

	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	Entwurf Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3 (IEC 65A/527/CDV:2008); Deutsche Fassung FprEN 61508-6:2008 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 65A/527/CDV:2008); German version FprEN 61508-6:2008 Anwendungswarnvermerk Dieser Norm-Entwurf mit Erscheinungstermin 2009-06-08 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt. Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren. Stellungnahmen werden erbeten – vorzugsweise als Datei per E-Mail an dke@vde.com in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.dke.de/stellungnahme abgerufen werden – oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main. Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevante Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen. Gesamtumfang 212 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE	

Beginn der Gültigkeit

Diese Norm gilt ab ...

Nationales Vorwort

Die Deutsche Fassung des europäischen Dokuments FprEN 61508-6:2008 „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3“ (Entwurf in der Umfrage) ist unverändert in diesen Norm-Entwurf übernommen worden.

Die Internationale Elektrotechnische Kommission (IEC) und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dem entsprechend ist das internationale Dokument IEC 65A/527/CDV:2008 „Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3“ unverändert in den Entwurf FprEN 61508-6:2008 übernommen worden.

Da die Deutsche Fassung noch nicht endgültig mit der Englischen und Französischen Fassung abgeglichen ist, ist die englische Originalfassung des IEC-CDV entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom SC 65A „System aspects“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet.

Bei der Abstimmung zu dem Europäischen Schluss-Entwurf bei CENELEC und dem Internationalen Schluss-Entwurf bei IEC [Final Draft International Standard (FDIS)] sind jeweils nur „JA/NEIN“-Entscheidungen möglich, wobei „NEIN“-Entscheidungen fundiert begründet werden müssen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Für diesen Norm-Entwurf 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.

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.

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
FprEN61508-1:2008	65A/522/CDV:2008	E DIN EN 61805-1 (VDE 0803-1) in Vorbereitung	(VDE 0803-1)
FprEN61508-2:2008	65A/523/CDV:2008	E DIN EN 61805-2 (VDE 0803-2) in Vorbereitung	(VDE 0803-2)
FprEN61508-3:2008	65A/524/CDV:2008	E DIN EN 61805-3 (VDE 0803-3) in Vorbereitung	(VDE 0803-3)
FprEN61508-4:2008	65A/525/CDV:2008	E DIN EN 61805-4 (VDE 0803-4) in Vorbereitung	(VDE 0803-4)
FprEN61508-5:2008	65A/526/CDV:2008	E DIN EN 61805-5 (VDE 0803-5) in Vorbereitung	(VDE 0803-5)
FprEN61508-7:2008	65A/528/CDV:2008	E DIN EN 61805-7 (VDE 0803-7) in Vorbereitung	(VDE 0803-7)
–	IEC Guide 104:1997	–	–
–	IEC/ISO Guide 51:1990	–	–

Nationaler Anhang NB (informativ)

Literaturhinweise

E DIN EN 61805-1 (VDE 0803-1), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen*

E DIN EN 61805-2 (VDE 0803-2), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*

E DIN EN 61805-3 (VDE 0803-3), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software*

E DIN EN 61805-4 (VDE 0803-4), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen*

E DIN EN 61805-5 (VDE 0803-5), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 5: Beispiele von Methoden für die Bestimmung von Sicherheits-Integritätsleveln*

E DIN EN 61805-7 (VDE 0803-7), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 7: Anwendungshinweise über Verfahren und Maßnahmen*

Deutsche Fassung

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer
Systeme –

Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3

Inhalt

	Seite
Einleitung	6
1 Anwendungsbereich	8
2 Normative Verweisungen	10
3 Begriffe und Abkürzungen	10
Anhang A (informativ) Anwendung der IEC 61508-2 und der IEC 61508-3	11
A.1 Allgemeines	11
A.2 Funktionale Schritte in der Anwendung der IEC 61508-2	13
A.3 Funktionale Schritte in der Anwendung der IEC 61508-3	17
Anhang B (informativ) Beispiel eines Verfahrens für die Bewertung von Ausfallwahrscheinlichkeiten der Hardware	19
B.1 Allgemeines	19
B.2 Grundsätzliche Betrachtungen zu Wahrscheinlichkeitsberechnungen	20
B.2.1 Einleitung	20
B.2.2 Sicherheitsbezogenes E/E/PE-System mit niedriger Anforderungsrate	20
B.2.3 Sicherheitsbezogenes E/E/PE-System mit hoher Anforderungsrate oder kontinuierlicher Anforderung	21
B.3 RBD-Ansatz mit angenommener konstanter Ausfallrate	23
B.3.1 Grundlegende Hypothese	23
B.3.2 Mittlere Ausfallwahrscheinlichkeit bei Anforderung (für die Betriebsart mit niedriger Anforderungsrate)	27
B.3.3 Wahrscheinlichkeit eines Ausfalls je Stunde (für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung)	42
B.4 Boolescher Ansatz	51
B.4.1 Einleitung	51
B.4.2 Modell des Zuverlässigkeits-Blockdiagramms	51
B.4.3 Fehlzustandsbaumanalysen-Modell	52
B.4.4 PFD-Berechnungen	52
B.5 Zustand/Übergangs-Ansätze	57
B.5.1 Einleitung	57
B.5.2 Markov-Ansatz	57
B.5.3 Auf Petri-Netze und Monte Carlo-Simulation basierte Ansätze	66
B.5.4 Weitere Ansätze	71

	Seite
B.6 Unsicherheitenbehandlung	73
B.7 Verweise	74
Anhang C (informativ) Ausgearbeitetes Beispiel für die Berechnung des Diagnosedeckungsgrads und des Anteils sicherer Ausfälle.....	75
Anhang D (informativ) Eine Methode zur Quantifizierung der Auswirkungen von hardwarebedingten Ausfällen infolge gemeinsamer Ursache in E/E/PE-Systemen	78
D.1 Allgemeines	78
D.2 Anwendungsbereich der Methode	82
D.3 Durch die Methode berücksichtigte Punkte	82
D.4 Verwendung des β -Faktor, um die Wahrscheinlichkeit eines Ausfalls eines sicherheitsbezogenen E/E/PE-Systems durch Ausfälle infolge gemeinsamer Ursache zu berechnen	83
D.5 Schätzung von β unter Verwendung der Tabellen	84
D.6 Beispiele für die Anwendung der β -Faktor-Methode	89
D.7 CCF-Ansatz mit Binomial-Ausfallraten Modell (Modell mit Zufallsstörungen)	90
D.8 Literaturhinweise	92
Anhang E (informativ) Beispiele für die Anwendung der Tabellen zur Sicherheitsintegrität der Software aus der IEC 61508-3	93
E.1 Allgemeines	93
E.2 Beispiel für den Sicherheits-Integritätslevel 2.....	93
E.3 Beispiel für den Sicherheits-Integritätslevel 3.....	98
Literaturhinweise	103
Bilder	
Bild 1 – Gesamtrahmen der IEC 61508	9
Bild A.1 – Anwendung der IEC 61508-2	15
Bild A.2 – Anwendung der IEC 61508-2	16
Bild A.3 – Anwendung der IEC 61508-3	18
Bild B.1 – Zuverlässigkeits-Blockdiagramm einer vollständigen Sicherheitsschleife	20
Bild B.2 – Beispielkonfiguration für zwei Kanäle mit Sensoren	25
Bild B.3 – Struktur mit Teilsystemen	27
Bild B.4 – Blockschaltbild für 1oo1	29
Bild B.5 – Zuverlässigkeits-Blockdiagramm für 1oo1.....	29
Bild B.6 – Blockschaltbild für 1oo2.....	30
Bild B.7 – Zuverlässigkeits-Blockdiagramm für 1oo2.....	30
Bild B.8 – Blockschaltbild für 2oo2.....	31
Bild B.9 – Zuverlässigkeits-Blockdiagramm für 2oo2.....	31
Bild B.10 – Blockschaltbild für 1oo2D	31
Bild B.11 – Zuverlässigkeits-Blockdiagramm für 1oo2D	32
Bild B.12 – Blockschaltbild für 2oo3.....	32
Bild B.13 – Zuverlässigkeits-Blockdiagramm für 2oo3	33

	Seite
Bild B.14 – Architektur des Beispiels für die Betriebsart mit niedriger Anforderungsrate	39
Bild B.15 – Architektur des Beispiels für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung.....	49
Bild B.16 – RBD einer einfachen vollständigen Schleife mit Sensoren und 2oo3-Architektur	52
Bild B.17 – Einfache Fehlzustandsbaumanalyse, entsprechend dem in Bild B.1 dargestellten RBD.....	52
Bild B.18 – Äquivalenz von Fehlzustandsbaum und Zuverlässigkeits-Blockdiagramm	53
Bild B.19 – Augenblickliche Nichtverfügbarkeit $U(t)$ einzelner periodisch getesteter Bauteile.....	54
Bild B.20 – Prinzip der Berechnung von PFD_{avg} durch Fehlzustandsbaumanalysen.....	55
Bild B.21 – Auswirkung von versetzten Tests	56
Bild B.22 – Beispiel einer komplexen Teststruktur	56
Bild B.23 – Markov-Graph, der das Verhalten eines Zwei-Komponenten-Systems modelliert.....	58
Bild B.24 – Prinzip der Modellierung eines mehrphasigen Markov-Prozesses	59
Bild B.25 – Sägezahnprofil für den mehrphasigen Markov-Ansatz	60
Bild B.26 – Markov-Modell-Approximation.....	60
Bild B.27 – Auswirkung der Ausfälle durch die Anforderung selbst	61
Bild B.28 – Modellierung der Auswirkung der Testdauer	61
Bild B.29 – Mehrphasiges Markov-Modell mit DD- und auch DU-Ausfällen.....	61
Bild B.30 – Logikänderung (2oo3 nach 1oo2) anstelle einer Reparatur des ersten Ausfalls	62
Bild B.31 – Markov-Graphen für die „Zuverlässigkeit“ mit einem absorbierenden Zustand.....	63
Bild B.32 – Markov-Graphen für die „Verfügbarkeit“ ohne absorbierende Zustände	64
Bild B.33 – Petri-Netz für die Modellierung einer einzelnes periodisch getestetes Bauteil	66
Bild B.34 – PN zur Modellierung von CCF und der Reparaturressourcen	69
Bild B.35 – RBD für die PN-Modellbildung und Zusatz-PN für die PFD - und PFH -Berechnungen	69
Bild B.36 – Einfaches PN für ein Einzelbauteil und entdeckten Ausfällen und Reparaturen	70
Bild B.37 – Beispiel der funktionalen und dysfunktionalen Modellierung mit einer formalen Sprache.....	72
Bild B.38 – Prinzip der Unsicherheitsverteilung.....	73
Bild D.1 – Beziehung zwischen Ausfällen infolge gemeinsamer Ursache und Ausfällen einzelner Kanäle.....	80
Bild D.2 – Umsetzung des Modells mit Zufallsstörungen anhand von Fehlzustandsbäumen.....	91
Tabellen	
Tabelle B.1 – In diesem Anhang verwendete Benennungen und ihre zugehörigen Parameterbereiche	26
Tabelle B.2 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für ein Wiederholungsprüfungsintervall von 6 Monaten und eine mittlere Zeit zur Wiederherstellung von 8 h	34
Tabelle B.3 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für ein Wiederholungsprüfungsintervall von einem Jahr und eine mittlere Zeit zur Wiederherstellung von 8 h	35
Tabelle B.4 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für ein Wiederholungsprüfungsintervall von zwei Jahren und eine mittlere Zeit zur Wiederherstellung von 8 h.....	37

Tabelle B.5 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für ein Wiederholungsprüfungsintervall von 10 Jahren und eine mittlere Zeit zur Wiederherstellung von 8 h	38
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>)	39
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>)	40
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>)	40
Tabelle B.9 – Beispiel für eine nicht ausreichende Wiederholungsprüfung	42
Tabelle B.10 – Wahrscheinlichkeit eines Ausfalls je Stunde (für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung) für ein Wiederholungsprüfungsintervall von einem Monat und eine mittlere Zeit zur Wiederherstellung von 8 h	44
Tabelle B.11 – Wahrscheinlichkeit eines Ausfalls je Stunde (für die Betriebsart mit hoher oder Anforderungsrate kontinuierlicher Anforderung) für ein Wiederholungsprüfungsintervall von drei Monaten und eine mittlere Zeit zur Wiederherstellung von 8 h	45
Tabelle B.12 – Wahrscheinlichkeit eines Ausfalls je Stunde (für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung) für ein Wiederholungsprüfungsintervall von 6 Monaten und eine mittlere Zeit zur Wiederherstellung von 8 h	47
Tabelle B.13 – Wahrscheinlichkeit eines Ausfalls je Stunde (für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung) für ein Wiederholungsprüfungsintervall von einem Jahr und eine mittlere Zeit zur Wiederherstellung von 8 h	48
Tabelle B.14 – Wahrscheinlichkeit des Ausfalls je Stunde 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>)	49
Tabelle B.15 – Wahrscheinlichkeit eines Ausfalls je Stunde 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>)	50
Tabelle B.16 – Wahrscheinlichkeit eines Ausfalls je Stunde 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>)	50
Tabelle C.1 – Beispielberechnung für den Diagnosedeckungsgrad und den Anteil sicherer Ausfälle	76
Tabelle C.2 – Diagnosedeckungsgrad und Wirksamkeit für verschiedene Teilsysteme	77
Tabelle D.1 – Anrechnung programmierbarer Elektronik oder Sensoren/Stellglieder	86
Tabelle D.2 – Werte für <i>Z</i> : programmierbare Elektronik	88
Tabelle D.3 – Werte für <i>Z</i> : Sensoren oder Stellglieder	88
Tabelle D.4 – Berechnung von β oder β_0	89
Tabelle D.5 – Berechnung von β für Redundanzsysteme größer als 1oo2	89
Tabelle D.6 – Beispielwerte für programmierbare Elektroniken	90
Tabelle E.1 – Spezifikation der Software-Sicherheitsanforderungen (siehe IEC 61508-3, 7.2)	94
Tabelle E.2 – Software-Entwurf und -Entwicklung: Entwurf der Software-Architektur (siehe IEC 61508-3, 7.4.3)	95
Tabelle E.3 – Software-Entwurf und -Entwicklung: Hilfswerkzeuge und Programmiersprachen (siehe IEC 61508-3, 7.4.4)	96

	Seite
Tabelle E.4 – Software-Entwurf und -Entwicklung: Detaillierter Entwurf (siehe IEC 61508-3, 7.4.5 und 7.4.6).....	96
Tabelle E.5 – Software-Entwurf und -Entwicklung: Test der Software-Module und der Integration der Software (siehe IEC 61508-3, 7.4.7 und 7.4.8)	96
Tabelle E.6 – Integration der programmierbaren Elektronik (Hardware und Software) (siehe IEC 61508-3, 7.5)	97
Tabelle E.7 – Validierung der Software bezüglich der Sicherheit (siehe IEC 61508-3, 7.7)	97
Tabelle E.8 – Software-Modifikation (siehe IEC 61508-3, 7.8).....	97
Tabelle E.9 – Software-Verifikation (siehe IEC 61508-3, 7.9)	97
Tabelle E.10 – Beurteilung der funktionalen Sicherheit (siehe IEC 61508-3, Abschnitt 8)	98
Tabelle E.11 – Spezifikation der Software-Sicherheitsanforderungen (siehe IEC 61508-3, 7.2).....	99
Tabelle E.12 – Software-Entwurf und -Entwicklung: Entwurf der Software-Architektur (siehe IEC 61508-3, 7.4.3)	99
Tabelle E.13 – Software-Entwurf und -Entwicklung: Hilfswerkzeuge und Programmiersprachen (siehe IEC 61508-3, 7.4.4)	100
Tabelle E.14 – Software-Entwurf und -Entwicklung: Detaillierter Entwurf (siehe IEC 61508-3, 7.4.5 und 7.4.6).....	100
Tabelle E.15 – Software-Entwurf und -Entwicklung: Test der Software-Module und -Integration (siehe IEC 61508-3, 7.4.7 und 7.4.8)	101
Tabelle E.16 – Integration der programmierbaren Elektronik (Hardware und Software) (siehe IEC 61508-3, 7.5)	101
Tabelle E.17 – Validierung der Softwaresicherheit (siehe IEC 61508-3, 7.7)	101
Tabelle E.18 – Software-Modifikation (siehe IEC 61508-3, 7.8)	102
Tabelle E.19 – Software-Verifikation (siehe IEC 61508-3, 7.9)	102
Tabelle E.20 – Beurteilung der funktionalen Sicherheit (siehe IEC 61508-3, Abschnitt 8)	102

Einleitung

Systeme, die aus elektrischen und/oder elektronischen Bauteilen bestehen, werden seit vielen Jahren verwendet, um Sicherheitsfunktionen in vielen Anwendungsbereichen auszuführen. Auf Rechnern basierende Systeme (allgemein bezeichnet als 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 Verantwortlichen für die Entscheidungsfindung ausreichende Hilfestellung bezüglich der Sicherheitsaspekte erhalten, nach denen Entscheidungen getroffen werden.

