC 61508-2 und IEC 61508-3 errichteten sicherheitsbezogenen E/E/PE-Systemen dar. Er ist informativ und sollte nicht als Darstellung der einzigen möglichen Bewertungsverfahren interpretiert werden. Er stellt jedoch sowohl einen verhältnismäßig einfachen Ansatz für die Beurteilung der Fähigkeiten von sicherheitsbezogenen E/E/PE-Systemen dar, als auch eine Anleitung für die Verwendung alternativer Verfahren, die von den herkömmlichen Methoden zur Zuverlässigkeitsberechnung abgeleitet sind.

ANMERKUNG 1 Die in diesem Teil gezeigten Systemarchitekturen stellen Beispiele dar und ihre Darstellung erhebt keinen Anspruch auf Vollständigkeit, da es viele andere Architekturen gibt, die verwendet werden können.

ANMERKUNG 2 Siehe ISA-TR84.00.02-2002 [17] in den Literaturhinweisen.

Einige Zuverlässigkeitsverfahren sind mehr oder weniger direkt für die Analyse der Sicherheitsintegrität der Hardware sicherheitsbezogener E/E/PE-Systeme anwendbar. Üblicherweise werden sie nach den folgenden zwei Gesichtspunkten unterteilt:

- Modelle: statische (boolesch) im Vergleich zu dynamischen (Zustände/Übergänge);
- Berechnungen: analytische im Vergleich zu Monte-Carlo-Simulationen.

Die Booleschen Modelle umfassen alle Modelle, welche die statischen logischen Verknüpfungen zwischen einfachen Ausfällen und Ausfällen, die das gesamte System betreffen, beschreiben. Zu den Booleschen Modellen gehören Zuverlässigkeitsblockdiagramme (RBD, en: reliability block diagram) (siehe IEC 61508-7, C.6.4 und IEC 61078 [4]) und Fehlerbäume (FTA) (siehe IEC 61508-7, B.6.6.5 und B.6.6.9 und IEC 61025 [18]).

Die Zustands-Übergangs-Modelle umfassen alle Modelle, die beschreiben, wie sich das System entsprechend der auftretenden Ereignisse (Ausfälle, Reparaturen, Tests usw.) verhält (Übergänge von einem in den anderen Zustand). Das Markov-Modell (siehe IEC 61508-7, B.6.6.6 und IEC 61165 [5]), Petri-Netze (siehe IEC 61508-7, B.2.3.3 und B.6.6.10 und IEC 62551 [19]) und formale Sprachmodelle gehören zu den Zustands-Übergangs-Modellen. Es werden zwei Ansätze des Markov-Modells untersucht: ein vereinfachter Ansatz basierend auf spezifischen Formeln (B.3) und ein allgemeiner Ansatz, der Berechnungen unmittelbar an Graphen des Markov-Modells (B.5.2) ermöglicht. Für Sicherheitssysteme, die nicht nach Markov modelliert werden können, können stattdessen Monte-Carlo-Simulationen verwendet werden. Mit heutigen PCs ist dies selbst für SIL 4-Berechnungen erreichbar. Die Unterabschnitte B.5.3 und B.5.4 dieses Anhangs enthalten Anleitungen zur Anwendung der Monte-Carlo-Simulation (siehe IEC 61508-7, B.6.6.8) auf Verhaltensmodelle basierend auf Petri-Netzen und formalen Sprachmodellen.

Der vereinfachte Ansatz, der zuerst vorgestellt wird, basiert auf grafischen RBD-Darstellungen und spezifischen Formeln des Markov-Modells, erhalten aus Taylor-Reihen und den zugrunde liegenden, leicht konservativen in B.3.1 beschriebenen Hypothesen.

All diese Verfahren können für die Mehrzahl von sicherheitsbezogenen Systeme verwendet werden und wenn für jede einzelne Anwendung entschieden wird, welches Verfahren angewendet wird, ist es sehr wichtig, dass der Anwender mit der Anwendung des Verfahrens vertraut ist. Dies kann wichtiger sein als die Wahl des Verfahrens selbst. Es liegt in der Verantwortung des Analytikers nachzuweisen, dass die zugrunde liegenden Hypothesen jeder einzelnen Methode erfüllt sind oder ob Anpassungen erforderlich sind, um ein ausreichend realistisches, konservatives Ergebnis zu erhalten. Im Fall schlechter Zuverlässigkeitsdaten oder eines dominanten Ausfalls infolge gemeinsamer Ursache kann die Anwendung der einfachsten Modelle/

Verfahren ausreichend sein. Ob der Genauigkeitsverlust maßgeblich ist, kann nur unter den jeweiligen Umständen ermittelt werden.

Wenn für die Durchführung der Berechnung Softwareprogramme verwendet werden, muss der in der Praxis Tätige die von dem Softwarepaket verwendeten Formeln/Verfahren verstehen, um sicherzustellen, dass deren Verwendung für die bestimmte Anwendung ausreichend ist. Er sollte außerdem durch einige manuell berechnete Testfälle das Ergebnis des Softwareprogramms überprüfen.

Stellt ein Ausfall des EUC-Leit- oder Steuerungssystems eine Anforderung an das sicherheitsbezogene E/E/PE-System, hängt die Wahrscheinlichkeit eines gefährlichen Vorfalls auch von der Wahrscheinlichkeit eines Ausfalls des EUC-Leit- oder Steuerungssystems ab. In dieser Situation ist es notwendig, die Möglichkeit gleichzeitiger Ausfälle von Komponenten des EUC-Leit- oder Steuerungssystems und des sicherheitsbezogenen E/E/PE-Systems aufgrund von Ausfallmechanismen mit gemeinsamer Ursache zu betrachten. Bei unzureichender Berücksichtigung können solche Ausfälle zu einem höheren als dem erwarteten Restrisiko führen.

B.2 Betrachtungen zu grundlegenden Wahrscheinlichkeitsberechnungen

B.2.1 Einleitung

Das Zuverlässigkeitsblockdiagramm (RBD) in Bild B.1 zeigt eine PLT-Schutzeinrichtung mit drei Sensoren (A, B, C), einem Logiksystem (D), zwei Stellgliedern (E, F) und Ausfällen infolge gemeinsamer Ursachen (CCF).