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

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

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

Diese Internationale Norm:

- betrachtet alle relevanten sicherheitsbezogenen Phasen des Gesamtsystems des E/E/PE und des Software-Sicherheitslebenszyklus (zum Beispiel vom anfänglichen Konzept über Entwurf, Durchführung, Betrieb und Instandhaltung bis zur Außerbetriebnahme), wenn E/E/PE benutzt werden, um Sicherheitsfunktionen auszuführen;
- wurde unter Berücksichtigung einer sich schnell entwickelnden Technologie entworfen. Der Betrachtungsrahmen ist ausreichend robust und ausführlich genug, um auch für zukünftige Entwicklungen verwendbar zu sein;
- ermöglicht die Erstellung anwendungsspezifischer Internationaler Normen, die sich mit sicherheitsbezogenen E/E/PE befassen; die Entwicklung anwendungsspezifischer Normen sollte innerhalb des Rahmens dieser Internationalen Norm zu einem hohen Grad an Übereinstimmung (zum Beispiel von zugrunde liegenden Prinzipien, Terminologie usw.) führen, sowohl innerhalb der Anwendungsbereiche als auch über die Anwendungsbereiche hinweg. Dies hat sowohl sicherheitstechnische als auch wirtschaftliche Vorteile;

ANMERKUNG 1 Die Verweise [1] und [2] in den Literaturhinweisen sind anwendungsspezifische Internationaler Normen.

- liefert eine Methode für die Entwicklung der Spezifikation der Sicherheitsanforderungen, die notwendig ist, um die notwendige funktionale Sicherheit des sicherheitsbezogenen E/E/PE-Systems zu erreichen;
- verwendet einen auf dem Risiko basierenden Lösungsansatz für die Festlegung der Anforderungen der Sicherheits-Integritätslevel;
- verwendet Sicherheits-Integritätslevel für die Spezifikation der Zielvorgabe der Sicherheitsintegrität der Sicherheitsfunktionen, die in dem sicherheitsbezogenen E/E/PE-System implementiert werden;

ANMERKUNG 2 Die Norm legt weder die Sicherheitsintegritätsanforderungen aller Sicherheitsfunktionen fest, noch, wie die Sicherheits-Integritätslevel bestimmt werden. Sie liefert stattdessen einen risikobasierenden konzeptionellen Rahmen und Verfahrensbeispiele.

- setzt numerische Ausfallgrenzwerte für sicherheitsbezogene E/E/PE-Systeme, die mit Sicherheits-Integritätsleveln verbunden sind;
- setzt eine untere Grenze des Ausfallgrenzwertes für eine gefahrbringende Ausfallart, der für ein einzelnes sicherheitsbezogenes E/E/PE-System beansprucht werden kann. Für sicherheitsbezogene E/E/PE-Systeme, die:
 - in der Betriebsart mit einer niedrigen Anforderungsrate betrieben werden, ist die untere Grenze der mittleren Wahrscheinlichkeit, die entworfene Funktion auf Anforderung nicht auszuführen, auf 10^{-5} festgelegt;
 - in der Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung betrieben werden, ist die untere Grenze der Wahrscheinlichkeit eines gefahrbringenden Ausfalls auf 10^{-9} [h⁻¹] je Stunde festgelegt;

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

ANMERKUNG 4 Es kann möglich sein, Entwürfe von sicherheitsbezogenen Systemen mit niedrigen Zielvorgaben für die Sicherheitsintegrität von nichtkomplexen Systemen zu erhalten, diese Grenzwerte sind aber dafür gedacht, darzustellen, was für relativ komplexe Systeme (zum Beispiel für programmierbare elektronische Sicherheitssysteme) zum gegenwärtigen Zeitpunkt erreicht werden kann.

- bestimmt, basierend auf der Beurteilung der gewonnenen praktischen Erfahrungswerte der Industrie die Anforderungen zur Vermeidung und Beherrschung von systematischen Fehlern. Selbst wenn die Wahrscheinlichkeit des Auftretens eines systematischen Fehlers im Allgemeinen nicht quantifiziert werden kann, ermöglicht die Norm dennoch, dass bei einer Beanspruchung, für eine festgelegte Sicherheitsfunktion darauf geachtet werden kann, den mit der Sicherheitsfunktion verbundenen Ausfallgrenzwert zu erreichen, wenn alle Anforderungen dieser Norm erfüllt wurden.
- lässt einen weiten Bereich von Prinzipien, Techniken und Maßnahmen zu, um funktionale Sicherheit für sicherheitsbezogene E/E/PE-Systeme zu erreichen, verwendet aber nicht das Fail-safe-Konzept, das genutzt werden kann, wenn das Ausfallverhalten gut definiert und das Niveau der Komplexität verhältnismäßig niedrig ist. Das Fail-safe-Konzept wurde wegen des weiten Bereiches der Komplexität von sicherheitsbezogenen E/E/PE-Systemen, die im Rahmen der Norm behandelt werden, als ungeeignet betrachtet.

1 Anwendungsbereich

1.1 Dieser Teil der IEC 61508 enthält Informationen und Richtlinien für die 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 Verfahren zur Berechnung der Wahrscheinlichkeiten von Hardwareausfällen und sollte in Verbindung mit IEC 61508-2, 7.4.3 und Anhang C und 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 ausgearbeitete Beispiele für die Anwendung der Tabellen der Sicherheitsintegrität der Software, die im Anhang A der IEC 61508-3 für die Sicherheits-Integritätslevel 2 und 3 festgelegt sind.

1.2 Die Teile 1, 2, 3 und 4 dieser Norm sind Sicherheits-Grundnormen, dieser Status ist aber im Zusammenhang mit einfachen sicherheitsbezogenen E/E/PE-Systemen nicht anwendbar (siehe 3.4.4 von Teil 4). Als Sicherheits-Grundnormen sind sie für die Verwendung durch Technische Komitees bei der Erstellung von Normen nach *IEC Guide 104* und *ISO/IEC Guide 51* vorgesehen. Die Teile 1,2,3 und 4 sind ebenfalls zur Verwendung als eigenständige Normen vorgesehen. Die horizontale Sicherheitsfunktion dieser Norm gilt nicht für medizinische Geräte nach der Normenreihe IEC 60601.

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

1.3 Bild 1 zeigt den Gesamtrahmen für die Teile 1 bis 7 der IEC 61508 und zeigt die Rolle, die die IEC 61508-4 beim Erreichen der funktionalen Sicherheit für sicherheitsbezogene E/E/PE-Systeme spielt.

— **Entwurf** —

E DIN EN 61508-6 (VDE 0803-6):2009-06
FprEN 61508-6:2008

Bild 1 – Gesamtrahmen der 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 (alle Teile), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC Guide 104:1997, *Guide to the drafting of safety standards and the role of committees with safety pilot functions and safety group functions*

IEC/ISO Guide 51:1990, *Guidelines for the inclusion of safety aspects in standards*

3 Begriffe und Abkürzungen

Für die Anwendung dieser Norm 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

Eine Maschine, eine Prozessanlage und andere Betriebsmittel können im Fall einer Fehlfunktion (z. B. aufgrund von Ausfällen elektromechanischer, 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.

Die IEC 61508-1 liefert mit einem risikobasiertem Ansatz den gesamten Rahmen 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 im Falle eines notwendigen Sicherheitseingriffs nicht verfügbar machen.

Die 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.

Die IEC 61508-1 fordert weiter, dass der durch die Risikoanalyse festgestellte Betrag der Risikominderung zur Festlegung verwendet wird, für welche Sicherheitsfunktionen (jede mit einer spezifizierten Sicherheitsintegrität¹⁾) ein oder mehrere sicherheitsbezogene Systeme²⁾ notwendig sind.

Die IEC 61508-2 und die IEC 61508-3 nehmen die Sicherheitsfunktionen und Anforderungen an die Sicherheitsintegrität auf, die jedem System zugeordnet sind, das durch die Anwendung der IEC 61508-1 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
- sich auf Mittel zur Verhinderung und/oder Beherrschung zufälliger Hardware- und systematischer Ausfälle (des E/E/PES und Sicherheitslebenszyklus der Software³⁾) konzentrieren.

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

²⁾ 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 E/E/PE-sicherheitsbezogenes System bezeichnet und schließen alle Betriebsmittel ein, die zur Ausführung der erforderlichen Sicherheitsfunktionen (siehe IEC 61508-4, 3.4.1) notwendig sind.

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) aufeinander folgen. Es sei jedoch hervor gehoben, dass jeder Ansatz für einen Lebenszyklus verwendet werden kann, vorausgesetzt, dass eine Aussage zur Gleichwertigkeit im Sicherheitsplan für das Projekt (siehe IEC 61508-1, Abschnitt 7) gemacht worden ist.

Die IEC 61508-2 und die IEC 61508-3 geben keine Anleitung, welches Sicherheits-Integritätslevel für ein gegebenes 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 vermeidende Methoden; und
- die Beherrschung systematischer Ausfälle (einschließlich Softwarefehler) und zufälliger Hardwareausfälle durch Entwurfsmerkmale wie Fehleraufdeckung, Redundanz und strukturelle Merkmale (z. B. Diversität).

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

- den Anforderungen zur Hardware-Fehlertoleranz (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 der IEC 61508-2 als auch in der IEC 61508-3 wird die Zusicherung, dass das Ziel der Sicherheitsintegrität für systematische Ausfälle erreicht worden ist, aufgrund

- der korrekten Anwendung von Sicherheits-Management-Verfahren;
- des Einsatzes fachkundigen Personals;
- der Anwendung der im Sicherheitslebenszyklus festgelegten Tätigkeiten einschließlich der festgelegten Verfahren und Maßnahmen⁶⁾; und
- einer unabhängigen Beurteilung der funktionalen Sicherheit⁷⁾

gegeben.

Das gesamte Ziel ist es, sicherzustellen, dass entsprechend des Sicherheits-Integritätslevels verbliebene systematische Fehler keinen Ausfall des sicherheitsbezogenen E/E/PE-Systems verursachen.

Die 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 Hardwareausfälle als auch gegen systematische Hardwareausfälle gefordert. Diese beinhalten, wie oben dargelegt, eine angemessene Kombination von fehlervermeidenden und ausfallbeherrschenden Maßnahmen. Wird ein Bedienereingriff für die funktionale Sicherheit benötigt, werden Anforderungen an die Bedienerschnittstelle gestellt. In der IEC 61508-2 werden ebenfalls auf Software und Hardware (z. B. Diversität) basierende Diagnosetest-Verfahren und -Maßnahmen zur Aufdeckung zufälliger Hardwareausfälle festgelegt.

Die IEC 61508-3 ist entwickelt worden, um Anforderungen zum Erreichen der Sicherheitsintegrität der Software, und zwar sowohl der Embedded-Software (einschließlich Dienste für Diagnose und Fehleraufdeckung) als auch der Anwendungssoftware, zur Verfügung zu stellen. Die IEC 61508-3 fordert eine Kombination von Ansätzen zur Fehlervermeidung (Qualitätssicherung) und Fehlertoleranz (Softwarearchitektur), da es keinen

⁴⁾ Die für jeden Sicherheits-Integritätslevel geforderten Techniken und Maßnahmen werden in IEC 61508-2 und IEC 61508-3 gezeigt.

⁵⁾ Systematische Ausfälle können gewöhnlich nicht quantifiziert werden. Ursachen hierfür sind u. a.: Spezifikations- und Entwurfsfehler in Hardware und Software; Ausfälle auf Grund 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 Sicherheitsplanung 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).

⁸⁾ Einschließlich fest eingebauter Software oder softwareähnlich (auch Firmware genannt), wie z. B. anwendungsspezifische integrierte Schaltungen.

bekannten Weg zum Nachweis der Fehlerfreiheit in einigermaßen komplexer sicherheitsbezogener Software, besonders der Freiheit von Spezifikations- und Entwurfsfehlern, gibt. Die IEC 61508-3 fordert die Anwendung von Software-Entwurfsprinzipien wie Top-Down-Entwurf, Modularität, Verifikation jeder Phase des Entwicklungslebenszyklus, geprüfte Software-Module und Software-Modul-Bibliotheken 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 E/E/PES-Entwicklung 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 in 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 im 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 Sicherheitsanforderungen (siehe IEC 61508-1). Angemessene Aktualisierung der Sicherheitsplanung während der E/E/PES-Entwicklung.
- b) Bestimmung der Anforderungen für die E/E/PES-Sicherheit, einschließlich der Anforderungen zur Sicherheitsintegrität für jede Sicherheitsfunktion (siehe IEC 61508-2, 7.2). Zuweisung der Anforderungen an die Software und Übergabe an die Softwarelieferanten und/oder Entwickler für die Anwendung der IEC 61508-3.

ANMERKUNG 1 An dieser Stelle ist es notwendig, die Möglichkeit gleichzeitiger Ausfälle im EUC-Leit- und Steuersystem und E/E/PE-sicherheitsbezogenen System(en) zu berücksichtigen (siehe IEC 61508-5, A.5.4). Diese können aus Bauteilausfällen infolge gemeinsamer Ursache, z. B. 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 bezüglich der Sicherheit des sicherheitsbezogenen E/E/PE-Systems (siehe IEC 61508-2, 7.3).
- d) Spezifikation der Architektur (Konfiguration) für das Logik-Teilsystem des E/E/PES, 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.
- f) Festlegung der Systemparameter für jedes der Teilsysteme (Bauteile), die in dem sicherheitsbezogenen E/E/PE-System verwendet werden. Für jedes wird Folgendes bestimmt:
 - das Wiederholungsprüfungsintervall für Ausfälle, die nicht automatisch aufgedeckt werden;
 - die mittlere Zeit zur Wiederherstellung;
 - der Diagnosedeckungsgrad (siehe IEC 61508-2, Anhang C);
 - die Ausfallwahrscheinlichkeit;
 - für Route 1_H siehe IEC 61508-2, 7.4.4.2 und Anhang C
 - 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 Gleichung, die die Beziehung zwischen der Verfügbarkeit und den relevanten Parametern der Einrichtung und der Einsatzbedingungen zeigt.

- i) 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 nicht den Ausfallgrenzwert erreicht 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 IEC 61508-2, 7.4.3.2.2, Anmerkung 9 für die Liste einiger Methoden, die verwendet werden können).

- j) Implementierung des Entwurfs des sicherheitsbezogenen E/E/PE-Systems. Auswahl von Maßnahmen und Verfahren, um systematische Hardwareausfälle, Ausfälle durch Umwelteinflüsse und Bedienungsfehler (siehe IEC 61508-2, Anhang A) zu beherrschen.
- k) Integration der verifizierten Software (siehe IEC 61508-3) in die Ziel-Hardware (siehe IEC 61508-2, 7.5 und 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)).
- l) Validierung des E/E/PES (siehe IEC 61508-2, 7.7 und Anhang B) zusammen mit dem Softwareentwickler (siehe IEC 61508-3, 7.7).
- m) Übergabe der Hardware und Ergebnisse der Validierung des E/E/PES bezüglich der Sicherheit an die Systemingenieure für die weitere Integration in das Gesamtsystem.
- n) 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 E/E/PES 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 E/E/PES-Sicherheits-Verfahren und Maßnahmen im Hinblick auf das erforderliche 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. Aus den Tabellen wird für jedes Verfahren und jede Maßnahme auf eine Kurzbeschreibung mit Literaturhinweisen verwiesen (siehe IEC 61508-7, Anhang 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 Sicherheitsplanung schriftlich begründet werden (siehe IEC 61508-1, Abschnitt 6).

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

Bild A.1 – Anwendung der IEC 61508-2

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

Bild A.2 – Anwendung der IEC 61508-2

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

Die funktionalen Schritte der 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 Sicherheitsplanung (siehe IEC 61508-2, 7.3). Angemessene Aktualisierung der Sicherheitsplanung 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
 - der Software innerhalb jedes sicherheitsbezogenen E/E/PE-Systems Funktionen 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 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 E/E/PES-Lieferanten/Entwickler. Falls notwendig, Wiederholung dieses Schrittes.
 - d) Beginn der Planung für die Verifikation und Validierung der Software bezüglich der Sicherheit (siehe IEC 61508-3, 7.3 und 7.9).
 - e) Entwurf, Entwicklung und Verifizieren/Testen der Software nach:
 - der Planung der Softwaresicherheit;
 - dem Software-Sicherheits-Integritätslevel; und
 - dem Sicherheitslebenszyklus der Software.
 - 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 des integrierten sicherheitsbezogenen E/E/PE-Systems (siehe IEC 61508-3, 7.7) zusammen mit dem Hardwareentwickler (siehe IEC 61508-2, 7.7).
 - h) Übergabe der Ergebnisse der Validierung der Software bezüglich der Sicherheit an die Systemingenieure für die weitere Integration in das Gesamtsystem.
 - i) Falls eine Modifikation der E/E/PES-Software während der Betriebszeit notwendig wird, erneute Anwendung der IEC 61508-3 (siehe IEC 61508-3, 7.8), sofern angebracht.

Einige Tätigkeiten finden im gesamten Sicherheitslebenszyklus des E/E/PES 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 E/E/PES-Sicherheits-Verfahren und Maßnahmen im Hinblick auf das erforderliche 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. Aus 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 die IEC 61508-7 beinhaltet einen probabilistischen Ansatz für die Bestimmung der Sicherheitsintegrität von vorentwickelter 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 Sicherheitsplanung schriftlich begründet werden (siehe IEC 61508-1, Abschnitt 6).