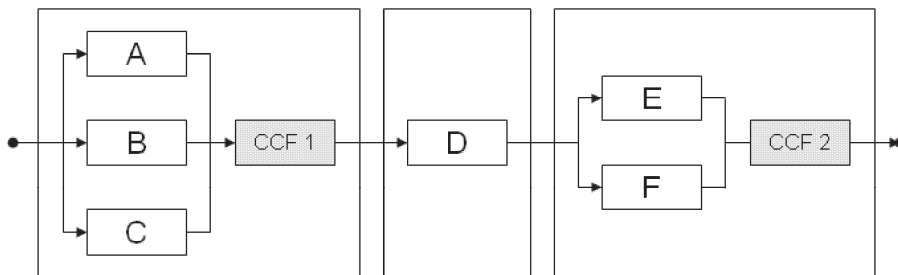


Bild B.1 – Zuverlässigkeitsblockdiagramm einer vollständigen PLT-Schutzeinrichtung

Dies ermöglicht die Identifikation von fünf Fehlerkombinationen, die zum Ausfall des sicherheitsbezogenen E/E/PE-Systems führen. Jedes ist ein sogenannter Minimalschnitt (en: minimal cut set):

- (A, B, C) ist ein Dreifachausfall,
- (E, F) ist ein Doppelausfall,
- (D), (CCF1), (CCF2) sind Einzelausfälle.

B.2.2 Sicherheitsbezogenes E/E/PE-System mit niedriger Anforderungsrate

Wenn ein sicherheitsbezogenes E/E/PE-System in der Betriebsart mit niedriger Anforderungsrate verwendet wird, verlangt die Norm die Beurteilung dessen $PF_{D_{avg}}$ (d. h. dessen mittlerer Nichtverfügbarkeit). Diese ist schlicht das Verhältnis $MDT(T)/T$, wobei $MDT(T)$ die mittlere Ausfalldauer des sicherheitsbezogenen E/E/PE-Systems über den Zeitraum $[0, T]$ ist.

Die Wahrscheinlichkeit des Ausfalls ist für ein Sicherheitssystem in der Regel sehr gering und die Wahrscheinlichkeit des gleichzeitigen Auftretens zweier Minimalschnitte ist vernachlässigbar. Daher ergibt die Summe der mittleren Ausfalldauern infolge der einzelnen Minimalschnitte eine konservative Schätzung der mittleren Ausfalldauer des Gesamtsystems. Aus Bild B.1 kann entnommen werden:

$$MDT \approx MDT^{ABC} + MDT^D + MDT^{EF}$$

Dividiert durch T ergibt dies:

$$PFD_{avg} \approx PFD_{avg}^{ABC} + PFD_{avg}^D + PFD_{avg}^{EF}$$

Daher sind die Berechnungen von PFD_{avg} für in Reihe geschaltete Teile sehr ähnlich denen, die mit gewöhnlichen Wahrscheinlichkeiten durchgeführt werden, wenn diese sehr klein im Vergleich zu 1 sind.

Für parallel angeordnete Teile, wo erst bei Mehrfachausfällen etwa von (E, F) ein Funktionsverlust eintritt, ist jedoch klar, dass $MDT^{EF NA1)}$ nicht direkt aus MDT^E und MDT^F berechnet werden kann. Die MDT des (E, F)-Systems wird wie folgt berechnet:

$$MDT^{EF} = \int_0^T PFD^E(t) PFD^F(t) dt$$

Daher sind die gewöhnlichen Wahrscheinlichkeitsberechnungen (Additionen und Multiplikationen) für die PFD_{avg} -Berechnungen (Integrale) von parallel geschalteten Teilen nicht gültig. PFD_{avg} hat nicht die gleichen Eigenschaften einer echten Wahrscheinlichkeit und die Anpassung daran würde voraussichtlich nicht zu einem konservativen Ergebnis führen. Insbesondere ist es nicht möglich, nur durch das Zusammenfassen der $PFD_{avg,i}$ seiner Komponenten auf konventionelle Weise die PFD_{avg} eines sicherheitsbezogenen E/E/PE-Systems zu erhalten. Da dies zuweilen von den käuflichen booleschen Softwareprogrammen so unterstützt wird, sollten die Analytiker aufmerksam sein, um solche nicht konservativen Berechnungen, welche im Umgang mit der Sicherheit unerwünscht sind, zu verhindern.

BEISPIEL Für einen redundanten (1oo2) Kanal mit einer Rate gefahrbringender unerkannter Ausfälle λ_{DU} und einem Intervall τ für die Wiederholungsprüfung könnte eine ungenaue Wahrscheinlichkeitsberechnung $(\lambda_{DU} \cdot \tau)^2/4$ ergeben, bei einem tatsächlichen Ergebnis von $(\lambda_{DU} \cdot \tau)^2/3$.

Die Berechnungen können analytisch oder unter Verwendung von Monte-Carlo-Simulation durchgeführt werden. Dieser Anhang beschreibt die Ausführung unter Verwendung konventioneller Zuverlässigkeitsmodelle basierend auf booleschen Modellen (RBD oder Fehlerbaum) oder Zustands-Übergangs-Modellen (Markov, Petri-Netze, usw.)

B.2.3 Sicherheitsbezogenes E/E/PE-System mit hoher Anforderungsrate oder kontinuierlicher Anforderung

B.2.3.1 Allgemeine PFH-Formel

Wenn ein sicherheitsbezogenes E/E/PE-System in der Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung verwendet wird, verlangt die Norm die Berechnung seiner PFH (d. h. der mittleren Häufigkeit eines gefahrbringenden Ausfalls). Dies ist der Mittelwert der sogenannten unbedingten Ausfallintensität $w(t)$ (auch Ausfallhäufigkeit genannt) über den betreffenden Zeitraum:

$$PFH(T) = \frac{1}{T} \int_0^T w(t) dt$$

Arbeitet das sicherheitsbezogene E/E/PE-System in der Betriebsart mit kontinuierlicher Anforderung und bildet es die allerletzte Barriere für die Sicherheit, dann führt der Gesamtausfall des sicherheitsbezogenen E/E/PE-Systems unmittelbar zu einer möglicherweise gefährlichen Situation. Deshalb kann für Ausfälle, die den Verlust der Gesamtsicherheitsfunktion verursachen, eine Reparatur des sicherheitsbezogenen Gesamtsystems in der Berechnung nicht berücksichtigt werden. Wenn der Ausfall des sicherheitsbezogenen Gesamtsystems jedoch aufgrund einer anderen Sicherheitsbarriere oder des Ausfalls einer Einrichtung nicht unmittelbar zu einer möglichen Gefahr führt, dann ist es möglich, die Erkennung und die Reparatur des sicherheitsbezogenen Systems in seiner Berechnung der Risikominderung zu berücksichtigen.

NA1) Nationale Fußnote: Für die Bedeutung der Indizes siehe DIN EN 61508-4 (VDE 0803-4):2011, 3.6.15.

B.2.3.2 Unzuverlässigkeit (z. B. eine einzelne Barriere arbeitet in der Betriebsart mit kontinuierlicher Anforderung)

Dieser Fall ist von Bedeutung, wenn das sicherheitsbezogene E/E/PE-System, welches in der Betriebsart mit kontinuierlicher Anforderung arbeitet, die allerletzte Barriere für die Sicherheit bildet. Sobald es ausfällt, kann eine mögliche Gefährdung eintreten. Es sind keine Ausfälle des Gesamtsystems über den betreffenden Zeitraum zulässig.