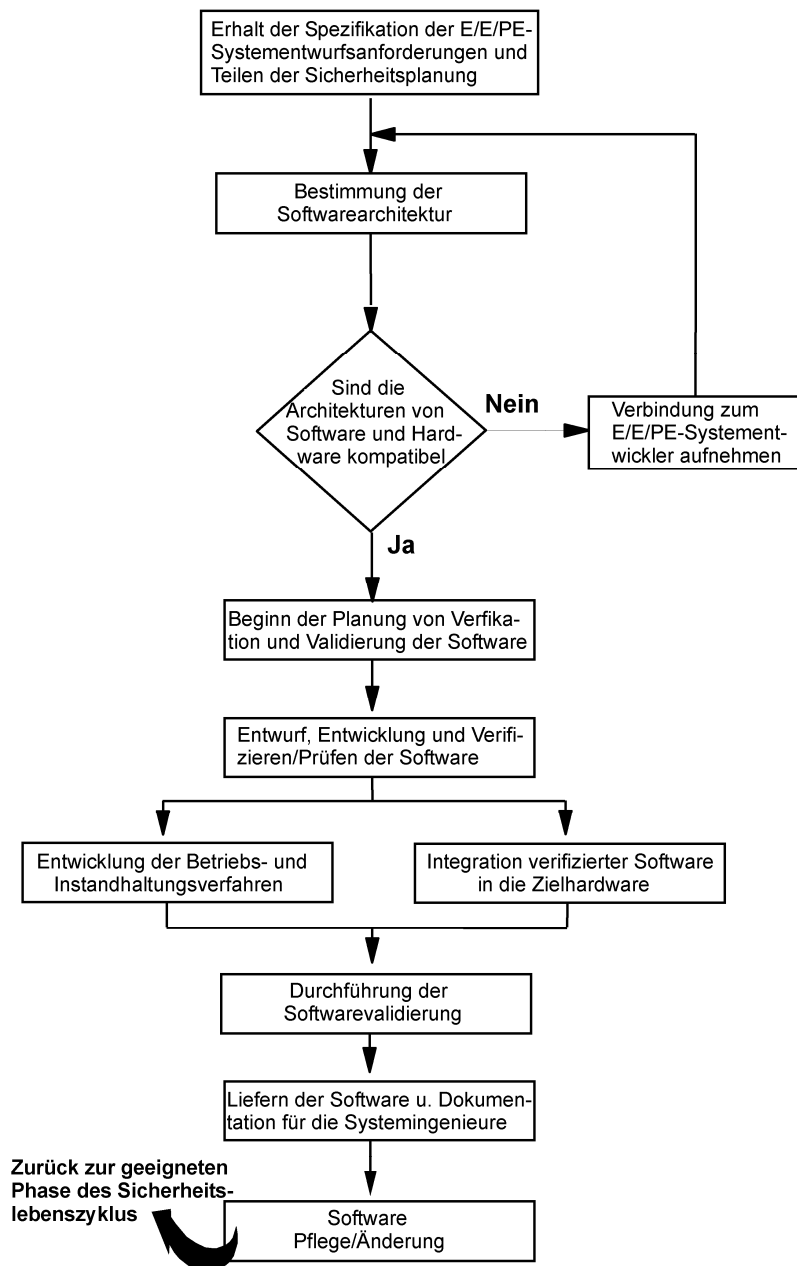


Bild A.3 – Anwendung der IEC 61508-3

Anhang B (informativ)

Beispiel eines Verfahrens 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 E/E/PE sicherheitsbezogenen 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 Techniken, die von den herkömmlichen Methoden zur Zuverlässigkeitsberechnung abgeleitet sind.

ANMERKUNG 1 Andere Verfahren werden z. B. in ANSI/ISA S84.01-1996 „Applikation of safety instrumented systems for the process industries“ beschrieben.

Es gibt eine Anzahl von Zuverlässigkeitsverfahren, die für die Analyse der Sicherheitsintegrität der Hardware sicherheitsbezogener E/E/PE-Systeme mehr oder weniger aufwendig sind. Allgemein werden sie nach den folgenden zwei Gesichtspunkten unterteilt:

- statische (Boolesch) oder dynamische (Zustand/Übergang) Modelle;
- analytische oder Monte-Carlo Simulationsberechnungen.

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 Zuverlässigkeits-Blockdiagramme (en: RBD) (siehe IEC 61508-7, C.6.5 und IEC 61078) und Fehlzustandsbäume (en: FT) (siehe IEC 61508-7, B.6.6.5 und C.6.7 und IEC 61025).

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, C.6.4 und IEC 61165), Petri-Netze (siehe IEC 61508-7, B.2.3.3 und C.6.8) und formale Sprachmodelle gehören zu den Zustands-Übergangs-Modellen. Es werden zwei Ansätze des Markov-Modells untersucht: ein vereinfachter Ansatz basierend auf spezifischen Gleichungen (B.3) und ein allgemeiner Ansatz, der Berechnungen unmittelbar an Graphen des Markov-Modells (B.5.2) ermöglicht. Für Sicherheitssysteme, nicht nach dem Markov-Modell, können stattdessen Monte-Carlo Simulationen verwendet werden. Mit Echtzeitrechnern ist dies selbst für SIL4-Berechnungen erreichbar. Die Abschnitte B.5.3 und B.5.4 dieses Anhangs enthalten Anleitungen zur Anwendung der Monte Carlo-Simulation (siehe IEC 61508-7, C.6.6) an Verhaltensmodellen basierend auf Petri-Netzen und formalen Sprachmodellen.

Der vereinfachte Ansatz, der zu erst vorgestellt wird, basiert auf grafischen RBD-Darstellungen und spezifischen Gleichungen des Markov-Modells, erhalten aus der Taylor-Formel und den konservativen in B.3.1 beschriebenen Hypothesen.

All diese Verfahren können für die Mehrzahl der sicherheitsbezogenen Systeme verwendet werden und wenn für jede einzelne Anwendung entschieden wurde, welches Verfahren angewandt wird, ist es sehr wichtig, dass diese vom Anwender fachgerecht ausgeführt werden. Das kann mehr Auswirkung haben, als die Entscheidung, welches Verfahren angewandt wird. 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 vorrangig vorkommenden 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 die ausführende Fachkraft die von dem Softwarepaket verwendeten Gleichungen/Verfahren verstehen, um sicherzustellen, dass deren Verwendung für die bestimmte Anwendung ausreichend ist. Die Fachkraft sollte außerdem durch einige manuelle Berechnungen das Ergebnis des Softwareprogramms überprüfen.

Stellt ein Ausfall des EUC-Leit- oder Steuerungssystems eine Anforderung an das E/E/PE sicherheitsbezogene 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 E/E/PE sicherheitsbezogenen 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 Grundsätzliche Betrachtungen zu Wahrscheinlichkeitsberechnungen

B.2.1 Einleitung

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

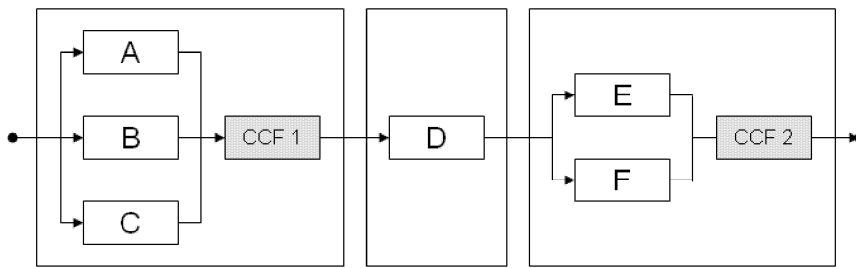


Bild B.1 – Zuverlässigkeits-Blockdiagramm einer vollständigen Sicherheitsschleife

Daraus ergeben sich fünf Fehlerkombinationen, die zum Ausfall des sicherheitsbezogenen E/E/PE-Systems führen. Jedes ist ein sogenannter minimaler kritischer Pfad (en: 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 PFD_{avg} (d. h. dessen mittlerer Nichtverfügbarkeit). Diese ist das Verhältnis von $MDT(T)/T$, wobei $MDT(T)$ die mittlere Unklarzeit des sicherheitsbezogenen E/E/PE-Systems über einen Zeitraum $[0, T]$ ist.

Die Wahrscheinlichkeit des Ausfalls ist für ein Sicherheitssystem in der Regel sehr gering und die Wahrscheinlichkeit zweier minimaler kritische Pfade gleichzeitig, ist vernachlässigbar. Außerdem gibt die Summe der mittleren Unklarzeit infolge aller kritischen Pfade eine konservative Schätzung der mittleren Unklarzeit des gesamten Systems an. Aus Bild B.1 kann entnommen werden:

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

dividiert durch T ergibt:

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

Hierfür sind die Berechnungen von PFD_{avg} für in Reihe geschaltete Teile sehr ähnlich denen, die mit einfacher Wahrscheinlichkeit 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} nicht einfach aus MDT^E und MDT^F berechnet werden kann:

Die (E, F)-System MDT wird mit $MDT^{EF} = \int_0^T PFD^E(t) PFD^F(t) dt$ berechnet.

Für die Berechnungen von PFD_{avg} für parallel geschaltete Teile (Integrale) sind die einfachen Wahrscheinlichkeitsberechnungen (Addition und Multiplikation) nicht länger zulässig. 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 ausgerechnet 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 gewerblichen booleschen Softwareprogrammen so unterstützt wird, müssen die Analytiker aufmerksam sein, um solche nicht konservativen Berechnungen, welche im Umgang mit der Sicherheit unerwünscht sind, zu verhindern.

ANMERKUNG Zum Beispiel könnte für einen redundanten (1oo2) Kanal mit einer gefahrbringenden unerkannten Ausfallrate λ_{DU} und einem Intervall τ für die Wiederholungsprüfung, eine ungenaue Wahrscheinlichkeitsberechnung $(\lambda_{DU} \cdot \tau)^2/4$ ergeben, bei einem tatsächlichen Ergebnis von $(\lambda_{DU} \cdot \tau)^2/3$.

Die Berechnungen müssen analytisch oder mit der Monte Carlo-Simulation durchgeführt werden. Dieser Anhang beschreibt diese Anwendung mit Hilfe konventioneller Zuverlässigkeitsmodelle basierend auf Boolesch (RBD bzw. Fehlzustandsbaum) 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-Gleichung

Wenn ein sicherheitsbezogenes E/E/PE-System in der Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung verwendet wird, verlangt die Norm die Berechnung der Wahrscheinlichkeit dessen Ausfalls je Stunde (PFH), d. h. die mittlere Ausfallhäufigkeit pro Zeiteinheit. Dies ist der Durchschnittswert der sogenannten unbedingten Ausfallintensität $w(t)$ (auch Ausfallhäufigkeit genannt) über einen bestimmten 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 es bildet die allerletzte Barriere für die Sicherheit, dann führt der Ausfall des gesamten sicherheitsbezogenen E/E/PE-System unmittelbar zu einer möglicherweise gefährlichen Situation. Deshalb kann für Ausfälle die einen Verlust der gesamten Sicherheitsfunktion verursachen, eine Reparatur des gesamten sicherheitsbezogenen Systems in der Berechnung nicht berücksichtigt werden. Wenn der Ausfall des gesamten sicherheitsbezogenen Systems jedoch aufgrund des Ausfalls mancher anderen Sicherheitsbarriere bzw. Einrichtung nicht unmittelbar zu einer möglichen Gefahr führt, dann ist es möglich, die Erkennung und die Reparatur des sicherheitsbezogenen Systems in der Risikominderungsrechnung zu berücksichtigen.

B.2.3.2 Unzuverlässigkeit (z. B. einzelne Barrieren arbeiten 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 aller letzte Barriere für die Sicherheit bildet. Sobald ein Fehler

auftritt kann eine mögliche Gefährdung eintreten. Es ist kein Ausfall 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 gesamten Systems kann zeitabhängig oder konstant sein.

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

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

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

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 sind, können nicht berücksichtigt werden. Außerdem ist bei einer redundanten Konfiguration, bei der es darauf ankommt die Wiederholungsprüfungen zu berücksichtigen, 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 es bildet nicht die aller letzte Barriere, erhöhen dessen Ausfälle lediglich die Anforderungshäufigkeit auf die anderen Sicherheitsbarrieren, bzw. 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 Approximationen: $PFH = \frac{1}{MUT + MDT} = \frac{1}{MTBF} \approx \frac{1}{MUT} \approx \frac{1}{MTTF}$

B.2.3.4 Betrachtungen zur Ausfallrate

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

In Reihe geschaltete Strukturen sind 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 minimalen kritischen Pfade sind.

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

1. Wenn E und F nicht reparabel sind (z.B. DU-Ausfälle), wechselt $\Lambda^{ef}(t)$ kontinuierlich von 0 zu λ (Ausfallrate von E oder F). Ein asymptotischer Wert wird erreicht, wenn einer der beiden Komponenten voraussichtlich ausfallen wird. Das ist ein sehr langsamer Prozess, da dies eintritt, wenn t größer als $1/\lambda$ wird. Dieser asymptotische Wert wird, wenn E und F periodisch (wiederholend) mit einem Testintervall von $\tau < 1/\lambda$ geprüft werden, tatsächlich niemals erreicht werden.
2. Wenn E und F schnell reparabel sind (z.B. DD-Ausfälle), geht $\Lambda^{ef}(t)$ zügig 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 bzw. drei Mal größer wird, als die größte MTTR der Komponenten. Dies ist ein spezieller Fall der vollständig und schnell reparablen Systeme, die oben behandelt wurden.

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

B.3 RBD-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 des Teilsystems ist kleiner als 10^{-1} , bzw. die sich ergebende Wahrscheinlichkeit eines Ausfalls je Stunde des Teilsystems ist kleiner als 10^{-5} ;
- die Bauteil-Ausfallraten sind während der Lebensdauer des Systems konstant;
- das Sensor- (Eingangs-) Teilsystem besteht aus 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.1);
- das Logik-Teilsystem besteht aus den Bauteilen, 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 zusätzlich berechnet);
- die Kanäle in einer Gruppe mit Ausgangsvergleich oder Mehrheitsentscheider haben alle die gleichen Ausfallraten und Diagnosedeckungsgrade;
- die Gesamtausfallrate der Hardware eines Kanals eines Teilsystems ist die Summe der Rate der gefährbringenden Ausfälle und der Rate der sicheren Ausfälle, die als gleich angenommen werden;

ANMERKUNG 1 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 ungenügenden Wiederholungsprüfung siehe jedoch B.2.5;

- das Wiederholungsprüfungsintervall ist mindestens um eine Zehnerpotenz größer als das Diagnose-Testintervall;
- für jedes Teilsystem gibt es genau ein Intervall für die Wiederholungsprüfung und eine mittlere Zeit zur Wiederherstellung;

ANMERKUNG 2 Die mittlere Zeit zur Wiederherstellung ist in IEC 61508-2, 7.4.3.2.2, Anmerkung 5 definiert und schließt die Zeit zur Erkennung des Ausfalls ein. In diesem Anhang beinhaltet der einzelne angenommene Wert für die mittlere Zeit zur Wiederherstellung für sowohl erkannte als auch unerkannte Ausfälle das Diagnosetestintervall, nicht aber das Wiederholungsprüfungsintervall. Bei unerkannten Ausfällen sollte für Berechnungen das Diagnosetestintervall nicht in die mittlere Zeit bis zur Wiederherstellung eingehen; da aber die mittlere Zeit zur Wiederherstellung immer zum Wiederholungsprüfungsintervall hinzu addiert wird, dieser Wert aber um eine Zehnerpotenz größer als das Diagnosetestintervall ist, ist die Abweichung unbedeutend.

- das erwartete Intervall zwischen den Anforderungen ist mindestens um eine Zehnerpotenz größer als die mittlere Zeit zur Wiederherstellung;
- 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 mittleren Zeit zur Wiederherstellung sowohl erkannt als auch repariert. Diese Zeit wurde bei der Festlegung der Anforderungen an die Sicherheitsintegrität der Hardware benutzt;

BEISPIEL Falls eine mittlere Zeit zur Wiederherstellung von 8 h angenommen wird, schließt dies das Diagnosetestintervall ein, das typischerweise kleiner als 1 h ist, der Rest ist die eigentliche Reparaturzeit.

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 Die Prozess-Sicherheitszeit ist in IEC 61508-2, 7.4.3.2.5 als die Zeitspanne zwischen dem Auftreten eines Ausfalls der EUC oder des EUC-Leit- oder Steuerungssystems (mit dem Potential zu einem gefahrbringenden Vorfall) und dem Auftreten des gefahrbringenden Vorfalls bei nicht ausgeführter Sicherheitsfunktion definiert.

- wenn ein Ausfall der Leistungsversorgung ein E/E/PE sicherheitsbezogenes System betrifft und das System beim Abschalten der Versorgung einen sicheren Zustand einnimmt, beeinflusst die Leistungsversorgung 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 Leistungsversorgung ein Ausfallverhalten hat, das einen unsicheren Betrieb des sicherheitsbezogenen E/E/PE-Systems verursachen kann, dann sollte die Leistungsversorgung 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.