In diesem Fall kann die *PFH* mit Hilfe der Unzuverlässigkeit über den betreffenden Zeitraum berechnet werden.

$$F(T): PFH(T) = \frac{1 - \exp\left[-\int_0^T \Lambda(t) dt\right]}{T} = \frac{F(T)}{T}$$

Die Ausfallrate $\Lambda(t)$ des Gesamtsystems kann zeitabhängig oder konstant sein.

$$\text{Bei Zeitabhängigkeit gilt: } PFH(T) = \frac{1 - \exp(-\Lambda_{avg} \cdot T)}{T} \approx \Lambda_{avg}$$

Wenn das System aus vollständig und schnell reparierbaren Bauteilen mit konstanten Ausfall- und Reparaturraten besteht (z. B. gefahrbringende erkannte Ausfälle), erreicht $\Lambda(t)$ schnell einen konstanten asymptotischen Wert Λ_{as} und, falls $PFH(T) \ll 1$, gilt:

$$PFH(T) = \frac{1 - \exp(-\Lambda_{as} \cdot T)}{T} \approx \Lambda_{as} = \frac{1}{MTTF}$$

Λ_{as} ist nur vorhanden, wenn das sicherheitsbezogene E/E/PE-System in der Betriebsart mit kontinuierlicher Anforderung arbeitet und nur sichere und DD-Ausfälle (d. h. schnell erkannt und repariert) auftreten. Reparaturen von Ausfällen, die unmittelbare Ursache des Gesamtausfalls der Sicherheitsfunktion sein können, können nicht berücksichtigt werden. Bei einer redundanten Konfiguration, bei der es darauf ankommt, die Wiederholungsprüfungen zu berücksichtigen, ist die asymptotische Ausfallrate nicht von Bedeutung und es sind die vorhergehenden Gleichungen anzuwenden. Es ist die Aufgabe des Analysten, zu bestimmen, welcher Fall zutreffend ist.

B.2.3.3 Nichtverfügbarkeit (z. B. mehrere Sicherheitsbarrieren)

Arbeitet das sicherheitsbezogene E/E/PE-System in der Betriebsart mit kontinuierlicher Anforderung und bildet es nicht die allerletzte Barriere, erhöhen dessen Ausfälle lediglich die Anforderungshäufigkeit auf die anderen Sicherheitsbarrieren, oder arbeitet es in der Betriebsart mit hoher Anforderungsrate, so ist es möglich, einen Fehler, der unmittelbar die Ursache für den Verlust der Sicherheitsfunktion sein könnte, innerhalb des erwarteten Anforderungszeitraum zu erkennen (automatisch oder manuell) und zu reparieren. Unter diesen Umständen kann dessen Gesamtausfall behoben werden, und die *PFH* kann aus der Verfügbarkeit $A(t)$ und aus der bedingten Ausfallintensität $\Lambda_v(t)$ des Systems berechnet werden.

Besteht das System wiederum aus Komponenten, die vollständig und schnell zu reparieren sind (d. h. wenn es in allen sich verschlechternden Situationen eine hohe Wahrscheinlichkeit gibt, schnell wieder in einen funktionierenden Zustand zu gelangen), erreicht $\Lambda_v(t)$ schnell den asymptotischen Wert Λ_{vas} , welcher darüber hinaus auch ein guter Schätzwert der in B.2.3.2 dargestellten wahren asymptotischen Ausfallrate Λ_{as} des Gesamtsystems ist.

Dies führt zu den folgenden Näherungen:

$$PFH = \frac{1}{MUT + MDT} = \frac{1}{MTBF} \approx \frac{1}{MUT} \approx \frac{1}{MTTF}$$

Dabei ist

- MUT die Abkürzung für die mittlere ausfallfreie Betriebsdauer;
- MDT die Abkürzung für die mittlere Ausfalldauer;
- MTBF die Abkürzung für die mittlere Betriebsdauer zwischen Ausfällen; und
- MTTF die Abkürzung für die mittlere Dauer bis zum Ausfall.

B.2.3.4 Betrachtungen zur Ausfallrate

Einige der obigen Formeln verwenden die Ausfallrate $\Lambda(t)$ des Gesamtsystems. Deren Berechnung ist nicht so einfach und erfordert einige Überlegungen.

In Reihe geschaltete Strukturen sind sehr leicht zu handhaben, da die Ausfallraten addiert werden können. Aus dem [Bild B.1](#) können wir entnehmen: $\Lambda(t) = \Lambda^{abc}(t) + \lambda^{CCF1}(t) + \lambda^d(t) + \Lambda^{ef}(t) + \lambda^{CCF2}(t)$, wobei $\Lambda(t)$ die Gesamtausfallrate des sicherheitsbezogenen E/E/PE-Systems ist und $\Lambda^{abc}(t)$, $\lambda^{CCF1}(t)$, $\lambda^d(t)$, $\Lambda^{ef}(t)$ und $\lambda^{CCF2}(t)$ die Ausfallraten der fünf Minimalschnitte sind.

Für parallele Strukturen ist dies nicht so leicht, da keine einfachen Beziehungen zu den Ausfallraten der einzelnen Komponenten existieren. Als Beispiel dient die Betrachtung des Minimalschnittes (E, F):

- 1) Wenn E und F nicht unmittelbar ersetzt werden können (z. B. DU-Ausfälle), wechselt $\Lambda^{ef}(t)$ kontinuierlich von 0 zu λ (Ausfallrate von E oder F). Ein asymptotischer Wert wird erreicht, wenn eine der beiden Komponenten voraussichtlich ausgefallen sein wird. Dies ist ein sehr langsamer Prozess, da dies eintritt, wenn t größer als $1/\lambda$ wird. Dieser asymptotische Wert wird tatsächlich niemals erreicht, wenn E und F periodisch einer Wiederholungsprüfung mit einem Testintervall von $\tau \ll 1/\lambda$ unterzogen werden.
- 2) Wenn E und F in einer relativ kurzen Zeitspanne ersetzt werden (z. B. DD-Ausfälle), geht $\Lambda^{ef}(t)$ sehr schnell in einen asymptotischen Wert $\Lambda_{AS}^{ef} = 2\lambda^2/\mu$ über, der als eine entsprechende kontinuierliche Ausfallrate verwendet werden kann. Dieser wird erreicht, wenn t zwei- oder dreimal größer wird, als die größte MTTR der Komponenten. Dies ist ein spezieller Fall der vollständig und schnell reparierbaren Systeme, die oben behandelt wurden.