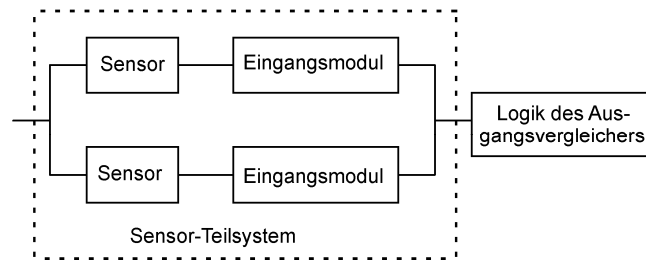


Bild B.2 – Beispielkonfiguration für zwei Kanäle mit Sensoren

**Tabelle B.1 – In diesem Anhang verwendete Benennungen und ihre zugehörigen
Parameterbereiche**
(Anzuwenden auf 1oo1, 1oo2, 2oo2, 1oo2D, 1oo3 und 2oo3)

Abkürzung	Beschreibung (Einheit)	Parameterbereich der 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 Zeit zur Wiederherstellung (en: Mean time to restoration) (in Stunden)	8 h
DC	Diagnosedeckungsgrad (in einer Gleichung als Bruch dargestellt, sonst in Prozent)	0 % 60 % 90 % 99 %
β	Anteil unerkannter Ausfälle infolge gemeinsamer Ursache (in einer Gleichung als Bruch dargestellt, sonst in Prozent). (In den Tabellen B.2 bis B.5 und B.10 bis B.13 wird $\beta = 2 \times \beta_0$ angenommen.)	2 % 10 % 20 %
β_0	Der Anteil der Ausfälle infolge gemeinsamer Ursache, die durch den Diagnosetest erkannt werden (in einer Gleichung als Bruch dargestellt, sonst in Prozent). (In den Tabellen B.2 bis B.5 und B.10 bis B.13 wird $\beta = 2 \times \beta_0$ angenommen.)	1 % 5 % 10 %
λ_{DU}	Rate gefahrbringender 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}
PFD_G	Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung einer Gruppe von Kanälen mit Ausgangsvergleicher oder Mehrheitsentscheider (en: PFD 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 bzw. 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	
PFD_{SYS}	Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für die Sicherheitsfunktion eines E/E/PE sicherheitsbezogenen Systems	
PFH_G	Ausfallwahrscheinlichkeit je Stunde 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 bzw. PFH_{FE} .)	
PFH_S	Ausfallwahrscheinlichkeit je Stunde für das Sensor-Teilsystem	
PFH_L	Ausfallwahrscheinlichkeit je Stunde für das Logik-Teilsystem	
PFH_{FE}	Ausfallwahrscheinlichkeit je Stunde für das Stellglied-Teilsystem	
PFH_{SYS}	Ausfallwahrscheinlichkeit je Stunde für die Sicherheitsfunktion eines E/E/PE sicherheitsbezogenen Systems	
λ	Gesamtausfallrate (je Stunde) eines Kanal 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 Äquivalenzunklarzeit (in Stunden) eines Kanals für 1oo1, 1oo2-, 2oo2- und 2oo3-Architekturen (Dies ist die gemeinsame Unklarzeit für alle Komponenten in einem Kanal des Teilsystems.)	

Tabelle B.1 (fortgesetzt)

Abkürzung	Beschreibung (Einheit)	Parameterbereich der Tabellen B.2 bis B.5 und B.10 bis B.13
t_{GE}	mittlere Äquivalenzunklarzeit (in Stunden) für eine Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider mit 1oo2- und 2oo3-Architekturen. (Dies ist die gemeinsame Unklarzeit für alle Kanäle in einer Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider.)	
t_{CE}^1	mittlere Äquivalenzunklarzeit (in Stunden) eines Kanals für eine 1oo2D-Architektur. (Dies ist die gemeinsame Unklarzeit für alle Komponenten in einem Kanal des Teilsystems.)	
t_{GE}^1	mittlere Äquivalenzunklarzeit (in Stunden) für eine Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider mit 1oo2D-Architektur. (Dies ist die gemeinsame Unklarzeit für alle Kanäle in einer Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider.)	
T_2	Intervall zwischen den Anforderungen (in Stunden)	
K	Anteil des Erfolges der Eigentestschaltung im 1oo2-System	
PTC	Wiederholungsprüfungsdeckungsgrad	
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 E/E/PE sicherheitsbezogenen Systems wird durch die Berechnung und Zusammenführung der mittleren Wahrscheinlichkeiten eines Ausfalls bei Anforderung aller Teilsysteme, die gemeinsam die Sicherheitsfunktion erbringen, bestimmt. Da in diesem Anhang die Wahrscheinlichkeiten klein sind, kann dies wie folgt ausgedrückt werden (siehe Bild B.2):

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

Dabei ist

- PFD_{SYS} die mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung einer Sicherheitsfunktion des E/E/PE sicherheitsbezogenen 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.

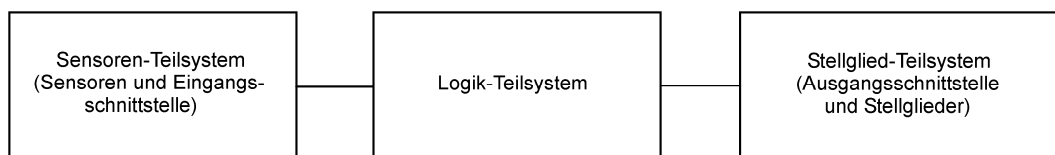


Bild B.3 – Struktur mit Teilsystemen

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:

- 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, Barrieren oder Schaltungen zur Signalkonditionierung sein; Bauteile des Logik-Teilsystems z. B. Prozessoren und Scanner-Einrichtungen; Bauteile des Stellglied-Teilsystems z. B.

Ausgangsfilter, Barrieren und Aktoren. Darstellen jedes Teilsystems als eine oder mehrere 1oo1-, 1oo2-, 2oo2-, 1oo2D- 1oo3, oder 2oo3-Gruppen mit Ausgangsvergleicher oder Mehrheitsentscheider.

- b) Aus den Tabellen B.2 bis B.5 die zutreffende aufsuchen, je nachdem, ob ein 6-Monate-, 1-Jahr-, 2-Jahre- oder 10-Jahre-Wiederholungsprüfungsintervall vorgesehen ist. Diese Tabellen nehmen alle eine Zeit von 8 h bis zur Wiederherstellung für jeden aufgedeckten Ausfall an.
- c) In der zutreffenden Tabelle für jede Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider im Teilsystem folgende Parameter aufsuchen:
- Architektur (z. B. 2oo3);
 - Diagnosedeckungsgrad jedes Kanals (z. B. 60 %);
 - die Rate gefahrbringender Ausfälle (je Stunde) λ_D jedes Kanals (z. B. $2,5 \times 10^{-06}$);
 - im Hinblick auf das Zusammenwirken der Kanäle in einer Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider die β -Faktoren für den Ausfall infolge gemeinsamer Ursachen, β und β_D (z. B. 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 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 bleibenden gefahrbringenden Ausfällen), das Zweifache von β_D , dem β -Faktor für durch Diagnosetests erkannte Ausfälle, beträgt.

- d) Aus der zugehörigen Tabelle (B.2 bis B.5) die mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für eine Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider entnehmen.
- 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 folgende Gleichungen bestimmt; hierbei sind PFD_{Gi} und PFD_{Gj} die mittleren Ausfallwahrscheinlichkeiten bei Anforderung für jede derartige Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider mit Sensoren bzw. Stellgliedern:

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

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

Die in allen Gleichungen verwendeten Formeln sowohl für PFD als auch die Systemausfallrate sind Funktionen von Bauteilausfallrate und mittlerer Unklarzeit (MDT). Dort, wo mehrere Bauteile in dem System vorhanden sind und es erforderlich ist, für alle Bauteile gemeinsam PFD bzw. die Ausfallrate des gesamten Systems zu berechnen, wird oft ein Einzelwert für MDT in der Gleichung verwendet. Jedes Bauteil kann jedoch über eine andere Ausfallerkennung mit unterschiedlichen MDT verfügen bzw. können die verschiedenen Bauteile unterschiedliche MDT für ein und denselben Ausfallmechanismus aufweisen, wofür es notwendig ist einen Einzelwert für die MDT zu ermitteln, der für alle Bauteile im Pfad gültig ist. Dies kann durchgeführt werden, wenn die Gesamtausfallrate des vollständigen Pfades berücksichtigt wird und dann die einzelnen MDT 's entsprechend ihres Anteils an der zu betrachteten Gesamtausfallrate aufgeteilt werden.

Zum Beispiel, wenn zwei Bauteile in Reihe geschaltet sind und eines einer Wiederholungsprüfung T_1 und das andere einer Wiederholungsprüfung T_2 unterworfen wird, ist der entsprechende Einzelwert für MDT :

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

und

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

B.3.2.2 Architekturen für die Betriebsart mit niedriger Anforderungsrate

ANMERKUNG 1 Dieser Unterabschnitt sollte in der richtigen Reihenfolge gelesen werden, da Gleichungen für mehrere Architekturen nur bei ihrer ersten Verwendung angegeben werden.

ANMERKUNG 2 Die Gleichungen basieren auf den Annahmen in B.1.

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.

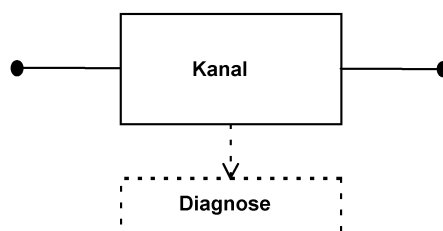


Bild B.4 – Blockschaltbild für 1oo1

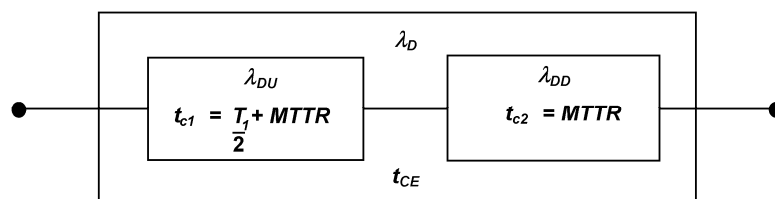


Bild B.5 – Zuverlässigkeits-Blockdiagramm für 1oo1

Bild B.4 enthält das zugehörige Blockschaltbild und Bild B.5 das Zuverlässigkeits-Blockdiagramm. 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 Äquivalenzunklarzeit t_{CE} des Kanals zu berechnen, indem man die einzelnen Unklarzeiten der beiden Komponenten, t_{c1} und t_{c2} , addiert, jeweils bewertet mit dem Verhältnis, mit dem sie in die Ausfallwahrscheinlichkeit des Kanals eingehen:

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

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

$$\lambda_{DU} = \frac{\lambda}{2} (1 - DC); \quad \lambda_{DD} = \frac{\lambda}{2} DC$$

Für einen Kanal mit einer durch einen gefährbringenden Ausfall bedingten Unklarzeit 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 gefährbringender Ausfall in beiden Kanälen vorliegen, bevor die Sicherheitsfunktion bei Anforderung ausfallen würde. Es wird vorausgesetzt, dass jeder Diagnosetest erkannte Fehler nur meldet und keine Ausgangszustände oder den Ausgangsvergleich ändert.

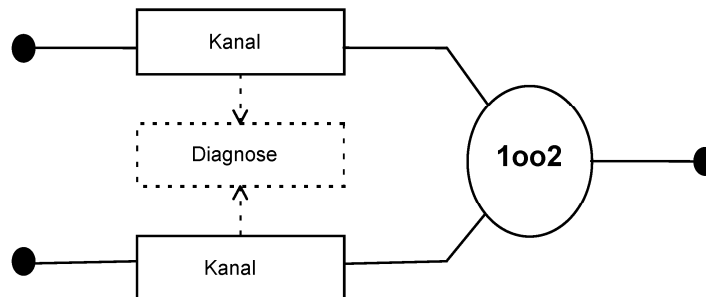


Bild B.6 – Blockschaltbild für 1oo2

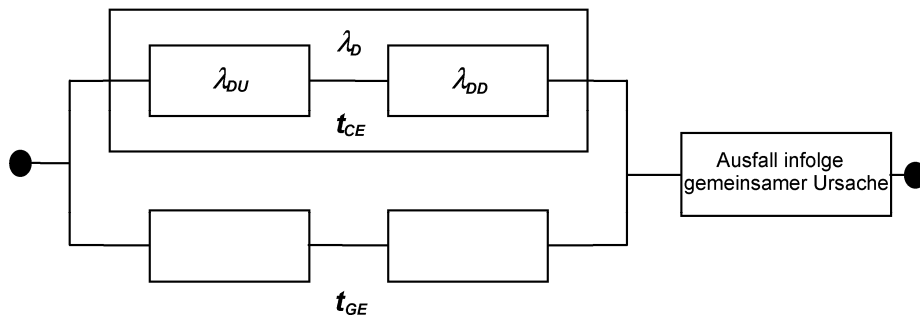


Bild B.7 – Zuverlässigkeits-Blockdiagramm für 1oo2

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

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D} \left(\frac{T_1}{3} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

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

$$PFD_G = 2((1 - \beta_D) \lambda_{DD} + (1 - \beta) \lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU} \left(\frac{T_1}{2} + MTR \right)$$

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 vorausgesetzt, dass jeder Diagnosetest erkannte Fehler nur meldet und keine Ausgangszustände oder den Ausgangsvergleich ändert.

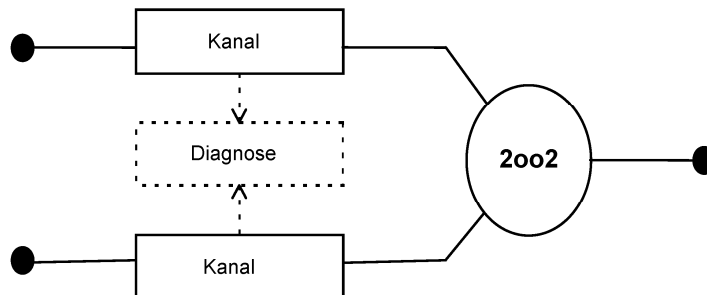


Bild B.8 – Blockschaltbild für 2oo2

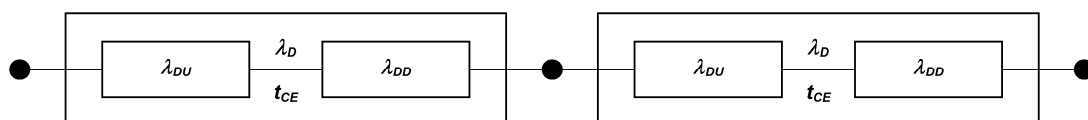


Bild B.9 – Zuverlässigkeits-Blockdiagramm für 2oo2

Bild B.8 enthält das zugehörige Blockschaltbild und Bild B.9 das Zuverlässigkeits-Blockdiagramm. 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 Gesamtzustand 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 Kanalvergleich/Umschalter ist möglicherweise nicht 100 % wirksam, deshalb wird K für die Darstellung der Effizienz dieses kanalübergreifenden Vergleichs-/Umschaltmechanismus verwendet, d. h. der Ausgang kann, sogar wenn ein Kanal als fehlerhaft erkannt wird, über den 2oo2-Ausgangsvergleich erhalten werden.

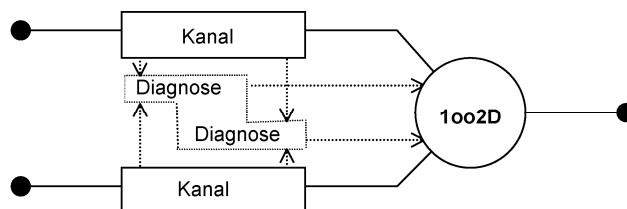


Bild B.10 – Blockschaltbild für 1oo2D

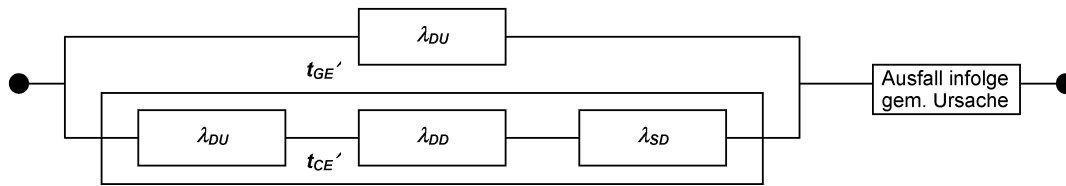


Bild B.11 – Zuverlässigkeits-Blockdiagramm für 1oo2D

Die Rate erkannter sicherer Ausfälle für jeden Kanal ist gegeben durch

$$\lambda_{SD} = \frac{\lambda}{2} DC$$

Bild B.10 enthält das zugehörige Blockschaltbild und Bild B.11 das Zuverlässigkeits-Blockdiagramm. Die Werte der mittleren Äquivalenzunklarzeit 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

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

$$t_{GE}' = \frac{T_1}{3} + MTTR$$

Die mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für diese Architektur ist

$$PFD_G = 2(1-\beta)\lambda_{DU}((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} + \lambda_{SD})t_{CE}'t_{GE}' + 2(1-K)\lambda_{DD}t_{CE}' + \beta\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right)$$

B.3.2.2.5 2oo3

Diese Architektur besteht aus drei parallelen Kanälen, verbunden mit einem Mehrheitsentscheider, so dass sich der Ausgangszustand nicht ändert, wenn nur ein Kanal ein von den beiden anderen unterschiedliches Ergebnis liefert.

Es wird vorausgesetzt, dass jeder Diagnosetest erkannte Fehler nur meldet und keine Ausgangszustände oder den Mehrheitsentscheid ändert.

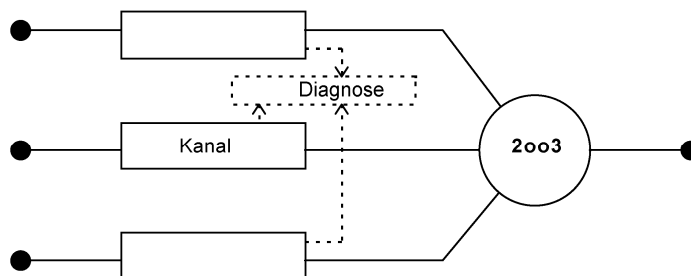


Bild B.12 – Blockschaltbild für 2oo3

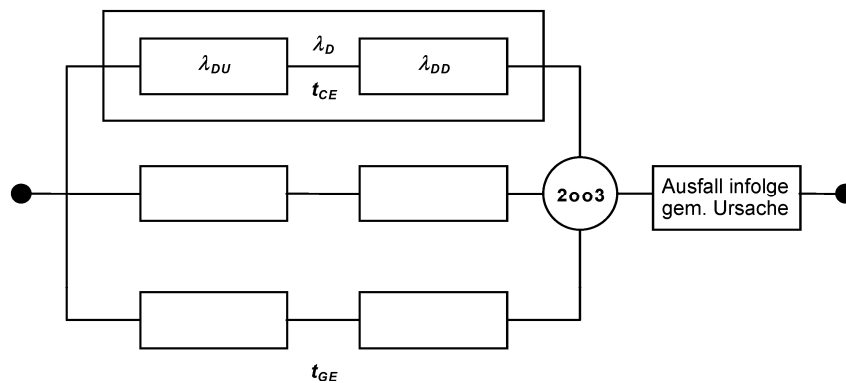


Bild B.13 – Zuverlässigkeits-Blockdiagramm für 2oo3

Bild B.12 enthält das zugehörige Blockschaltbild und Bild B.13 das Zuverlässigkeits-Blockdiagramm. Der Wert für t_{CE} ist wie in B.3.2.2.1 und der Wert für t_{GE} wie im B.3.2.2.2 angegeben. Die mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für diese Architektur ist:

$$PFD_G = 6((1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU} \left(\frac{T_1}{2} + MTTR \right)$$

B.3.2.2.6 1oo3

Diese Architektur besteht aus drei parallelen Kanälen, verbunden mit einem Mehrheitsentscheider, so dass der Ausgangszustand sich nach dem 1oo3-Mehrheitsentscheider ausrichtet.

Es wird vorausgesetzt, dass jeder Diagnosetest erkannte Fehler nur meldet und keine Ausgangszustände oder den Mehrheitsentscheid ändert.

Das Zuverlässigkeits-Blockdiagramm entspricht dem für 2oo3, allerdings mit 1oo3-Mehrheitsentscheider. Der Wert für t_{CE} ist wie in B.3.2.2.1 und der Wert für t_{GE} wie im B.3.2.2.2 angegeben. Die mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für diese Architektur ist:

$$PFD_G = 6((1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU})^3 t_{CE} t_{GE} t_{G2E} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU} \left(\frac{T_1}{2} + MTTR \right)$$

Dabei ist

$$t_{G2E} = \frac{\lambda_{DU}}{\lambda_D} \left(\frac{T_1}{4} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

B.3.2.3 Tabellen für die Betriebsart mit niedriger Anforderungsrate

**Tabelle B.2 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung
für ein Wiederholungsprüfungsintervall von 6 Monaten und eine mittlere Zeit zur
Wiederherstellung von 8 h**

Architektur	DC	$\lambda_D = 0,5E-07$			$\lambda_D = 2,5E-07$			$\lambda_D = 0,5E-06$		
		$\beta = 2\%$ $\beta_b = 1\%$	$\beta = 10\%$ $\beta_b = 5\%$	$\beta = 20\%$ $\beta_b = 10\%$	$\beta = 2\%$ $\beta_b = 1\%$	$\beta = 10\%$ $\beta_b = 5\%$	$\beta = 20\%$ $\beta_b = 10\%$	$\beta = 2\%$ $\beta_b = 1\%$	$\beta = 10\%$ $\beta_b = 5\%$	$\beta = 20\%$ $\beta_b = 10\%$
1oo1 (s. Anm. 2)	0 %		1,1E-04			5,5E-04			1,1E-03	
	60 %		4,4E-05			2,2E-04			4,4E-04	
	90 %		1,1E-05			5,7E-05			1,1E-04	
	99 %		1,5E-06			7,5E-06			1,5E-05	
1oo2	0 %	2,2E-06	1,1E-05	2,2E-05	1,1E-05	5,5E-05	1,1E-04	2,4E-05	1,1E-04	2,2E-04
	60 %	8,8E-07	4,4E-06	8,8E-06	4,5E-06	2,2E-05	4,4E-05	9,1E-06	4,4E-05	8,8E-05
	90 %	2,2E-07	1,1E-06	2,2E-06	1,1E-06	5,6E-06	1,1E-05	2,3E-06	1,1E-05	2,2E-05
	99 %	2,6E-08	1,3E-07	2,6E-07	1,3E-07	6,5E-07	1,3E-06	2,6E-07	1,3E-06	2,6E-06
2oo2 (s. Anm. 2)	0 %		2,2E-04			1,1E-03			2,2E-03	
	60 %		8,8E-05			4,4E-04			8,8E-04	
	90 %		2,3E-05			1,1E-04			2,3E-04	
	99 %		3,0E-06			1,5E-05			3,0E-05	
1oo2D (s. Anm. 3)	0 %	2,2E-06	1,1E-05	2,2E-05	1,1E-05	5,5E-05	1,1E-04	2,4E-05	1,1E-04	2,2E-04
	60 %	1,4E-06	4,9E-06	9,3E-06	7,1E-06	2,5E-05	4,7E-05	1,4E-05	5,0E-05	9,3E-05
	90 %	4,3E-07	1,3E-06	2,4E-06	2,2E-06	6,6E-06	1,2E-05	4,3E-06	1,3E-05	2,4E-05
	99 %	6,0E-08	1,5E-07	2,6E-07	3,0E-07	7,4E-07	1,3E-06	6,0E-07	1,5E-06	2,6E-06
2oo3	0 %	2,2E-06	1,1E-05	2,2E-05	1,2E-05	5,6E-05	1,1E-04	2,7E-05	1,1E-04	2,2E-04
	60 %	8,9E-07	4,4E-06	8,8E-06	4,6E-06	2,2E-05	4,4E-05	9,6E-06	4,5E-05	8,9E-05
	90 %	2,2E-07	1,1E-06	2,2E-06	1,1E-06	5,6E-06	1,1E-05	2,3E-06	1,1E-05	2,2E-05
	99 %	2,6E-08	1,3E-07	2,6E-07	1,3E-07	6,5E-07	1,3E-06	2,6E-07	1,3E-06	2,6E-06
1oo3	0 %	2,2E-06	1,1E-05	2,2E-05	1,2E-05	5,5E-05	1,1E-04	2,2E-05	1,1E-04	2,2E-04
	60 %	8,8E-07	4,4E-06	8,8E-06	4,4E-06	2,2E-05	4,4E-05	8,8E-06	4,4E-05	8,8E-05
	90 %	2,2E-07	1,1E-06	2,2E-06	1,1E-06	5,6E-06	1,1E-05	2,2E-06	1,1E-05	2,2E-05
	99 %	2,6E-08	1,3E-07	2,6E-07	1,3E-07	6,5E-07	1,3E-06	2,6E-07	1,3E-06	2,6E-06

Architektur	DC	$\lambda_D = 2,5E-06$			$\lambda_D = 0,5E-05$			$\lambda_D = 2,5E-05$		
		$\beta = 2\%$ $\beta_b = 1\%$	$\beta = 10\%$ $\beta_b = 5\%$	$\beta = 20\%$ $\beta_b = 10\%$	$\beta = 2\%$ $\beta_b = 1\%$	$\beta = 10\%$ $\beta_b = 5\%$	$\beta = 20\%$ $\beta_b = 10\%$	$\beta = 2\%$ $\beta_b = 1\%$	$\beta = 10\%$ $\beta_b = 5\%$	$\beta = 20\%$ $\beta_b = 10\%$
1oo1 (s. Anm. 2)	0 %		5,5E-03			1,1E-02			5,5E-02	
	60 %		2,2E-03			4,4E-03			2,2E-02	
	90 %		5,7E-04			1,1E-03			5,7E-03	
	99 %		7,5E-05			1,5E-04			7,5E-04	
1oo2	0 %	1,5E-04	5,8E-04	1,1E-03	3,7E-04	1,2E-03	2,3E-03	5,0E-03	8,8E-03	1,4E-02
	60 %	5,0E-05	2,3E-04	4,5E-04	1,1E-04	4,6E-04	9,0E-04	1,1E-03	2,8E-03	4,9E-03
	90 %	1,2E-05	5,6E-05	1,1E-04	2,4E-05	1,1E-04	2,2E-04	1,5E-04	6,0E-04	1,2E-03
	99 %	1,3E-06	6,5E-06	1,3E-05	2,6E-06	1,3E-05	2,6E-05	1,4E-05	6,6E-05	1,3E-04
2oo2 (s. Anm. 2)	0 %		1,1E-02			2,2E-02			>1E-01	
	60 %		4,4E-03			8,8E-03			4,4E-02	
	90 %		1,1E-03			2,3E-03			1,1E-02	
	99 %		1,5E-04			3,0E-04			1,5E-03	
1oo2D (s. Anm. 3)	0 %	1,5E-04	5,8E-04	1,1E-03	3,8E-04	1,2E-03	2,3E-03	5,0E-03	9,0E-03	1,4E-02
	60 %	7,7E-05	2,5E-04	4,7E-04	1,7E-04	5,2E-04	9,5E-04	1,3E-03	3,0E-03	5,1E-03
	90 %	2,2E-05	6,6E-05	1,2E-04	4,5E-05	1,3E-04	2,4E-04	2,6E-04	6,9E-04	1,2E-03
	99 %	3,0E-06	7,4E-06	1,3E-05	6,0E-06	1,5E-05	2,6E-05	3,0E-05	7,4E-05	1,3E-04
2oo3	0 %	2,3E-04	6,5E-04	1,2E-03	6,8E-04	1,5E-03	2,5E-03	1,3E-02	1,5E-02	1,9E-02
	60 %	6,3E-05	2,4E-04	4,6E-04	1,6E-04	5,1E-04	9,4E-04	2,3E-03	3,9E-03	5,9E-03
	90 %	1,2E-05	5,7E-05	1,1E-04	2,7E-05	1,2E-04	2,3E-04	2,4E-04	6,8E-04	1,2E-03
	99 %	1,3E-06	6,5E-06	1,3E-05	2,7E-06	1,3E-05	2,6E-05	1,5E-05	6,7E-05	1,3E-04
1oo3	0 %	1,1E-04	5,5E-04	1,1E-03	2,2E-04	1,1E-03	2,2E-03	1,4E-03	5,7E-03	1,1E-02
	60 %	4,4E-05	2,2E-04	4,4E-04	8,8E-05	4,4E-04	8,8E-04	4,6E-04	2,2E-03	4,4E-03
	90 %	1,1E-05	5,6E-05	1,1E-04	2,2E-05	1,1E-04	2,2E-04	1,1E-04	5,6E-04	1,1E-03
	99 %	1,3E-06	6,5E-06	1,3E-05	2,6E-06	1,3E-05	2,6E-05	1,3E-05	6,5E-05	1,3E-04

Tabelle B.2 (fortgesetzt)

ANMERKUNG 1 Diese Tabelle liefert Beispielwerte für PFD_G, berechnet unter Verwendung der Gleichungen aus B.2.2 und beruhend auf den Annahmen in B.1. Wenn das Sensor-, Logik- oder Stellglied-Teilsystem nur aus einer Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider besteht, ist PFD_G gleich PFD_S, PFD_L bzw. PFD_{FE} (siehe B.2.1). ANMERKUNG 2 Diese Tabelle nimmt $\beta = 2 \times \beta_0$ an. Die Werte für β und β_0 beeinflussen die mittlere Wahrscheinlichkeit eines Ausfalls bei 1oo1- und 2oo2-Architekturen nicht. ANMERKUNG 3 Es werden gleiche Raten sicherer wie gefahrbringender Ausfälle angenommen, sowie $K = 0,98$.									
--	--	--	--	--	--	--	--	--	--

**Tabelle B.3 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung
für ein Wiederholungsprüfungsintervall von einem Jahr und eine mittlere Zeit zur
Wiederherstellung von 8 h**

Architektur	DC	$\lambda_D = 0,5E-07$			$\lambda_D = 2,5E-07$			$\lambda_D = 0,5E-06$		
		$\beta = 2 \%$ $\beta_0 = 1 \%$	$\beta = 10 \%$ $\beta_0 = 5 \%$	$\beta = 20 \%$ $\beta_0 = 10 \%$	$\beta = 2 \%$ $\beta_0 = 1 \%$	$\beta = 10 \%$ $\beta_0 = 5 \%$	$\beta = 20 \%$ $\beta_0 = 10 \%$	$\beta = 2 \%$ $\beta_0 = 1 \%$	$\beta = 10 \%$ $\beta_0 = 5 \%$	$\beta = 20 \%$ $\beta_0 = 10 \%$
1oo1 (s. Anm. 2)	0 %	2,2E-04			1,1E-03			2,2E-03		
	60 %	8,8E-05			4,4E-04			8,8E-04		
	90 %	2,2E-05			1,1E-04			2,2E-04		
	99 %	2,6E-06			1,3E-05			2,6E-05		
1oo2	0 %	4,4E-06	2,2E-05	4,4E-05	2,3E-05	1,1E-04	2,2E-04	5,0E-05	2,2E-04	4,4E-04
	60 %	1,8E-06	8,8E-06	1,8E-05	9,0E-06	4,4E-05	8,8E-05	1,9E-05	8,9E-05	1,8E-04
	90 %	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,5E-06	2,2E-05	4,4E-05
	99 %	4,8E-08	2,4E-07	4,8E-07	2,4E-07	1,2E-06	2,4E-06	4,8E-07	2,4E-06	4,8E-06
2oo2 (s. Anm. 2)	0 %	4,4E-04			2,2E-03			4,4E-03		
	60 %	1,8E-04			8,8E-04			1,8E-03		
	90 %	4,5E-05			2,2E-04			4,5E-04		
	99 %	5,2E-06			2,6E-05			5,2E-05		
1oo2D (s. Anm. 3)	0 %	4,5E-06	2,2E-05	4,4E-05	2,4E-05	1,1E-04	2,2E-04	5,0E-05	2,2E-04	4,4E-04
	60 %	2,8E-06	9,8E-06	1,9E-05	1,4E-05	4,9E-05	9,3E-05	2,9E-05	9,9E-05	1,9E-04
	90 %	8,5E-07	2,6E-06	4,8E-06	2,3E-06	1,3E-05	2,4E-05	8,5E-06	2,6E-05	4,8E-05
	99 %	1,0E-07	2,8E-07	5,0E-07	5,2E-07	1,4E-06	2,5E-06	1,0E-06	2,8E-06	5,0E-06
2oo3	0 %	4,6E-06	2,2E-05	4,4E-05	2,7E-05	1,1E-04	2,2E-04	6,2E-05	2,4E-04	4,5E-04
	60 %	1,8E-06	8,8E-06	1,8E-05	9,5E-06	4,5E-05	8,8E-05	2,1E-05	9,1E-05	1,8E-04
	90 %	4,4E-07	2,2E-06	4,4E-06	2,3E-06	1,1E-05	2,2E-05	4,6E-06	2,2E-05	4,4E-05
	99 %	4,8E-08	2,4E-07	4,8E-07	2,4E-07	1,2E-06	2,4E-06	4,8E-07	2,4E-06	4,8E-06
1oo3	0 %	4,4E-06	2,2E-05	4,4E-05	2,2E-05	1,1E-04	2,2E-04	4,4E-05	2,2E-04	4,4E-04
	60 %	1,8E-06	8,8E-06	1,8E-05	8,8E-06	4,4E-05	8,8E-05	1,8E-05	8,8E-05	1,8E-04
	90 %	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,4E-06	2,2E-05	4,4E-05
	99 %	4,8E-08	2,4E-07	4,8E-07	2,4E-07	1,2E-06	2,4E-06	4,8E-07	2,4E-06	4,8E-06

Tabelle B.3 (fortgesetzt)

Architektur	DC	$\lambda_D = 2,5E-06$			$\lambda_D = 0,5E-05$			$\lambda_D = 2,5E-05$		
		$\beta = 2\%$ $\beta_D = 1\%$	$\beta = 10\%$ $\beta_D = 5\%$	$\beta = 20\%$ $\beta_D = 10\%$	$\beta = 2\%$ $\beta_D = 1\%$	$\beta = 10\%$ $\beta_D = 5\%$	$\beta = 20\%$ $\beta_D = 10\%$	$\beta = 2\%$ $\beta_D = 1\%$	$\beta = 10\%$ $\beta_D = 5\%$	$\beta = 20\%$ $\beta_D = 10\%$
1oo1 (s. Anm. 2)	0 %	1,1E-02			2,2E-02			>1E-01		
	60 %	4,4E-03			8,8E-03			4,4E-02		
	90 %	1,1E-03			2,2E-03			1,1E-02		
	99 %	1,3E-04			2,6E-04			1,3E-03		
1oo2	0 %	3,7E-04	1,2E-03	2,3E-03	1,1E-03	2,7E-03	4,8E-03	1,8E-02	2,4E-02	3,2E-02
	60 %	1,1E-04	4,6E-04	9,0E-04	2,8E-04	9,7E-04	1,8E-03	3,4E-03	6,6E-03	1,1E-02
	90 %	2,4E-05	1,1E-04	2,2E-04	5,1E-05	2,3E-04	4,5E-04	3,8E-04	1,3E-03	2,3E-03
	99 %	2,4E-06	1,2E-05	2,4E-05	4,9E-06	2,4E-05	4,8E-05	2,6E-05	1,2E-04	2,4E-04
2oo2 (s. Anm. 2)	0 %	2,2E-02			4,4E-02			>1E-01		
	60 %	8,8E-03			1,8E-02			8,8E-02		
	90 %	2,2E-03			4,5E-03			2,2E-02		
	99 %	2,6E-04			5,2E-04			2,6E-03		
1oo2D (s. Anm. 3)	0 %	3,8E-04	1,2E-03	2,3E-03	1,1E-03	2,7E-03	4,9E-03	1,8E-02	2,5E-02	3,4E-02
	60 %	1,7E-04	5,1E-04	9,5E-04	3,8E-04	1,1E-03	1,9E-03	3,9E-03	7,1E-03	1,1E-02
	90 %	4,4E-05	1,3E-04	2,4E-04	9,1E-05	2,7E-04	4,8E-04	5,8E-04	1,4E-03	2,5E-03
	99 %	5,2E-06	1,4E-05	2,5E-05	1,0E-05	2,8E-05	5,0E-05	5,4E-05	1,4E-04	2,5E-04
2oo3	0 %	6,8E-04	1,5E-03	2,5E-03	2,3E-03	3,8E-03	5,6E-03	4,8E-02	5,0E-02	5,3E-02
	60 %	1,6E-04	5,1E-04	9,4E-04	4,8E-04	1,1E-03	2,0E-03	8,4E-03	1,1E-02	1,5E-02
	90 %	2,7E-05	1,2E-04	2,3E-04	6,4E-05	2,4E-04	4,6E-04	7,1E-04	1,6E-03	2,6E-03
	99 %	2,5E-06	1,2E-05	2,4E-05	5,1E-06	2,4E-05	4,8E-05	3,1E-05	1,3E-04	2,5E-04
1oo3	0 %	2,2E-04	1,1E-03	2,2E-03	4,6E-04	2,2E-03	4,4E-03	4,7E-03	1,3E-02	2,3E-02
	60 %	8,8E-05	4,4E-04	8,8E-04	1,8E-04	8,8E-04	1,8E-03	1,0E-03	4,5E-03	8,9E-03
	90 %	2,2E-05	1,1E-04	2,2E-04	4,4E-05	2,2E-04	4,4E-04	2,2E-04	1,1E-03	2,2E-03
	99 %	2,4E-06	1,2E-05	2,4E-05	4,8E-06	2,4E-05	4,8E-05	2,4E-05	1,2E-04	2,4E-04

ANMERKUNG 1 Diese Tabelle liefert Beispielwerte für PFD_G , berechnet unter Verwendung der Gleichungen aus B.2.2 und beruhend auf den Annahmen in B.1. Wenn das Sensor-, Logik- oder Stellglied-Teilsystem nur aus einer Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider besteht, ist PFD_G gleich PFD_S , PFD_L bzw. PFD_{FE} (siehe B.2.1).