Das Abschätzen der Ausfallrate des Gesamtsystems setzt daher im Allgemeinen komplexere Berechnungen voraus, als für die einfacheren in Reihe geschaltete Strukturen.

B.3 Zuverlässigkeitsblockdiagramm-Ansatz mit angenommener konstanter Ausfallrate

B.3.1 Grundlegende Hypothese

Die Berechnungen basieren auf den folgenden Annahmen:

- die sich ergebende mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für das System ist kleiner als 10^{-1} oder die sich ergebende mittlere Häufigkeit eines gefahrbringenden Ausfalls des Systems ist kleiner als 10^{-5} h^{-1} ,

ANMERKUNG 1 Diese Annahme bedeutet, dass das sicherheitsbezogene E/E/PE-System im Anwendungsbereich der IEC 61508 liegt und sich innerhalb des SIL 1-Bandes befindet (siehe IEC 61508-1, Tabellen 2 und 3).

- die Bauteilausfallraten sind während der Lebensdauer des Systems konstant;
- das Sensor-(Eingangs-)Teilsystem besteht aus dem/den eigentlichen Sensor(en) und allen anderen Bauteilen und Verdrahtungen, bis hin zu denjenigen, in denen die Signale erstmalig durch Ausgangsvergleich oder eine andere Verarbeitung zusammengeführt werden, letztere aber nicht mit eingeschlossen (z. B. eine zweikanalige Sensorkonfiguration nach [Bild B.2](#));
- das Logik-Teilsystem besteht aus dem/den Bauteil(en), in denen die Signale erstmalig zusammengeführt werden, sowie aus allen anderen Bauteilen bis hin zu denjenigen, die die Ausgangssignale dem Ausgangs-Teilsystem übergeben, letztere mit eingeschlossen;

- das Stellglied-(Ausgangs-)Teilsystem besteht aus allen Bauteilen und Verdrahtungen, die die Ausgangssignale des Logik-Teilsystems verarbeiten, die Stellglieder eingeschlossen;
- die Hardwareausfallraten, die als Eingangswerte für die Berechnungen und Tabellen herangezogen werden, gelten für einen Kanal eines Teilsystems (wenn z. B. 2oo3-Sensoren verwendet werden, wird die Ausfallrate eines einkanalen Sensors genommen und die Auswirkung von 2oo3 gesondert berechnet);
- die Kanäle in einer Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider haben alle die gleichen Ausfallraten und Diagnosedeckungsgrade;
- die Gesamtausfallrate der Hardware eines Kanals eines Teilsystems ist die Summe der Rate der gefahrbringenden Ausfälle und der Rate der sicheren Ausfälle, die als gleich angenommen werden;

ANMERKUNG 2 Diese Annahme beeinflusst den Anteil sicherer Ausfälle (siehe IEC 61508-2, Anhang C), dieser beeinflusst aber nicht die berechneten Werte der Ausfallwahrscheinlichkeiten in diesem Anhang.

- für jede Sicherheitsfunktion gibt es eine vollständige Wiederholungsprüfung und Reparatur (d. h. alle Ausfälle, die unerkannt geblieben sind, werden bei der Wiederholungsprüfung erkannt), für den Fall einer unvollständigen Wiederholungsprüfung siehe jedoch [B.3.2.5](#);
- das Intervall für die Wiederholungsprüfung ist mindestens um eine Zehnerpotenz größer als die MTR;
- für jedes Teilsystem gibt es genau ein Intervall für die Wiederholungsprüfung und die MTR;
- das erwartete Intervall zwischen den Anforderungen ist mindestens um eine Zehnerpotenz größer als das Intervall für die Wiederholungsprüfung;
- für alle Teilsysteme, die in der Betriebsart mit niedriger Anforderungsrate betrieben werden, und für 1oo2-, 1oo2D-, 1oo3- und 2oo3-Systeme mit Ausgangsvergleich oder Mehrheitsentscheider, die in der Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung betrieben werden, wird der durch den Diagnosedeckungsgrad festgelegte Anteil von Ausfällen innerhalb der MTTR sowohl erkannt als auch repariert. Diese Zeit wurde bei der Festlegung der Anforderungen an die Sicherheitsintegrität der Hardware benutzt;

BEISPIEL Falls eine MTTR von 8 h angenommen wird, schließt dies das Diagnosetestintervall ein, das typischerweise kleiner als 1 h ist, der Rest ist die MRT.

ANMERKUNG 3 Für 1oo2-, 1oo2D-, 1oo3- und 2oo3-Gruppen mit Ausgangsvergleich oder Mehrheitsentscheider wird angenommen, dass jede Reparatur bei laufendem Betrieb durchgeführt wird. Wenn ein sicherheitsbezogenes E/E/PE-System so konfiguriert wird, dass jeder erkannte Fehler die EUC-Einrichtung in einen sicheren Zustand versetzt, dann wird die mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung verbessert. Der Grad der Verbesserung hängt vom Diagnosedeckungsgrad ab.

- für 1oo1- und 2oo2-Gruppen mit Ausgangsvergleich, die in der Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung betrieben werden, geht das sicherheitsbezogene E/E/PE-System nach Erkennen eines gefahrbringenden Fehlers immer in einen sicheren Zustand über. Um dies zu erreichen, ist das erwartete Intervall zwischen den Anforderungen mindestens um eine Zehnerpotenz größer als das Diagnosetestintervall oder die Summe der Diagnosetestintervalle, und die Zeit, um den sicheren Zustand zu erreichen, ist kleiner als die Prozess-Sicherheitszeit;

ANMERKUNG 4 Zur Prozess-Sicherheitszeit siehe IEC 61508-4, 3.6.20.

- wenn ein Ausfall der Energieversorgung ein sicherheitsbezogenes E/E/PE-System betrifft und das System beim Abschalten der Energie einen sicheren Zustand einnimmt, beeinflusst die Energieversorgung nicht die mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung des sicherheitsbezogenen E/E/PE-Systems. Falls jedoch zum Einnehmen des sicheren Zustandes des Systems das Aufrechterhalten der Versorgung notwendig ist oder die Energieversorgung ein Ausfallverhalten hat, das einen unsicheren Betrieb des sicherheitsbezogenen E/E/PE-Systems verursachen kann, dann sollte die Energieversorgung in die Bewertung mit eingeschlossen werden;
- wenn der Ausdruck Kanal verwendet wird, beschränkt sich dies auf den betrachteten Teil des Systems, also üblicherweise auf das Sensor-, Logik- oder Stellglied-Teilsystem;
- die Abkürzungen der verwendeten Benennungen sind in [Tabelle B.1](#) enthalten.

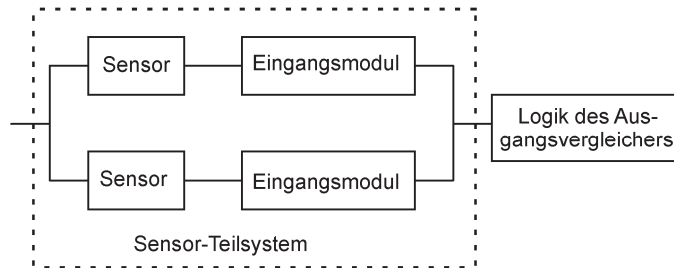


Bild B.2 – Beispielkonfiguration für zwei Kanäle mit Sensoren

Tabelle B.1 – In diesem Anhang verwendete Benennungen und ihre zugehörigen Parameterbereiche
(zutreffend für 1oo1-, 1oo2-, 2oo2-, 1oo2D-, 1oo3- und 2oo3-Architekturen)

Abkürzung	Beschreibung (Einheit)	Parameterbereiche in den Tabellen B.2 bis B.5 und B.10 bis B.13
T_1	Intervall der Wiederholungsprüfung (in Stunden)	Ein Monat (730 h) ¹⁾ Drei Monate (2 190 h) ¹⁾ Sechs Monate (4 380 h) Ein Jahr (8 760 h) Zwei Jahre (17 520 h) ²⁾ Zehn Jahre (87 600 h) ²⁾
$MTTR$	Mittlere Dauer bis zur Wiederherstellung (en: Mean time to restoration) (in Stunden)	8 h ANMERKUNG: $MTTR = MTR = 8$ Stunden basiert auf der Annahme, dass die Dauer bis zur Erkennung eines gefahrbringenden Ausfalls bei einer automatischen Erkennung $\ll MRT$ ist.
MRT	Mittlere Reparaturdauer (en: Mean repair time) (in Stunden)	8 h ANMERKUNG: $MTTR = MTR = 8$ Stunden basiert auf der Annahme, dass die Dauer bis zur Erkennung eines gefahrbringenden Ausfalls bei einer automatischen Erkennung $\ll MRT$ ist.
DC	Diagnosedeckungsgrad (in Gleichungen als Bruch dargestellt, ansonst als Prozentwert)	0 % 60 % 90 % 99 %
β	Anteil unerkannter Ausfälle infolge gemeinsamer Ursache (in Gleichungen als Bruch dargestellt, ansonst als Prozentwert). (In den Tabellen B.2 bis B.5 und B.10 bis B.13 wird $\beta = 2 \times \beta_D$ angenommen.)	2 % 10 % 20 %
β_D	Der Anteil der Ausfälle infolge gemeinsamer Ursache, die durch den Diagnosetest erkannt werden (in Gleichungen als Bruch dargestellt, ansonst als Prozentwert). (In den Tabellen B.2 bis B.5 und B.10 bis B.13 wird $\beta = 2 \times \beta_D$ angenommen.)	1 % 5 % 10 %
$\lambda_{DU}^{NA2)}$	Rate gefahrbringender unerkannter Ausfälle (je Stunde) eines Kanals in einem Teilsystem	$0,05 \times 10^{-6}$ $0,25 \times 10^{-6}$ $0,5 \times 10^{-6}$ $2,5 \times 10^{-6}$ 5×10^{-6} 25×10^{-6}

^{NA2)} Nationale Fußnote: Die dargestellte Schreibweise λ_{DU} mit dem zweiten Indexbuchstaben als Großbuchstabe wird in diesem Teil und anderen Teilen der Norm nicht durchgängig verwendet. Teilweise wird Kleinschreibung verwendet (λ_{du}), dies gilt gleichermaßen auch für λ_{DD} und λ_{SD} .

Tabelle B.1 (fortgesetzt)

Abkürzung	Beschreibung (Einheit)	Parameterbereich der Tabellen B.2 bis B.5 und B.10 bis B.13
PFD_G	Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung einer Gruppe von Kanälen mit Ausgangsvergleicher oder Mehrheitsentscheider (en: <i>PFD</i> probability of failure on demand). (Wenn das Sensor-, Logik- oder Stellglied-Teilsystem aus nur einer Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider besteht, dann ist PFD_G gleich PFD_S , PFD_L oder PFD_{FE} .)	
PFD_S	Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für das Sensor-Teilsystem	
PFD_L	Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für das Logik-Teilsystem	
PFD_{FE}	Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für das Stellglied-Teilsystem (en: final element subsystem)	
PFD_{SYS}	Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für die Sicherheitsfunktion eines sicherheitsbezogenen E/E/PE-Systems	
PFH_G	Mittlere Häufigkeit eines gefahrbringenden Ausfalls für eine Gruppe von Kanälen mit Ausgangsvergleicher oder Mehrheitsentscheider. (Wenn das Sensor-, Logik- oder Stellglied-Teilsystem aus nur einer Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider besteht, dann ist PFH_G gleich PFH_S , PFH_L oder PFH_{FE} .)	
PFH_S	Mittlere Häufigkeit eines gefahrbringenden Ausfalls für das Sensor-Teilsystem	
PFH_L	Mittlere Häufigkeit eines gefahrbringenden Ausfalls für das Logik-Teilsystem	
PFH_{FE}	Mittlere Häufigkeit eines gefahrbringenden Ausfalls für das Stellglied-Teilsystem	
PFH_{SYS}	Mittlere Häufigkeit eines gefahrbringenden Ausfalls für die Sicherheitsfunktion eines sicherheitsbezogenen E/E/PE-Systems	
λ	Gesamtausfallrate (je Stunde) eines Kanals in einem Teilsystem	
λ_D	Rate gefahrbringender Ausfälle (je Stunde) eines Kanals eines Teilsystems, entspricht $0,5 \lambda$ (mit angenommenen 50 % gefahrbringender Ausfälle und 50 % sicherer Ausfälle, D = en: dangerous = gefahrbringend)	
λ_{DD}	Rate erkannter gefahrbringender Ausfälle (je Stunde) eines Kanals eines Teilsystems. (Dies ist die Summe aller Raten erkannter gefahrbringender Ausfälle innerhalb eines Kanals eines Teilsystems, DD = en: dangerous detected = gefahrbringend erkannt.)	
λ_{DU}	Rate unerkannter gefahrbringender Ausfälle (je Stunde) eines Kanals eines Teilsystems. (Dies ist die Summe aller Raten unerkannter gefahrbringender Ausfälle innerhalb eines Kanals eines Teilsystems, DU = en: dangerous undetected = gefahrbringend unerkannt.)	
λ_{SD}	Rate erkannter sicherer Ausfälle (je Stunde) eines Kanals eines Teilsystems. (Dies ist die Summe aller Raten erkannter sicherer Ausfälle innerhalb eines Kanals eines Teilsystems, SD = en: safe detected = sicher erkannt.)	
t_{CE}	Mittlere Ausfalldauer eines Kanals (in Stunden) für 1001-, 1oo2-, 2oo2- und 2oo3-Architekturen. (Dies ist die gemeinsame Ausfalldauer für alle Komponenten in einem Kanal des Teilsystems.)	
t_{GE}	Mittlere Ausfalldauer einer Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider (in Stunden) für 1oo2- und 2oo3-Architekturen. (Dies ist die gemeinsame Ausfalldauer für alle Kanäle in einer Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider.)	
t_{CE}'	Mittlere Ausfalldauer (in Stunden) eines Kanals für eine 1oo2D-Architektur. (Dies ist die gemeinsame Ausfalldauer für alle Komponenten in einem Kanal des Teilsystems.)	
t_{GE}'	Mittlere Ausfalldauer einer Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider (in Stunden) für eine 1oo2D-Architektur. (Dies ist die gemeinsame Ausfalldauer für alle Kanäle in einer Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider.)	
T_2	Intervall zwischen den Anforderungen (h)	
K	Anteil des Erfolges der Eigentestschaltung im 1oo2D-System	
PTC	Deckungsgrad der Wiederholungsprüfung	
¹⁾ Nur Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung. ²⁾ Nur Betriebsart mit niedriger Anforderungsrate.		