ANMERKUNG 2 Diese Tabelle nimmt $\beta = 2 \times \beta_D$ an. Die Werte für β und β_D beeinflussen die mittlere Wahrscheinlichkeit eines Ausfalls bei 1oo1- und 2oo2-Architekturen nicht.

ANMERKUNG 3 Es werden gleiche Raten sicherer wie gefährbringender Ausfälle angenommen, sowie $K = 0,98$.

**Tabelle B.4 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung
für ein Wiederholungsprüfungsintervall von zwei Jahren und eine mittlere Zeit zur
Wiederherstellung von 8 h**

Architektur	DC	$\lambda_D = 0,5E-07$			$\lambda_D = 2,5E-07$			$\lambda_D = 0,5E-06$		
		$\beta = 2\%$ $\beta_D = 1\%$	$\beta = 10\%$ $\beta_D = 5\%$	$\beta = 20\%$ $\beta_D = 10\%$	$\beta = 2\%$ $\beta_D = 1\%$	$\beta = 10\%$ $\beta_D = 5\%$	$\beta = 20\%$ $\beta_D = 10\%$	$\beta = 2\%$ $\beta_D = 1\%$	$\beta = 10\%$ $\beta_D = 5\%$	$\beta = 20\%$ $\beta_D = 10\%$
1oo1 (s. Anm. 2)	0 %	4,4E-04			2,2E-03			4,4E-03		
	60 %	1,8E-04			8,8E-04			1,8E-03		
	90 %	4,4E-05			2,2E-04			4,4E-04		
	99 %	4,8E-06			2,4E-05			4,8E-05		
1oo2	0 %	9,0E-06	4,4E-05	8,8E-05	5,0E-05	2,2E-04	4,4E-04	1,1E-04	4,6E-04	8,9E-04
	60 %	3,5E-06	1,8E-05	3,5E-05	1,9E-05	8,9E-05	1,8E-04	3,9E-05	1,8E-04	3,5E-04
	90 %	8,8E-07	4,4E-06	8,8E-06	4,5E-06	2,2E-05	4,4E-05	9,1E-06	4,4E-05	8,8E-05
	99 %	9,2E-08	4,6E-07	9,2E-07	4,6E-07	2,3E-06	4,6E-06	9,2E-07	4,6E-06	9,2E-06
2oo2 (s. Anm. 2)	0 %	8,8E-04			4,4E-03			8,8E-03		
	60 %	3,5E-04			1,8E-03			3,5E-03		
	90 %	8,8E-05			4,4E-04			8,8E-04		
	99 %	9,6E-06			4,8E-05			9,6E-05		
1oo2D (s. Anm. 3)	0 %	9,0E-06	4,4E-05	8,8E-05	5,0E-05	2,2E-04	4,4E-04	1,1E-04	4,6E-04	9,0E-04
	60 %	5,7E-06	2,0E-05	3,7E-05	2,9E-05	9,9E-05	1,9E-04	6,0E-05	2,0E-04	3,7E-04
	90 %	1,7E-06	5,2E-06	9,6E-06	8,5E-06	2,6E-05	4,8E-05	1,7E-05	5,2E-05	9,6E-05
	99 %	1,9E-07	5,4E-07	9,8E-07	9,5E-07	2,7E-06	4,9E-06	1,9E-06	5,4E-06	9,8E-06
2oo3	0 %	9,5E-06	4,4E-05	8,8E-05	6,2E-05	2,3E-04	4,5E-04	1,6E-04	5,0E-04	9,3E-04
	60 %	3,6E-06	1,8E-05	3,5E-05	2,1E-05	9,0E-05	1,8E-04	4,7E-05	1,9E-04	3,6E-04
	90 %	8,9E-07	4,4E-06	8,8E-06	4,6E-06	2,2E-05	4,4E-05	9,6E-06	4,5E-05	8,9E-05
	99 %	9,2E-08	4,6E-07	9,2E-07	4,6E-07	2,3E-06	4,6E-06	9,3E-07	4,6E-06	9,2E-06
1oo3	0 %	8,8E-06	4,4E-05	8,8E-05	4,4E-05	2,2E-04	4,4E-04	8,8E-05	4,4E-04	8,8E-04
	60 %	3,5E-06	1,8E-05	3,5E-05	1,8E-05	9,8E-05	1,8E-04	3,5E-05	1,8E-04	3,5E-04
	90 %	8,8E-07	4,4E-06	8,8E-06	4,6E-06	2,2E-05	4,4E-05	8,8E-06	4,4E-05	8,8E-05
	99 %	9,2E-08	4,6E-07	9,2E-07	4,6E-07	2,3E-06	4,6E-06	9,2E-07	4,6E-06	9,2E-06

Architektur	DC	$\lambda_D = 2,5E-06$			$\lambda_D = 0,5E-05$			$\lambda_D = 2,5E-05$		
		$\beta = 2\%$ $\beta_D = 1\%$	$\beta = 10\%$ $\beta_D = 5\%$	$\beta = 20\%$ $\beta_D = 10\%$	$\beta = 2\%$ $\beta_D = 1\%$	$\beta = 10\%$ $\beta_D = 5\%$	$\beta = 20\%$ $\beta_D = 10\%$	$\beta = 2\%$ $\beta_D = 1\%$	$\beta = 10\%$ $\beta_D = 5\%$	$\beta = 20\%$ $\beta_D = 10\%$
1oo1 (s. Anm. 2)	0 %	2,2E-02			4,4E-02			>1E-01		
	60 %	8,8E-03			1,8E-02			8,8E-02		
	90 %	2,2E-03			4,4E-03			2,2E-02		
	99 %	2,4E-04			4,8E-04			2,4E-03		
1oo2	0 %	1,1E-03	2,7E-03	4,8E-03	3,3E-03	6,5E-03	1,0E-02	6,6E-02	7,4E-02	8,5E-02
	60 %	2,8E-04	9,7E-04	1,8E-03	7,5E-04	2,1E-03	3,8E-03	1,2E-02	1,8E-02	2,5E-02
	90 %	5,0E-05	2,3E-04	4,5E-04	1,1E-04	4,6E-04	9,0E-04	1,1E-03	2,8E-03	4,9E-03
	99 %	4,7E-06	2,3E-05	4,6E-05	9,5E-06	4,6E-05	9,2E-05	5,4E-05	2,4E-04	4,6E-04
2oo2 (s. Anm. 2)	0 %	4,4E-02			8,8E-02			>1E-01		
	60 %	1,8E-02			3,5E-02			>1E-01		
	90 %	4,4E-03			8,8E-03			4,4E-02		
	99 %	4,8E-04			9,6E-04			4,8E-03		
1oo2D (s. Anm. 3)	0 %	1,1E-03	2,7E-03	4,8E-03	3,3E-03	6,6E-03	1,1E-02	6,7E-02	7,4E-02	9,0E-02
	60 %	3,8E-04	1,1E-03	1,9E-03	9,6E-04	2,3E-03	4,0E-03	1,3E-02	1,9E-02	2,6E-02
	90 %	9,0E-05	2,6E-04	4,8E-04	1,9E-04	5,4E-04	9,8E-04	1,5E-03	3,2E-03	5,3E-03
	99 %	9,6E-06	2,7E-05	4,9E-05	1,9E-05	5,4E-05	9,8E-05	1,0E-04	2,8E-04	5,0E-04
2oo3	0 %	2,3E-03	3,7E-03	5,6E-03	8,3E-03	1,1E-02	1,4E-02	1,9E-01	1,8E-01	1,7E-01
	60 %	4,8E-04	1,1E-03	2,0E-03	1,6E-03	2,8E-03	4,4E-03	3,2E-02	3,5E-02	4,0E-02
	90 %	6,3E-05	2,4E-04	4,6E-04	1,6E-04	5,1E-04	9,4E-04	2,4E-03	4,0E-03	6,0E-03
	99 %	4,8E-06	2,3E-05	4,6E-05	1,0E-05	4,7E-05	9,2E-05	6,9E-05	2,5E-04	4,8E-04
1oo3	0 %	4,6E-04	2,2E-03	4,4E-03	1,0E-03	4,5E-03	8,9E-03	2,4E-02	3,7E-02	5,5E-02
	60 %	1,8E-04	8,8E-04	1,8E-03	3,6E-04	1,8E-03	3,5E-03	3,1E-03	9,9E-03	1,8E-02
	90 %	4,4E-05	2,2E-04	4,4E-04	8,8E-05	4,4E-04	8,8E-04	4,6E-04	2,2E-03	4,4E-03
	99 %	4,6E-06	2,3E-05	4,6E-05	9,2E-06	4,6E-05	9,2E-05	4,6E-05	2,3E-04	4,6E-04

ANMERKUNG 1 Diese Tabelle liefert Beispielwerte für PF_{DG} , berechnet unter Verwendung der Gleichungen aus B.2.2 und beruhend auf den Annahmen in B.1. Wenn das Sensor-, Logik- oder Stellglied-Teilsystem nur aus einer Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider besteht, ist PF_{DG} gleich PF_{DS} , PF_{DL} bzw. PF_{FE} (siehe B.2.1).

ANMERKUNG 2 Diese Tabelle nimmt $\beta = 2 \times \beta_D$ an. Die Werte für β und β_D beeinflussen die mittlere Wahrscheinlichkeit eines Ausfalls bei 1oo1- und 2oo2-Architekturen nicht.

ANMERKUNG 3 Es werden gleiche Raten sicherer wie gefahrbringender Ausfälle angenommen, sowie $K = 0,98$.

**Tabelle B.5 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung
für ein Wiederholungsprüfungsintervall von 10 Jahren und eine mittlere Zeit zur
Wiederherstellung von 8 h**

Architektur	DC	$\lambda_D = 0,5E-07$			$\lambda_D = 2,5E-07$			$\lambda_D = 0,5E-06$		
		$\beta = 2\%$ $\beta_D = 1\%$	$\beta = 10\%$ $\beta_D = 5\%$	$\beta = 20\%$ $\beta_D = 10\%$	$\beta = 2\%$ $\beta_D = 1\%$	$\beta = 10\%$ $\beta_D = 5\%$	$\beta = 20\%$ $\beta_D = 10\%$	$\beta = 2\%$ $\beta_D = 1\%$	$\beta = 10\%$ $\beta_D = 5\%$	$\beta = 20\%$ $\beta_D = 10\%$
1oo1 (s. Anm. 2)	0 %	2,2E-03			1,1E-02			2,2E-02		
	60 %	8,8E-04			4,4E-03			8,8E-03		
	90 %	2,2E-04			1,1E-03			2,2E-03		
	99 %	2,2E-05			1,1E-04			2,2E-04		
1oo2	0 %	5,0E-05	2,2E-04	4,4E-04	3,7E-04	1,2E-03	2,3E-03	1,1E-03	2,7E-03	4,8E-03
	60 %	1,9E-05	8,9E-05	1,8E-04	1,1E-04	4,6E-04	9,0E-04	2,7E-04	9,6E-04	1,8E-03
	90 %	4,4E-06	2,2E-05	4,4E-05	2,3E-05	1,1E-04	2,2E-04	5,0E-05	2,2E-04	4,4E-04
	99 %	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,5E-06	2,2E-05	4,4E-05
2oo2 (s. Anm. 2)	0 %	4,4E-03			2,2E-02			4,4E-02		
	60 %	1,8E-03			8,8E-03			1,8E-02		
	90 %	4,4E-04			2,2E-03			4,4E-03		
	99 %	4,5E-05			2,2E-04			4,5E-04		
1oo2D (s. Anm. 3)	0 %	5,0E-05	2,2E-04	4,4E-04	3,7E-04	1,2E-03	2,3E-03	1,1E-03	2,7E-03	4,8E-03
	60 %	2,9E-05	9,9E-05	1,9E-04	1,7E-04	5,1E-04	9,5E-04	3,8E-04	1,1E-03	1,9E-03
	90 %	8,4E-06	2,6E-05	4,8E-05	4,3E-05	1,3E-04	2,4E-04	9,0E-05	2,6E-04	4,8E-04
	99 %	8,9E-07	2,6E-06	4,8E-06	4,5E-06	1,3E-05	2,4E-05	8,9E-06	2,6E-05	4,8E-05
2oo3	0 %	6,2E-05	2,3E-04	4,5E-04	6,8E-04	1,5E-03	2,5E-03	2,3E-03	3,7E-03	5,6E-03
	60 %	2,1E-05	9,0E-05	1,8E-04	1,6E-04	5,0E-04	9,3E-04	4,7E-04	1,1E-03	2,0E-03
	90 %	4,6E-06	2,2E-05	4,4E-05	2,7E-05	1,1E-04	2,2E-04	6,3E-05	2,4E-04	4,5E-04
	99 %	4,4E-07	2,2E-06	4,4E-06	2,3E-06	1,1E-05	2,2E-05	4,6E-06	2,2E-05	4,4E-05
1oo3	0 %	4,4E-05	2,2E-04	4,4E-04	2,2E-04	1,1E-03	2,2E-03	4,6E-04	2,2E-03	4,4E-03
	60 %	1,8E-05	8,8E-05	1,8E-04	8,8E-05	4,4E-04	8,8E-04	1,8E-04	8,8E-04	1,8E-03
	90 %	4,4E-06	2,2E-05	4,4E-05	2,2E-05	1,1E-04	2,2E-04	4,4E-05	2,2E-04	4,4E-04
	99 %	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,4E-06	2,2E-05	4,4E-05

Architektur	DC	$\lambda_D = 2,5E-06$			$\lambda_D = 0,5E-05$			$\lambda_D = 2,5E-05$		
		$\beta = 2\%$ $\beta_D = 1\%$	$\beta = 10\%$ $\beta_D = 5\%$	$\beta = 20\%$ $\beta_D = 10\%$	$\beta = 2\%$ $\beta_D = 1\%$	$\beta = 10\%$ $\beta_D = 5\%$	$\beta = 20\%$ $\beta_D = 10\%$	$\beta = 2\%$ $\beta_D = 1\%$	$\beta = 10\%$ $\beta_D = 5\%$	$\beta = 20\%$ $\beta_D = 10\%$
1oo1 (s. Anm. 2)	0 %	>1E-01			>1E-01			>1E-01		
	60 %	4,4E-02			8,8E-02			>1E-01		
	90 %	1,1E-02			2,2E-02			>1E-01		
	99 %	1,1E-03			2,2E-03			1,1E-02		
1oo2	0 %	1,8E-02	2,4E-02	3,2E-02	6,6E-02	7,4E-02	8,5E-02	>1E-01	>1E-01	>1E-01
	60 %	3,4E-03	6,6E-03	1,1E-02	1,2E-02	1,8E-02	2,5E-02	>1E-01	>1E-01	>1E-01
	90 %	3,8E-04	1,2E-03	2,3E-03	1,1E-03	2,8E-03	4,9E-03	1,8E-02	2,5E-02	3,5E-02
	99 %	2,4E-05	1,1E-04	2,2E-04	5,1E-05	2,3E-04	4,5E-04	3,8E-04	1,3E-03	2,3E-03
2oo2 (s. Anm. 2)	0 %	>1E-01			>1E-01			>1E-01		
	60 %	8,8E-02			>1E-01			>1E-01		
	90 %	2,2E-02			4,4E-02			>1E-01		
	99 %	2,2E-03			4,5E-03			2,2E-02		
1oo2D (s. Anm. 3)	0 %	1,8E-02	2,5E-02	3,3E-02	6,6E-02	7,7E-02	9,0E-02	1,6E+00	1,5E+00	1,4E+00
	60 %	3,9E-03	7,1E-03	1,1E-02	1,3E-02	1,9E-02	2,6E-02	2,6E-01	2,7E-01	2,8E-01
	90 %	5,7E-04	1,4E-03	2,5E-03	1,5E-03	3,1E-03	5,2E-03	2,0E-02	2,7E-02	3,5E-02
	99 %	4,6E-05	1,3E-04	2,4E-04	9,5E-05	2,7E-04	4,9E-04	6,0E-04	1,5E-03	2,5E-03
2oo3	0 %	4,8E-02	5,0E-02	5,3E-02	1,9E-01	1,8E-01	1,7E-01	4,6E+00	4,0E+00	3,3E+00
	60 %	8,3E-03	1,1E-02	1,4E-02	3,2E-02	3,5E-02	4,0E-02	7,6E-01	7,1E-01	6,6E-01
	90 %	6,9E-04	1,5E-03	2,6E-03	2,3E-03	3,9E-03	5,9E-03	4,9E-02	5,4E-02	6,0E-02
	99 %	2,7E-05	1,2E-04	2,3E-04	6,4E-05	2,4E-04	4,6E-04	7,1E-04	1,6E-03	2,6E-03
1oo3	0 %	4,7E-03	1,3E-02	2,3E-02	2,4E-02	3,7E-02	5,5E-02	2,5E+00	2,0E+00	1,6E+00
	60 %	1,0E-03	4,5E-03	8,9E-03	3,0E-03	9,8E-03	1,8E-02	1,7E-01	1,8E-01	1,9E-01
	90 %	2,2E-04	1,1E-03	2,2E-03	4,6E-04	2,2E-03	4,4E-03	4,8E-03	1,3E-02	2,4E-02
	99 %	2,2E-05	1,1E-04	2,2E-04	4,4E-05	2,2E-04	4,4E-04	2,2E-04	1,1E-03	2,2E-03

ANMERKUNG 1 Diese Tabelle liefert Beispielwerte für PF_{DG} , berechnet unter Verwendung der Gleichungen aus B.2.2 und beruhend auf den Annahmen in B.1. Wenn das Sensor-, Logik- oder Stellglied-Teilsystem nur aus einer Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider besteht, ist PF_{DG} gleich PF_{DS} , PF_{DL} bzw. PF_{FE} (siehe B.2.1).