B.3.2 Mittlere Ausfallwahrscheinlichkeit bei Anforderung (für die Betriebsart mit niedriger Anforderungsrate)

B.3.2.1 Verfahren für die Berechnung

Die mittlere Ausfallwahrscheinlichkeit bei Anforderung einer Sicherheitsfunktion eines sicherheitsbezogenen E/E/PE-Systems wird durch die Berechnung und Zusammenführung der mittleren Wahrscheinlichkeiten eines Ausfalls bei Anforderung aller Teilsysteme, die gemeinsam die Sicherheitsfunktion ausführen, bestimmt. Da die Wahrscheinlichkeiten in diesem Anhang klein sind, kann dies wie folgt ausgedrückt werden (siehe Bild B.3):

$$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE}$$

Dabei ist

- PFD_{SYS} die mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung einer Sicherheitsfunktion des sicherheitsbezogenen E/E/PE-Systems;
- PFD_S die mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für das Sensor-Teilsystem;
- PFD_L die mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für das Logik-Teilsystem; und
- PFD_{FE} die mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für das Stellglied-Teilsystem.

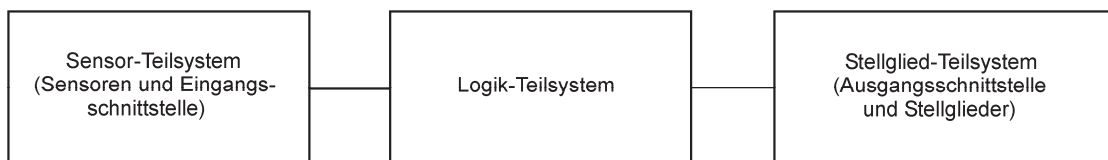


Bild B.3 – Struktur mit Teilsystemen

Um für jedes der Teilsysteme die mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung zu bestimmen, sollte das folgende Verfahren der Reihe nach für jedes Teilsystem angewendet werden:

- a) Zeichnen des Blockdiagramms, das die Bauteile des Sensor-Teilsystems (Eingang), des Logik-Teilsystems und des Stellglied-Teilsystems (Ausgang) aufzeigt. Bauteile des Sensor-Teilsystems können z. B. Sensoren, Schutzschaltungen oder Schaltungen zur Signalkonditionierung sein, Bauteile des Logik-Teilsystems z. B. Prozessoren und Abtasteinrichtungen, Bauteile des Stellglied-Teilsystems z. B. Signalumformer, Schutzschaltungen und Aktoren. Darstellung jedes Teilsystems als eine oder mehrere 1oo1-, 1oo2-, 2oo2-, 1oo2D-, 1oo3- oder 2oo3-Gruppen mit Ausgangsvergleicher oder Mehrheitsentscheider.
- b) Von den [Tabellen B.2 bis B.5](#) wird die zutreffende Tabelle aufgesucht, je nachdem, ob ein Intervall für die Wiederholungsprüfung von sechs Monaten, einem Jahr, zwei Jahren oder 10 Jahren vorgesehen ist. Diese Tabellen nehmen außerdem eine mittlere Dauer bis zur Wiederherstellung von 8 h für jeden Ausfall an, wenn er aufgedeckt worden ist.
- c) In der zutreffenden Tabelle für jede Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider im Teilsystem werden folgende Parameter aufgesucht:
 - Architektur (zum Beispiel 2oo3);
 - Diagnosedeckungsgrad jedes Kanals (zum Beispiel 60 %);
 - die Rate gefahrbringender Ausfälle (je Stunde) λ_D jedes Kanals (zum Beispiel $2,5 \times 10^{-06}$);
 - die β -Faktoren β und β_D für den Ausfall infolge gemeinsamer Ursachen, im Hinblick auf das Zusammenwirken der Kanäle in einer Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider (zum Beispiel 2 % bzw. 1 %).

ANMERKUNG 1 Es wird angenommen, dass jeder Kanal einer Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider den gleichen Diagnosedeckungsgrad und die gleiche Ausfallrate hat (siehe [Tabelle B.1](#)).

ANMERKUNG 2 In den Tabellen B.2 bis B.5 (und in den Tabellen B.10 bis B.13) wird angenommen, dass β , der β -Faktor ohne Diagnosetests (auch verwendet für bei Diagnosetests unerkannt bleibende gefahrbringende Ausfälle), das Zweifache von β_D , dem β -Faktor für durch Diagnosetests erkannte Ausfälle, beträgt.

- d) Aus der zugehörigen Tabelle (B.2 bis B.5) wird die mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für eine Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider entnommen.
- e) Wenn die Sicherheitsfunktion von mehr als einer Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider, die Sensoren enthält, oder von mehr als einer derartigen Gruppe mit Ausgangsvergleicher, die Stellglieder enthält, abhängt, sind die mittleren Ausfallwahrscheinlichkeiten bei Anforderung des Sensor-Teilsystems PFD_S und des Stellglied-Teilsystems PFD_{FE} durch nachfolgende Gleichungen bestimmt. Hierbei sind PFD_{Gi} und PFD_{Gj} die mittleren Ausfallwahrscheinlichkeiten bei Anforderung für jede Gruppe von Sensoren bzw. Stellgliedern mit Ausgangsvergleicher oder Mehrheitsentscheider:

$$PFD_S = \sum_i PFD_{Gi}$$

$$PFD_{FE} = \sum_j PFD_{Gj}$$

Die in allen Gleichungen verwendeten Formeln, sowohl für PFD als auch die Systemausfallrate, sind alle eine Funktion von Bauteilausfallraten und mittlerer Ausfalldauer (MDT). Dort, wo mehrere Elemente in dem System vorhanden sind und es erforderlich ist, die Gesamt- PFD kombinierter Elemente oder die Ausfallrate des Systems zu berechnen, ist es oft notwendig, einen einzelnen Wert für MDT in den Gleichungen zu verwenden. Jedes Element kann jedoch über eine andere Ausfallerkennung mit unterschiedlichen MDT verfügen und verschiedene Elemente können unterschiedliche MDT -Werte für ein und denselben Ausfallmechanismus aufweisen, wobei es in diesem Fall notwendig wird, einen einzelnen Wert für die MDT zu ermitteln, der für alle Elemente im Pfad gültig ist. Dies kann erreicht werden, indem die Gesamtausfallrate der gesamten Pfade berücksichtigt wird und dann die einzelnen $MDTs$ entsprechend ihres Ausfallratenanteils an der betrachteten Gesamtausfallrate aufgeteilt werden.

Wenn zum Beispiel zwei Elemente in Reihe geschaltet sind und eines einer Wiederholungsprüfung mit T_1 und das andere einer Wiederholungsprüfung mit T_2 unterworfen ist, dann beträgt der äquivalente Einzelwert für MDT :

$$\lambda_T = \lambda_1 + \lambda_2$$

und

$$MDT_E = \frac{\lambda_1}{\lambda_T} \left(\frac{T_1}{2} \right) + \frac{\lambda_2}{\lambda_T} \left(\frac{T_2}{2} \right)$$

B.3.2.2 Architekturen für die Betriebsart mit niedriger Anforderungsrate

ANMERKUNG 1 Dieser Unterabschnitt sollte der Reihe nach gelesen werden, da Gleichungen, die für mehrere Architekturen gültig sind, nur bei ihrer ersten Verwendung angegeben werden.

ANMERKUNG 2 Die Gleichungen basieren auf den in B.3.1 aufgeführten Annahmen.

ANMERKUNG 3 Die folgenden Beispiele stellen typische Konfigurationen dar, die Darstellung erhebt keinen Anspruch auf Vollständigkeit.

B.3.2.2.1 1oo1

Diese Architektur besteht aus einem einzelnen Kanal, bei ihr führt jeder gefahrbringende Ausfall zu einem Ausfall der Sicherheitsfunktion, wenn eine Anforderung auftritt.

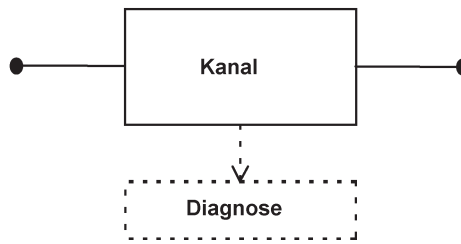


Bild B.4 – Blockschaltbild für 1oo1

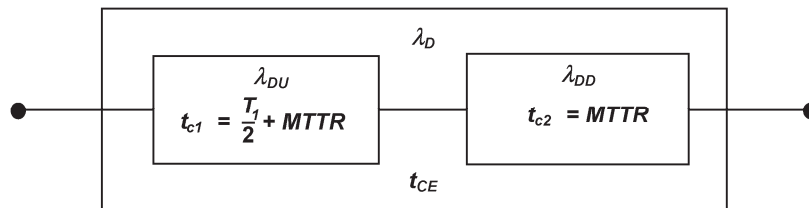


Bild B.5 – Zuverlässigkeitsblockdiagramm für 1oo1

Bild B.4 enthält das zugehörige Blockschaltbild und Bild B.5 das Zuverlässigkeitsblockdiagramm. Die Rate eines gefahrbringenden Ausfalls ist für einen Kanal gegeben durch:

$$\lambda_D = \lambda_{DU} + \lambda_{DD}$$

Bild B.5 zeigt, dass man sich einen Kanal als aus zwei Komponenten zusammengesetzt vorstellen kann, eine mit einer Rate für gefahrbringende Ausfälle λ_{DU} aufgrund unerkannter Ausfälle und eine mit einer Rate für gefahrbringende Ausfälle λ_{DD} aufgrund erkannter Ausfälle. Es ist möglich, die mittlere Ausfalldauer t_{CE} eines Kanals zu berechnen, indem man die einzelnen Ausfalldauern der beiden Komponenten t_{C1} und t_{C2} addiert, jeweils bewertet mit dem Verhältnis, mit dem sie in die Ausfallwahrscheinlichkeit des Kanals eingehen:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \left(\frac{T_1}{2} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

Für jede Architektur ist die Rate erkannter gefahrbringender Ausfälle und die Rate unerkannter gefahrbringender Ausfälle bestimmt durch:

$$\lambda_{DU} = \lambda_D(1 - DC); \quad \lambda_{DD} = \lambda_D DC$$

Für einen Kanal mit einer durch einen gefahrbringenden Ausfall bedingten Ausfalldauer t_{CE} gilt:

$$PFD = 1 - e^{-\lambda_D t_{CE}} \\ \approx \lambda_D t_{CE} \quad \text{da } \lambda_D t_{CE} \ll 1$$

Daher ist für eine 1oo1-Architektur die mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung:

$$PFD_G = (\lambda_{DU} + \lambda_{DD}) t_{CE}$$

B.3.2.2.2 1oo2

Diese Architektur besteht aus zwei parallelen Kanälen, so dass jeder der Kanäle die Sicherheitsfunktion ausführen kann. Daher müsste ein gefahrbringender Ausfall in beiden Kanälen vorliegen, bevor die Sicherheitsfunktion bei Anforderung ausfallen würde. Es wird angenommen, dass jeder Diagnosetest erkannte Fehler nur meldet und keine Ausgangszustände oder den Ausgangsvergleich ändert.