ANMERKUNG 2 Diese Tabelle nimmt $\beta = 2 \times \beta_D$ an. Die Werte für β und β_D beeinflussen die mittlere Wahrscheinlichkeit eines Ausfalls bei 1oo1- und 2oo2-Architekturen nicht.

ANMERKUNG 3 Es werden gleiche Raten sicherer wie gefährbringender Ausfälle angenommen, sowie $K = 0,98$.

B.3.2.4 Beispiel für die Betriebsart mit niedriger Anforderungsrate

Es sei eine Sicherheitsfunktion betrachtet, die ein System mit SIL 2 erfordert. Es sei weiter angenommen, dass die erste Beurteilung auf der Basis früherer Erfahrungen im Hinblick auf die Systemarchitektur zu einer Gruppe von drei analogen Drucksensoren mit 2oo3-Mehrheitsentscheider geführt hat. Das Logik-Teilsystem ist ein PES, das als redundantes 1oo2D-System aufgebaut ist und ein Absperr- und ein Ablassventil ansteuert. Zur Erreichung der Sicherheitsfunktion müssen beide Ventile arbeiten. Die entsprechende Architektur ist in Bild B.14 dargestellt. Bei der ersten Beurteilung wurde ein Wiederholungsprüfungsintervall von einem Jahr angenommen.

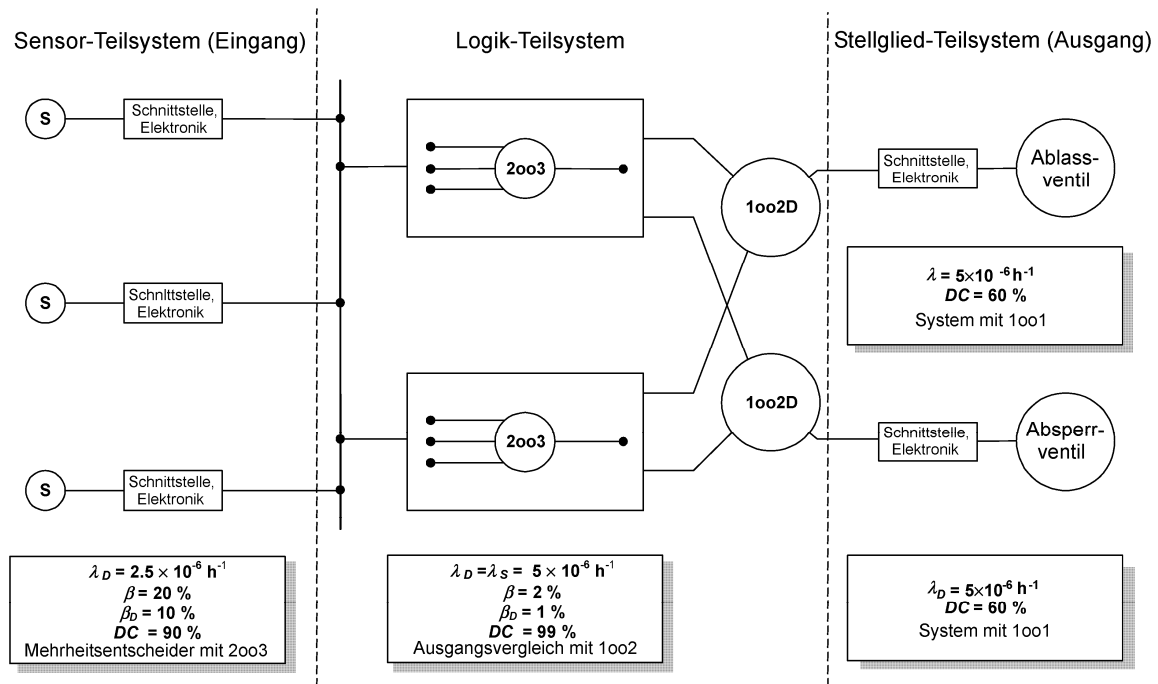


Bild B.14 – Architektur des Beispiels für die Betriebsart mit niedriger Anforderungsrate

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 MTTR)

Architektur	DC	$\lambda_D = 2,5E-06$		
		$\beta = 2 \%$ $\beta_D = 1 \%$	$\beta = 10 \%$ $\beta_D = 5 \%$	$\beta = 20 \%$ $\beta_D = 10 \%$
2oo3	0 %	6,8E-04	1,5E-03	2,5E-03
	60 %	1,6E-04	5,1E-04	9,4E-04
	90 %	2,7E-05	1,2E-04	2,3E-04
	99 %	2,5E-06	1,2E-05	2,4E-05
ANMERKUNG Diese Tabelle ist ein Auszug aus Tabelle B.3.				

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 MTTR)

Architektur	DC	$\lambda_D = 0,5E-05$		
		$\beta = 2 \%$ $\beta_D = 1 \%$	$\beta = 10 \%$ $\beta_D = 5 \%$	$\beta = 20 \%$ $\beta_D = 10 \%$
1002D	0 %	1,1E-03	2,7E-03	4,8E-03
	60 %	2,0E-04	9,0E-04	1,8E-03
	90 %	4,5E-05	2,2E-04	4,4E-04
	99 %	4,8E-06	2,4E-05	4,8E-05
ANMERKUNG Diese Tabelle ist ein Auszug aus Tabelle B.3.				

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 MTTR)

Architektur	DC	$\lambda_D = 2,5E-06$	$\lambda_D = 0,5E-05$
1001	0 %	1,1E-02	2,2E-02
	60 %	4,4E-03	8,8E-03
	90 %	1,1E-03	2,2E-03
	99 %	1,3E-04	2,6E-04
ANMERKUNG Diese Tabelle ist ein Auszug aus Tabelle B.3.			

Aus den Tabellen B.6 bis B.8 werden folgende Werte entnommen.

Für das Sensor-Teilsystem:

$$PFD_S = 2,3 \times 10^{-4}$$

Für das Logik-Teilsystem:

$$PFD_L = 4,8 \times 10^{-6}$$

Für das Stellglied-Teilsystem:

$$PFD_{FE} = 4,4 \times 10^{-3} + 8,8 \times 10^{-3}$$

$$= 1,3 \times 10^{-2}$$

Daraus ergibt sich für die Sicherheitsfunktion:

$$PFD_{SYS} = 2,3 \times 10^{-4} + 4,8 \times 10^{-6} + 1,3 \times 10^{-2}$$

$$= 1,3 \times 10^{-2}$$

$$\equiv \text{Sicherheits-Integritätslevel 1}$$

Um das System für den Sicherheits-Integritätslevel 2 zu ertüchtigen, kann eine der folgenden Maßnahmen durchgeführt werden:

- a) Wiederholungsprüfungsintervall auf 6 Monate bringen

$$PFD_S = 1,1 \times 10^{-4}$$

$$PFD_L = 2,6 \times 10^{-6}$$

$$\begin{aligned} PFD_{FE} &= 2,2 \times 10^{-3} + 4,4 \times 10^{-3} \\ &= 6,6 \times 10^{-3} \end{aligned}$$

$$PFD_{SYS} = 6,7 \times 10^{-3}$$

≡ **Sicherheits-Integritätslevel 2**

- b) Absperrventil (das ist das Ausgabegerät mit der niedrigeren Zuverlässigkeit) von 1oo1 auf 1oo2 (angenommenes $\beta = 10\%$ und $\beta_D = 5\%$) bringen

$$PFD_S = 2,3 \times 10^{-4}$$

$$PFD_L = 4,8 \times 10^{-6}$$

$$\begin{aligned} PFD_{FE} &= 4,4 \times 10^{-3} + 9,7 \times 10^{-4} \\ &= 5,4 \times 10^{-3} \end{aligned}$$

$$PFD_{SYS} = 5,6 \times 10^{-3}$$

≡ **Sicherheits-Integritätslevel 2**

B.3.2.5 Auswirkungen einer nicht ausreichenden Wiederholungsprüfung

Fehler im Sicherheitssystem, die weder während Diagnosetests noch durch die Wiederholungsprüfungen erkannt wurden, werden durch andere Vorgänge entdeckt, wie eine Anforderung an die Sicherheitsfunktion, Zeit zwischen der gesamten Einrichtung oder, wenn solche Vorfälle innerhalb der erwarteten Lebensdauer von Einrichtung/Anlage unwahrscheinlich sind, dann sollte der Zeitraum der Lebensdauer angewendet werden. Wird eine übliche Dauer für die Wiederholungsprüfung berücksichtigt, entspricht T_1 mit einem Wiederholungsprüfungsdeckungsgrad (PTC) und den anderweitig entdeckten Fehlern ($1-PTC$), der erwarteten Zeit T_2 zwischen den Anforderungen an das Sicherheitssystem. Demzufolge sind diese beiden Zeiten maßgeblich für die wirksame Unklarzeit.

Ein Beispiel hierfür wird unten stehend für eine 1oo2-Architektur gegeben. T_2 ist dabei die Zeit zwischen den Anforderungen an das System:

$$t_{CE} = \frac{\lambda_{DU}(PTC)}{\lambda_D} \left(\frac{T_1}{2} + MTTR \right) + \frac{\lambda_{DU}(1-PTC)}{\lambda_D} \left(\frac{T_2}{2} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$t_{GE} = \frac{\lambda_{DU}(PTC)}{\lambda_D} \left(\frac{T_1}{3} + MTTR \right) + \frac{\lambda_{DU}(1-PTC)}{\lambda_D} \left(\frac{T_2}{3} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$PFD_G = 2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU} (PTC) \left(\frac{T_1}{2} + MTTR \right) + \beta \lambda_{DU} (1-PTC) \left(\frac{T_2}{2} + MTTR \right)$$

Die Tabelle B.9 unten zeigt die zahlenmäßigen Ergebnisse eines 1oo2-Systems mit einer 100 %igen jährlichen Wiederholungsprüfung ($T_1 = 1$ Jahr) im Vergleich zu einer 90 %igen Wiederholungsprüfung, wobei die Anforderungsrate T_2 mit 10 Jahren angenommen wurde. Dieses Beispiel wurde unter der Annahme einer Ausfallrate von $0,5 \times 10^{-5}$ je Stunde, einem β -Wert von 10 % und einem β_D -Wert von 5 % berechnet.

Tabelle B.9 – Beispiel für eine nicht ausreichende Wiederholungsprüfung

Architektur	DC	$\lambda_D = 0,5E-05$	
		100 %-Wiederholungsprüfung	90 %-Wiederholungsprüfung
		$\beta = 10 \%$ $\beta_D = 5 \%$	$\beta = 10 \%$ $\beta_D = 5 \%$
1002	0 %	2,7E-03	6,0E-03
	60 %	9,7E-04	2,0E-03
	90 %	2,3E-04	4,4E-04
	99 %	2,4E-05	4,4E-05

B.3.3 Wahrscheinlichkeit eines Ausfalls je Stunde (für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung)

B.3.3.1 Verfahren für die Berechnung

Die Methode für die Berechnung der Wahrscheinlichkeit eines Ausfalls einer Sicherheitsfunktion eines E/E/PE sicherheitsbezogenen Systems in der Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung ist gleich derjenigen für ein System in der Betriebsart mit niedriger Anforderungsrate (siehe B.2.1), außer dass die mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung (PFH_{SYS}) durch die Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde (PFH_{SYS}) ersetzt wird.

Die Gesamtwahrscheinlichkeit eines gefahrbringenden Ausfalls einer Sicherheitsfunktion eines E/E/PE sicherheitsbezogenen Systems (PFH_{SYS}) wird bestimmt durch die Berechnung der Raten der gefahrbringenden Ausfälle aller Teilsysteme, die gemeinsam die Sicherheitsfunktion erbringen, und deren Addition. Da in diesem Anhang die Wahrscheinlichkeiten klein sind, kann dies wie folgt ausgedrückt werden:

$$PFH_{SYS} = PFH_S + PFH_L + PFH_{FE}$$

Dabei ist

- PFH_{SYS} die Wahrscheinlichkeit eines Ausfalls der Sicherheitsfunktion des E/E/PE-sicherheitsbezogenen Systems je Stunde;
- PFH_S die Wahrscheinlichkeit eines Ausfalls des Sensor-Teilsystems je Stunde;
- PFH_L die Wahrscheinlichkeit eines Ausfalls des Logik-Teilsystems je Stunde;
- PFH_{FE} die Wahrscheinlichkeit eines Ausfalls des Stellglied-Teilsystems je Stunde.

B.3.3.2 Architekturen für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung

ANMERKUNG 1 Dieser Unterabschnitt sollte in der richtigen Reihenfolge gelesen werden, da Gleichungen für mehrere Architekturen nur bei ihrer ersten Verwendung angegeben werden. Siehe auch B.3.2.2.

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

B.3.3.2.1 1001

Bild B.4 enthält das zugehörige Blockschaltbild und Bild B.5 das Zuverlässigkeits-Blockdiagramm.

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

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

$$\lambda_{DU} = \frac{\lambda}{2}(1-DC); \lambda_{DD} = \frac{\lambda}{2}DC$$

Wenn angenommen wird, dass das Sicherheitssystem bei jedem erkannten Ausfall die EUC in den sicheren Zustand bringt, wird für eine 1oo1-Architektur Folgendes erreicht:

$$PFH_G = \lambda_{DU}$$

B.3.3.2.2 1oo2

Bild B.6 enthält das zugehörige Blockschaltbild und Bild B.7 das Zuverlässigkeits-Blockdiagramm. Der Wert von t_{CE} ist wie in B.3.3.2.1 angegeben.

$$PFH_G = 2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} + \beta_D \lambda_{DD} + \beta \lambda_{DU}$$

B.3.3.2.3 2oo2

Bild B.8 enthält das zugehörige Blockschaltbild und Bild B.9 das Zuverlässigkeits-Blockdiagramm. Wenn angenommen wird, dass jeder Kanal bei Erkennen eines Fehlers in den sicheren Zustand gesetzt werden kann, wird für eine 2oo2-Architektur Folgendes erreicht:

$$PFH_G = 2\lambda_{DU}$$

B.3.3.2.4 1oo2D

Bild B.10 enthält das zugehörige Blockschaltbild und Bild B.11 das Zuverlässigkeits-Blockdiagramm.

$$\lambda_{SD} = \frac{\lambda}{2}DC$$

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

$$PFH_G = 2(1-\beta)\lambda_{DU}((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} + \lambda_{SD})t_{CE}' + 2(1-K)(\lambda_{DU} + \lambda_{DD}) + \beta\lambda_{DU}$$

B.3.3.2.5 2oo3

Bild B.12 enthält das zugehörige Blockschaltbild und Bild B.13 das Zuverlässigkeits-Blockdiagramm. Der Wert von t_{CE} ist wie in B.3.3.2.1 angegeben.

$$PFH_G = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} + \beta_D \lambda_{DD} + \beta \lambda_{DU}$$

B.3.3.2.6 1oo3

Bild B.12 enthält das zugehörige Blockschaltbild und Bild B.13 das Zuverlässigkeits-Blockdiagramm. Die Werte von t_{CE} und t_{GE} sind wie in B.3.3.2.1 angegeben.

$$PFH_G = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^3 t_{CE} t_{GE} + \beta_D \lambda_{DD} + \beta \lambda_{DU}$$

B.3.3.3 Tabellen für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung

Tabelle B.10 – Wahrscheinlichkeit eines Ausfalls je Stunde (für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung) für ein Wiederholungsprüfungsintervall von einem Monat und eine mittlere Zeit zur Wiederherstellung von 8 h

Architektur	DC	$\lambda_D = 0,5E-07$			$\lambda_D = 2,5E-07$			$\lambda_D = 0,5E-06$		
		$\beta = 2\%$ $\beta_D = 1\%$	$\beta = 10\%$ $\beta_D = 5\%$	$\beta = 20\%$ $\beta_D = 10\%$	$\beta = 2\%$ $\beta_D = 1\%$	$\beta = 10\%$ $\beta_D = 5\%$	$\beta = 20\%$ $\beta_D = 10\%$	$\beta = 2\%$ $\beta_D = 1\%$	$\beta = 10\%$ $\beta_D = 5\%$	$\beta = 20\%$ $\beta_D = 10\%$
1oo1 (s. Anm. 2)	0 %	5,0E-08			2,5E-07			5,0E-07		
	60 %	2,0E-08			1,0E-07			2,0E-07		
	90 %	5,0E-09			2,5E-08			5,0E-08		
	99 %	5,0E-10			2,5E-09			5,0E-09		
1oo2	0 %	1,0E-09	5,0E-09	1,0E-08	5,0E-09	2,5E-08	5,0E-08	1,0E-08	5,0E-08	1,0E-07
	60 %	7,0E-10	3,5E-09	7,0E-09	3,5E-09	1,8E-08	3,5E-08	7,1E-09	3,5E-08	7,0E-08
	90 %	5,5E-10	2,8E-09	5,5E-09	2,8E-09	1,4E-08	2,8E-08	5,5E-09	2,8E-08	5,5E-08
	99 %	5,1E-10	2,5E-09	5,1E-09	2,5E-09	1,3E-08	2,5E-08	5,1E-09	2,5E-08	5,1E-08
2oo2 (s. Anm. 2)	0 %	1,0E-07			5,0E-07			1,0E-06		
	60 %	4,0E-08			2,0E-07			4,0E-07		
	90 %	1,0E-08			5,0E-08			1,0E-07		
	99 %	1,0E-09			5,0E-09			1,0E-08		
1oo2D (s. Anm. 3)	0 %	1,0E-09	5,0E-09	1,0E-08	5,0E-09	2,5E-08	5,0E-08	1,0E-08	5,0E-08	1,0E-07
	60 %	1,6E-09	3,2E-09	5,2E-09	8,0E-09	1,6E-08	2,6E-08	1,6E-08	3,2E-08	5,2E-08
	90 %	1,9E-09	2,3E-09	2,8E-09	9,5E-09	1,2E-08	1,4E-08	1,9E-08	2,3E-08	2,8E-08
	99 %	2,0E-09	2,0E-09	2,1E-09	1,0E-08	1,0E-08	1,0E-08	2,0E-08	2,0E-08	2,1E-08
2oo3	0 %	1,0E-09	5,0E-09	1,0E-08	5,1E-09	2,5E-08	5,0E-08	1,1E-08	5,0E-08	1,0E-07
	60 %	7,0E-10	3,5E-09	7,0E-09	3,6E-09	1,8E-08	3,5E-08	7,2E-09	3,5E-08	7,0E-08
	90 %	5,5E-10	2,8E-09	5,5E-09	2,8E-09	1,4E-08	2,8E-08	5,6E-09	2,8E-08	5,5E-08
	99 %	5,1E-10	2,5E-09	5,1E-09	2,5E-09	1,3E-08	2,5E-08	5,1E-09	2,5E-08	5,1E-08
1oo3	0 %	1,0E-09	5,0E-09	1,0E-08	5,0E-09	2,5E-08	5,0E-08	1,0E-08	5,0E-08	1,0E-07
	60 %	7,0E-10	3,5E-09	7,0E-09	3,5E-09	1,8E-08	3,5E-08	7,0E-09	3,5E-08	7,0E-08
	90 %	5,5E-10	2,8E-09	5,5E-09	2,8E-09	1,4E-08	2,8E-08	5,5E-09	2,8E-08	5,5E-08
	99 %	5,1E-10	2,5E-09	5,1E-09	2,5E-09	1,3E-08	2,5E-08	5,1E-09	2,5E-08	5,1E-08

Architektur	DC	$\lambda_D = 2,5E-06$			$\lambda_D = 0,5E-05$			$\lambda_D = 2,5E-05$		
		$\beta = 2\%$ $\beta_D = 1\%$	$\beta = 10\%$ $\beta_D = 5\%$	$\beta = 20\%$ $\beta_D = 10\%$	$\beta = 2\%$ $\beta_D = 1\%$	$\beta = 10\%$ $\beta_D = 5\%$	$\beta = 20\%$ $\beta_D = 10\%$	$\beta = 2\%$ $\beta_D = 1\%$	$\beta = 10\%$ $\beta_D = 5\%$	$\beta = 20\%$ $\beta_D = 10\%$
1oo1 (s. Anm. 2)	0 %	2,5E-06			5,0E-06			>1E-05		
	60 %	1,0E-06			2,0E-06			1,0E-05		
	90 %	2,5E-07			5,0E-07			2,5E-06		
	99 %	2,5E-08			5,0E-08			2,5E-07		
1oo2	0 %	5,4E-08	2,5E-07	5,0E-07	1,2E-07	5,2E-07	1,0E-06	9,5E-07	2,9E-06	5,3E-06
	60 %	3,7E-08	1,8E-07	3,5E-07	7,7E-08	3,6E-07	7,1E-07	5,4E-07	1,9E-06	3,6E-06
	90 %	2,8E-08	1,4E-07	2,8E-07	5,7E-08	2,8E-07	5,5E-07	3,3E-07	1,4E-06	2,8E-06
	99 %	2,5E-08	1,3E-07	2,5E-07	5,1E-08	2,5E-07	5,1E-07	2,7E-07	1,3E-06	2,5E-06
2oo2 (s. Anm. 2)	0 %	5,0E-06			1,0E-05			>1E-05		
	60 %	2,0E-06			4,0E-06			>1E-05		
	90 %	5,0E-07			1,0E-06			5,0E-06		
	99 %	5,0E-08			1,0E-07			5,0E-07		
1oo2D (s. Anm. 3)	0 %	5,4E-08	2,5E-07	5,0E-07	1,2E-07	5,2E-07	1,0E-06	9,5E-07	2,9E-06	5,3E-06
	60 %	8,1E-08	1,6E-07	2,6E-07	1,6E-07	3,2E-07	5,2E-07	8,7E-07	1,7E-06	2,7E-06
	90 %	9,5E-08	1,2E-07	1,4E-07	1,9E-07	2,3E-07	2,8E-07	9,6E-07	1,2E-06	1,4E-06
	99 %	1,0E-07	1,0E-07	1,0E-07	2,0E-07	2,0E-07	2,1E-07	1,0E-06	1,0E-06	1,0E-06
2oo3	0 %	6,3E-08	2,6E-07	5,1E-07	1,5E-07	5,5E-07	1,0E-06	1,8E-06	3,6E-06	5,9E-06
	60 %	4,1E-08	1,8E-07	3,5E-07	9,2E-08	3,7E-07	7,2E-07	9,1E-07	2,2E-06	3,9E-06
	90 %	2,9E-08	1,4E-07	2,8E-07	6,2E-08	2,8E-07	5,6E-07	4,4E-07	1,5E-06	2,9E-06
	99 %	2,6E-08	1,3E-07	2,5E-07	5,2E-08	2,5E-07	5,1E-07	3,0E-07	1,3E-06	2,6E-06
1oo3	0 %	5,0E-08	2,5E-07	5,0E-07	1,0E-07	5,0E-07	1,0E-06	5,1E-07	2,5E-06	5,0E-06
	60 %	3,5E-08	1,8E-07	3,5E-07	7,0E-08	3,5E-07	7,0E-07	3,5E-07	1,8E-06	3,5E-06
	90 %	2,8E-08	1,4E-07	2,8E-07	5,5E-08	2,8E-07	5,5E-07	2,8E-07	1,4E-06	2,8E-06
	99 %	2,5E-08	1,3E-07	2,5E-07	5,1E-08	2,5E-07	5,1E-07	2,5E-07	1,3E-06	2,5E-06

ANMERKUNG 1 Diese Tabelle liefert Beispielwerte für PFH_G , berechnet unter Verwendung der Gleichungen aus B.3.2 und den Abhängigkeiten der Annahmen aus B.1. Wenn Sensor-, Logik- oder Stellglied-Teilsystem nur aus einer Gruppe mit Ausgangs-vergleicher oder Mehrheitsentscheider besteht, dann ist PFH_G gleich mit PFH_S , PFH_L bzw. PFH_{FE} (siehe B.3.1 und B.2.1).

ANMERKUNG 2 Diese Tabelle nimmt für $\beta = 2 \times \beta_D$ an. Die Werte für β und β_D für 1oo1- und 2oo2-Architekturen beeinflussen die durchschnittliche Wahrscheinlichkeit eines Ausfalls nicht.

ANMERKUNG 3 Es werden gleiche Raten sicherer wie gefährbringender Ausfälle angenommen, sowie $K = 0,98$.

Tabelle B.11 – Wahrscheinlichkeit eines Ausfalls je Stunde (für die Betriebsart mit hoher oder Anforderungsrate kontinuierlicher Anforderung) für ein Wiederholungsprüfungsintervall von drei Monaten und eine mittlere Zeit zur Wiederherstellung von 8 h

Architektur	DC	$\lambda_D = 0,5E-07$			$\lambda_D = 2,5E-07$			$\lambda_D = 0,5E-06$		
		$\beta = 2 \%$ $\beta_D = 1 \%$	$\beta = 10 \%$ $\beta_D = 5 \%$	$\beta = 20 \%$ $\beta_D = 10 \%$	$\beta = 2 \%$ $\beta_D = 1 \%$	$\beta = 10 \%$ $\beta_D = 5 \%$	$\beta = 20 \%$ $\beta_D = 10 \%$	$\beta = 2 \%$ $\beta_D = 1 \%$	$\beta = 10 \%$ $\beta_D = 5 \%$	$\beta = 20 \%$ $\beta_D = 10 \%$
1oo1 (s. Anm. 2)	0 %	5,0E-08			2,5E-07			5,0E-07		
	60 %	2,0E-08			1,0E-07			2,0E-07		
	90 %	5,0E-09			2,5E-08			5,0E-08		
	99 %	5,0E-10			2,5E-09			5,0E-09		
1oo2	0 %	1,0E-09	5,0E-09	1,0E-08	5,1E-09	2,5E-08	5,0E-08	1,1E-08	5,0E-08	1,0E-07
	60 %	7,0E-10	3,5E-09	7,0E-09	3,6E-09	1,8E-08	3,5E-08	7,2E-09	3,5E-08	7,0E-08
	90 %	5,5E-10	2,8E-09	5,5E-09	2,8E-09	1,4E-08	2,8E-08	5,6E-09	2,8E-08	5,5E-08
	99 %	5,1E-10	2,5E-09	5,1E-09	2,5E-09	1,3E-08	2,5E-08	5,1E-09	2,5E-08	5,1E-08
2oo2 (s. Anm. 2)	0 %	1,0E-07			5,0E-07			1,0E-06		
	60 %	4,0E-08			2,0E-07			4,0E-07		
	90 %	1,0E-08			5,0E-08			1,0E-07		
	99 %	1,0E-09			5,0E-09			1,0E-08		
1oo2D (s. Anm. 3)	0 %	1,0E-09	5,0E-09	1,0E-08	5,1E-09	2,5E-08	5,0E-08	1,1E-08	5,0E-08	1,0E-07
	60 %	1,6E-09	3,2E-09	5,2E-09	8,0E-09	1,6E-08	2,6E-08	1,6E-08	3,2E-08	5,2E-08
	90 %	1,9E-09	2,3E-09	2,8E-09	9,5E-09	1,2E-08	1,4E-08	1,9E-08	2,3E-08	2,8E-08
	99 %	2,0E-09	2,0E-09	2,1E-09	1,0E-08	1,0E-08	1,0E-08	2,0E-08	2,0E-08	2,1E-08
2oo3	0 %	1,0E-09	5,0E-09	1,0E-08	5,4E-09	2,5E-08	5,0E-08	1,2E-08	5,1E-08	1,0E-07
	60 %	7,1E-10	3,5E-09	7,0E-09	3,7E-09	1,8E-08	3,5E-08	7,7E-09	3,6E-08	7,0E-08
	90 %	5,5E-10	2,8E-09	5,5E-09	2,8E-09	1,4E-08	2,8E-08	5,7E-09	2,8E-08	5,5E-08
	99 %	5,1E-10	2,5E-09	5,1E-09	2,5E-09	1,3E-08	2,5E-08	5,1E-09	2,5E-08	5,1E-08
1oo3	0 %	1,0E-09	5,0E-09	1,0E-08	5,0E-09	2,5E-08	5,0E-08	1,0E-08	5,0E-08	1,0E-07
	60 %	7,0E-10	3,5E-09	7,0E-09	3,5E-09	1,8E-08	3,5E-08	7,0E-09	3,5E-08	7,0E-08
	90 %	5,5E-10	2,8E-09	5,5E-09	2,8E-09	1,4E-08	2,8E-08	5,5E-09	2,8E-08	5,5E-08
	99 %	5,1E-10	2,5E-09	5,1E-09	2,5E-09	1,3E-08	2,5E-08	5,1E-09	2,5E-08	5,1E-08

Tabelle B.11 (fortgesetzt)

Architektur	DC	$\lambda_D = 2,5E-06$			$\lambda_D = 0,5E-05$			$\lambda_D = 2,5E-05$		
		$\beta = 2 \%$ $\beta_D = 1 \%$	$\beta = 10 \%$ $\beta_D = 5 \%$	$\beta = 20 \%$ $\beta_D = 10 \%$	$\beta = 2 \%$ $\beta_D = 1 \%$	$\beta = 10 \%$ $\beta_D = 5 \%$	$\beta = 20 \%$ $\beta_D = 10 \%$	$\beta = 2 \%$ $\beta_D = 1 \%$	$\beta = 10 \%$ $\beta_D = 5 \%$	$\beta = 20 \%$ $\beta_D = 10 \%$
1oo1 (s. Anm. 2)	0 %	2,5E-06			5,0E-06			>1E-05		
	60 %	1,0E-06			2,0E-06			1,0E-05		
	90 %	2,5E-07			5,0E-07			2,5E-06		
	99 %	2,5E-08			5,0E-08			2,5E-07		
1oo2	0 %	6,3E-08	2,6E-07	5,1E-07	1,5E-07	5,4E-07	1,0E-06	1,8E-06	3,6E-06	5,9E-06
	60 %	4,0E-08	1,8E-07	3,5E-07	9,2E-08	3,7E-07	7,2E-07	8,9E-07	2,2E-06	3,9E-06
	90 %	2,9E-08	1,4E-07	2,8E-07	6,1E-08	2,8E-07	5,5E-07	4,2E-07	1,5E-06	2,9E-06
	99 %	2,5E-08	1,3E-07	2,5E-07	5,1E-08	2,5E-07	5,1E-07	2,8E-07	1,3E-06	2,5E-06
2oo2 (s. Anm. 2))	0 %	5,0E-06			1,0E-05			>1E-05		
	60 %	2,0E-06			4,0E-06			>1E-05		
	90 %	5,0E-07			1,0E-06			5,0E-06		
	99 %	5,0E-08			1,0E-07			5,0E-07		
1oo2D (s. Anm. 3)	0 %	6,3E-08	2,6E-07	5,1E-07	1,5E-07	5,4E-07	1,0E-06	1,8E-06	3,6E-06	5,9E-06
	60 %	8,2E-08	1,6E-07	2,6E-07	1,7E-07	3,3E-07	5,3E-07	1,0E-06	1,8E-06	2,8E-06
	90 %	9,5E-08	1,2E-07	1,4E-07	1,9E-07	2,3E-07	2,8E-07	9,6E-07	1,2E-06	1,4E-06
	99 %	1,0E-07	1,0E-07	1,0E-07	2,0E-07	2,0E-07	2,1E-07	1,0E-06	1,0E-06	1,0E-06
2oo3	0 %	9,0E-08	2,8E-07	5,3E-07	2,6E-07	6,3E-07	1,1E-06	4,5E-06	5,9E-06	7,6E-06
	60 %	5,1E-08	1,9E-07	3,6E-07	1,4E-07	4,1E-07	7,5E-07	2,0E-06	3,2E-06	4,7E-06
	90 %	3,2E-08	1,4E-07	2,8E-07	7,2E-08	2,9E-07	5,6E-07	7,1E-07	1,8E-06	3,1E-06
	99 %	2,6E-08	1,3E-07	2,5E-07	5,3E-08	2,6E-07	5,1E-07	3,2E-07	1,3E-06	2,6E-06
1oo3	0 %	5,0E-08	2,5E-07	5,0E-07	1,0E-07	5,0E-07	1,0E-06	5,7E-07	2,6E-06	5,0E-06
	60 %	3,5E-08	1,8E-07	3,5E-07	7,0E-08	3,5E-07	7,0E-07	3,6E-07	1,8E-06	3,5E-06
	90 %	2,8E-08	1,4E-07	2,8E-07	5,5E-08	2,8E-07	5,5E-07	2,8E-07	1,4E-06	2,8E-06
	99 %	2,5E-08	1,3E-07	2,5E-07	5,1E-08	2,5E-07	5,1E-07	2,5E-07	1,3E-06	2,5E-06

ANMERKUNG 1 Diese Tabelle liefert Beispielwerte für PFH_G , berechnet unter Verwendung der Gleichungen aus B.3.2 und den Abhängigkeiten der Annahmen aus B.1. Wenn das Sensor-, Logik- oder Stellglied-Teilsystem nur aus einer Gruppe mit Ausgangs-
vergleicher oder Mehrheitsentscheider besteht, dann ist PFH_G gleich mit PFH_S , PFH_L bzw. PFH_{FE} (siehe B.3.1 und B.2.1).

ANMERKUNG 2 Diese Tabelle nimmt für $\beta = 2 \times \beta_D$ an. Die Werte für β und β_D beeinflussen die mittlere Wahrscheinlichkeit eines Ausfalls bei 1oo1- und 2oo2-Architekturen nicht.

ANMERKUNG 3 Es werden gleiche Raten sicherer wie gefährbringender Ausfälle angenommen, sowie $K = 0,98$.