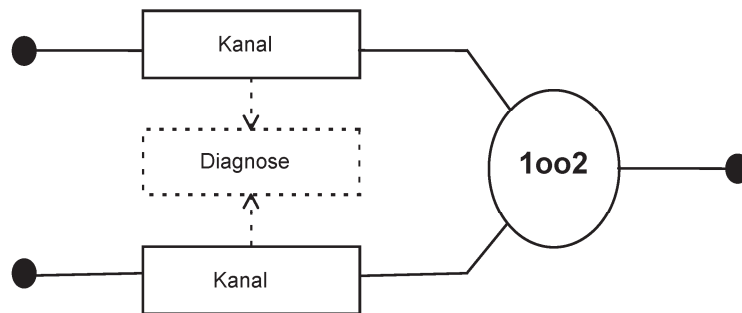


Bild B.6 – Blockschaltbild für 1oo2

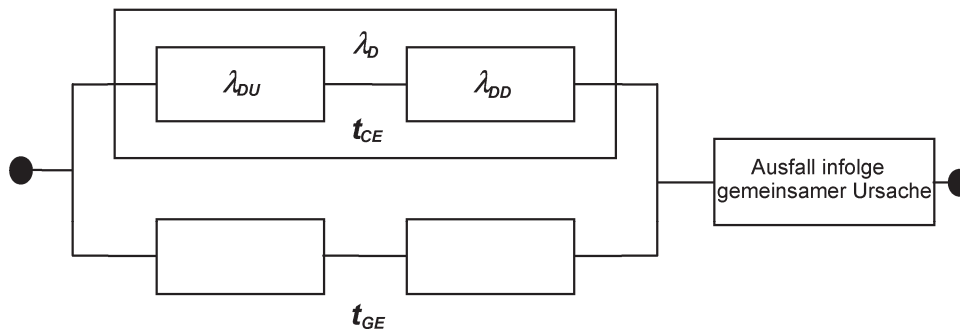


Bild B.7 – Zuverlässigkeitsblockdiagramm für 1oo2

Bild B.6 enthält das zugehörige Blockschaltbild und Bild B.7 das Zuverlässigkeitsblockdiagramm. Der Wert für t_{CE} ist wie in B.3.2.2.1 angegeben, aber jetzt ist es notwendig, die Ausfalldauer t_{GE} des Systems auch zu berechnen, die gegeben ist durch:

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D} \left(\frac{T_i}{3} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

Die mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für diese Architektur ist:

$$PFD_G = 2((1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU} \left(\frac{T_i}{2} + MRT \right)$$

B.3.2.2.3 2oo2

Diese Architektur besteht aus zwei parallelen Kanälen, so dass jeder der Kanäle die Sicherheitsfunktion anfordern muss, bevor sie ausgeführt werden kann. Es wird angenommen, dass jeder Diagnosetest erkannte Fehler nur meldet und keine Ausgangszustände oder den Ausgangsvergleich ändert.

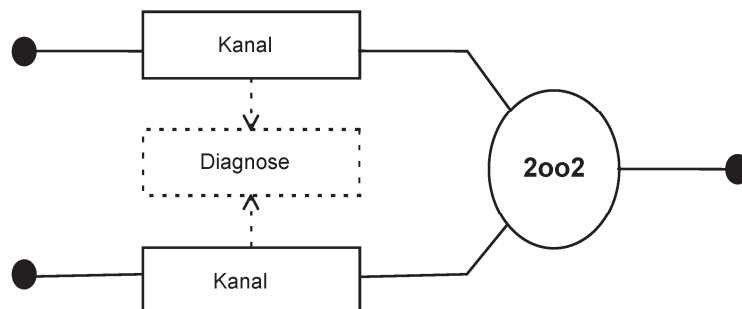


Bild B.8 – Blockschaltbild für 2oo2

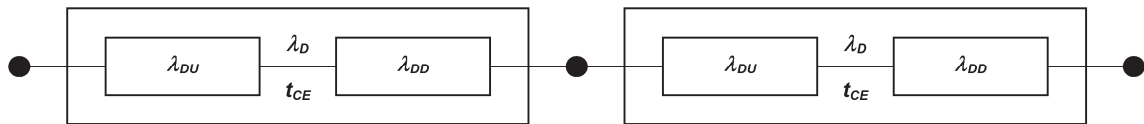


Bild B.9 – Zuverlässigkeitsblockdiagramm für 2oo2

Bild B.8 enthält das zugehörige Blockschaltbild und Bild B.9 das Zuverlässigkeitsblockdiagramm. Der Wert für t_{CE} ist wie in B.3.2.2.1 angegeben, und die mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für diese Architektur ist:

$$PFD_G = 2\lambda_D t_{CE}$$

B.3.2.2.4 1oo2D

Diese Architektur besteht aus zwei parallelen Kanälen. Während des normalen Betriebs müssen beide Kanäle die Sicherheitsfunktion anfordern, bevor sie ausgeführt werden kann. Sollte darüber hinaus der Diagnosetest in einem Kanal einen Fehler erkennen, wird der Ausgangsvergleich angepasst, so dass der Gesamtausgangszustand dem anderen Kanal folgt. Falls der Diagnosetest in beiden Kanälen Fehler erkennt oder eine Abweichung, die keinem der beiden Kanäle zugeordnet werden kann, begibt sich der Ausgang in den sicheren Zustand. Um eine Abweichung zwischen den beiden Kanälen zu erkennen, kann jeder Kanal den Zustand des anderen durch von ihm unabhängige Mittel bestimmen. Der Kanalvergleichs-/Umschalter ist möglicherweise nicht 100 % wirksam, deshalb wird K für die Darstellung der Wirksamkeit dieses kanalübergreifenden Vergleichs-/Umschaltmechanismus verwendet, d. h. der Ausgang kann, auch wenn ein Kanal als fehlerhaft erkannt wird, weiter dem 2oo2-Ausgangsvorgang folgen.

ANMERKUNG Der Parameter K ist im Rahmen einer FMEA festzulegen.

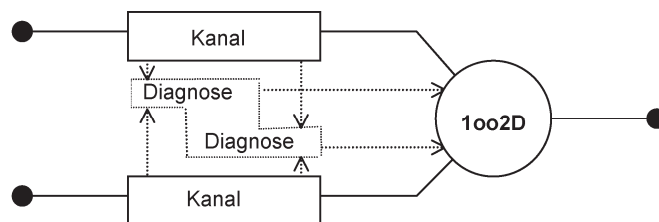


Bild B.10 – Blockschaltbild für 1oo2D

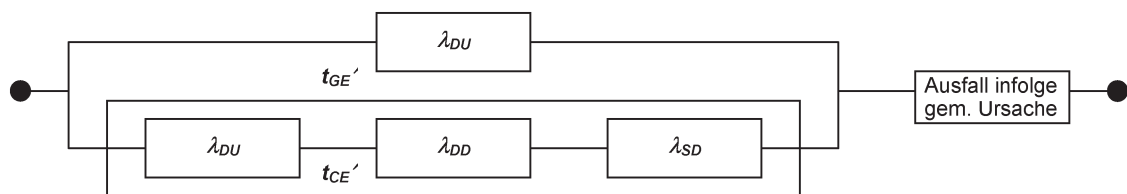


Bild B.11 – Zuverlässigkeitsblockdiagramm für 1oo2D

Die Rate erkannter sicherer Ausfälle für jeden Kanal ist gegeben durch:

$$\lambda_{SD} = \lambda_S DC$$

Bild B.10 enthält das zugehörige Blockschaltbild und Bild B.11 das Zuverlässigkeitsblockdiagramm. Die Werte der mittleren Ausfalldauern unterscheiden sich von denen der anderen Architekturen in B.3.2.2 und werden deshalb als t_{CE}' und t_{GE}' bezeichnet. Ihre Werte sind gegeben durch: