

	DIN EN 61508-2 (VDE 0803-2)	
	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.	
ICS 35.240.50 Ersatz für DIN EN 61508-2 (VDE 0803-2):2002-12 Siehe Anwendungsbeginn Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (IEC 61508-2:2010); Deutsche Fassung EN 61508-2:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems (IEC 61508-2:2010); German version EN 61508-2:2010 Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité (CEI 61508-2:2010); Version allemande EN 61508-2:2010 Gesamtumfang 104 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

Anwendungsbeginn

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

Daneben darf DIN EN 61508-2 (VDE 0803-2):2002-12 noch bis 2013-05-01 angewendet werden.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 61508-2 (VDE 0803-2):2009-06.

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

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

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

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

Änderungen

Gegenüber DIN EN 61508-2 (VDE 0803-2):2002-12 wurden folgende Änderungen vorgenommen:

- a) Um die Anwendbarkeit auf einzelne Geräte und Komponenten zu ermöglichen bzw. zu erleichtern, wurde:
 - die ehemalige „Spezifikation der E/E/PES-Sicherheitsanforderungen“ in den Teil 1, Unterabschnitt 7.10 verschoben und wird dort als „Spezifikation der Anforderungen an die Sicherheit des E/E/PE-Systems“ bezeichnet. In der ersten Phase der Realisierung des Sicherheitslebenszyklus des E/E/PE-Systems entsteht daher nun gemäß Unterabschnitt 7.2 des vorliegenden Teils eine „Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems“;
 - der Begriff „Element“ zur hierarchischen Gliederung eines E/E/PE-Systems unterhalb der Ebene von Teilsystemen eingeführt.
- b) Bestimmung der systematischen Eignung bei Synthese von Elementen nach 7.4.3;
- c) Einführung von Konformitätspfaden in 7.4.2.2, um die Übereinstimmung mit den Anforderungen zur systematischen Sicherheitsintegrität nachzuweisen;
- d) Einführung von Konformitätspfaden in 7.4.4, um die Übereinstimmung mit den Anforderungen der Sicherheitsintegrität der Hardware nachzuweisen, darunter auch der neue Pfad 2_H, basierend auf Bauteilzuverlässigkeitsdaten;
- e) Behandlung der Entwicklung von ASICs (d. h. auch FPGA, PLD, CPLD) für den Einsatz in einem sicherheitsbezogenen System in Analogie zur Entwicklung sicherheitsbezogener Software mit Einführung eines V-Modells für den ASIC-Entwicklungslebenszyklus (siehe Bild 3). Zur Vermeidung von Ausfällen im Rahmen von Entwurf und Entwicklung digitaler ASICs erforderliche Maßnahmen sind im informativen Anhang F aufgeführt. Die Tabellen F.1 und F.2 bilden eine nach Sicherheits-Integritätsleveln abgestufte Auflistung von erforderlichen Verfahren und Maßnahmen;
- f) Anhang D „Sicherheitshandbuch für konforme Objekte“ hinzugefügt, der alle Informationen enthält, die zur Integration eines Gegenstandes in ein sicherheitsbezogenes System erforderlich sind;
- e) Einführung von Regeln, die die Integration von zwei oder mehr Kanälen sowie Überwachungseinrichtungen auf dem Substrat eines digitalen ASICs erlauben, siehe Anhang E.

Frühere Ausgaben

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

Nationaler Anhang NA

(informativ)

Zusammenhang mit Europäischen und Internationalen Normen

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

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

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

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
EN ISO 14224	ISO 14224	DIN EN ISO 14224	–
EN 50205:2002	–	DIN EN 50205 (VDE 0435-2022):2003-01	VDE 0435-2022
EN 60300-3-2	IEC 60300-3-2	DIN EN 60300-3-2	–
EN 60947-5-1:2004 + Cor.:2005 + A1:2009	IEC 60947-5-1:2003 + A1:2009	DIN EN 60947-5-1 (VDE 0660-200):2010-04	VDE 0660-200
EN 60601 (alle Teile)	IEC 60601 (alle Teile)	DIN EN 60601 (VDE 0750-1) (alle Teile)	VDE 0750-1
EN 61000-6-2	IEC 61000-6-2	DIN EN 61000-6-2 (VDE 0839-6-2)	VDE 0839-6-2
EN 61078	IEC 61078	DIN EN 61078	–
EN 61164	IEC 61164	DIN EN 61164	–
EN 61165	IEC 61165	DIN EN 61165	–
EN 61326-3-1:2008	IEC 61326-3-1:2008	DIN EN 61326-3-1 Berichtigung 1 (VDE 0843-20-3-1 Berichtigung 1) :2009-04	VDE 0843-20-3-1 Berichtigung 1
EN 61508-1:2010	IEC 61508-1:2010	DIN EN 61508-1 (VDE 0803-1):2011-02	VDE 0803-1
EN 61508-3:2010	IEC 61508-3:2010	DIN EN 61508-3 (VDE 0803-3):2011-02	VDE 0803-3
EN 61508-4:2010	IEC 61508-4:2010	DIN EN 61508-4 (VDE 0803-4):2011-02	VDE 0803-4
EN 61508-5:2010	IEC 61508-5:2010	DIN EN 61508-5 (VDE 0803-5):2011-02	VDE 0803-5

Tabelle NA.1 (fortgesetzt)

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
EN 61508-6:2010	IEC 61508-6:2010	DIN EN 61508-6 (VDE 0803-6):2011-02	VDE 0803-6
EN 61508-7:2010	IEC 61508-7:2010	DIN EN 61508-7 (VDE 0803-7):2011-02	VDE 0803-7
EN 61511 (alle Teile)	IEC 61511 (alle Teile)	DIN EN 61511 (VDE 0810-1) (alle Teile)	VDE 0810-1
EN 61784-3:2010	IEC 61784-3:2010	DIN EN 61784-3 (VDE 0803-500):2011-02	VDE 0803-500
EN 61800-5-2	IEC 61800-5-2	DIN EN 61800-5-2 (VDE 0160-105-2)	VDE 0160-105-2
EN 62061	IEC 62061	DIN EN 62061 (VDE 0113-50)	VDE 0113-50
–	IEC 62280-1:2002	–	–
–	IEC 62280-2:2002	–	–
EN 62308	IEC 62308	DIN EN 62308	–
–	IEC 60050-191 ^{*)}	–	–
–	IEC Guide 104:1997	–	–
–	ISO/IEC Guide 51 :1999	–	–
–	IEEE 352:1987	–	–
EN ISO 9000	ISO 9000	DIN EN ISO 9000	–
–	IEC/TS 61000-1-2 :2008	–	–

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN ISO 14224, *Erdöl-, petrochemische und Erdgasindustrie – Sammlung und Austausch von Zuverlässigkeits- und Wartungsdaten für Ausrüstungen*

DIN EN 50205 (VDE 0435-2022):2003-01, *Relais mit (mechanisch) zwangsgeführten Kontakten; Deutsche Fassung EN 50205:2002*

DIN EN 60300-3-2, *Zuverlässigkeitsmanagement – Teil 3-2: Anwendungsleitfaden – Erfassung von Zuverlässigkeitsdaten im Betrieb*

DIN EN 60947-5-1 (VDE 0660-200):2010-04, *Niederspannungsschaltgeräte – Teil 5-1: Steuergeräte und Schaltelemente – Elektromechanische Steuergeräte (IEC 60947-5-1:2003 + A1:2009); Deutsche Fassung EN 60947-5-1:2004 + Cor.:2005 + A1:2009*

DIN EN 60601 (VDE 0750-1) (alle Teile), *Medizinische elektrische Geräte*

^{*)} „Internationales Elektrotechnisches Wörterbuch – Deutsche Ausgabe“, Online-Zugang: <http://www.dke.de/dke-iev>.

DIN EN 61000-6-2 (VDE 0839-6-2), *Elektromagnetische Verträglichkeit (EMV) – Teil 6-2: Fachgrundnormen – Störfestigkeit für Industriebereiche*

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

DIN EN 61164, *Zuverlässigkeitswachstum – Statistische Prüf- und Schätzverfahren*

DIN EN 61165, *Anwendung des Markoff-Verfahrens*

DIN EN 61326-3-1 Berichtigung 1 (VDE 0843-20-3-1 Berichtigung 1):2009-04, *Elektrische Mess-, Steuer-, Regel- und Laborgeräte – EMV-Anforderungen – Teil 3-1: Störfestigkeitsanforderungen für sicherheitsbezogene Systeme und für Geräte, die für sicherheitsbezogene Funktionen vorgesehen sind (Funktionale Sicherheit) – Allgemeine industrielle Anwendungen (IEC 61326-3-1:2008); Deutsche Fassung EN 61326-3-1:2008, Berichtigung zu DIN EN 61326-3-1 (VDE 0843-20-3-1):2008-11*

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

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

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

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

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

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

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

DIN EN 61784-3 (VDE 0803-500):2011-02, *Industrielle Kommunikationsnetze – Profile – Teil 3: Funktional sichere Übertragung bei Feldbussen – Allgemeine Regeln und Profilstellungen (IEC 61784-3:2010); Deutsche Fassung EN 61784-3:2010*

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

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

DIN EN 62308, *Zuverlässigkeit von Geräten – Verfahren zur Zuverlässigkeitsbewertung*

DIN EN ISO 9000, *Qualitätsmanagementsysteme – Grundlagen und Begriffe*

– Leerseite –

Funktionale Sicherheit sicherheitsbezogener
elektrischer/elektronischer/programmierbarer elektronischer Systeme –
Teil 2: Anforderungen an sicherheitsbezogene
elektrische/elektronische/programmierbare elektronische Systeme
(IEC 61508-2:2010)

Functional safety of
electrical/electronic/programmable electronic
safety-related systems –
Part 2: Requirements for
electrical/electronic/programmable electronic
safety-related systems
(IEC 61508-2:2010)

Sécurité fonctionnelle des systèmes
électriques/électroniques/électroniques
programmables relatifs à la sécurité –
Partie 2: Exigences pour les systèmes
électriques/électroniques/électroniques
programmables relatifs à la sécurité
(CEI 61508-2:2010)

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

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

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

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

CENELEC

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

Zentralsekretariat: Avenue Marnix 17, B-1000 Brüssel

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

Ref. Nr. EN 61508-2:2010 D

Vorwort

Der Text des Schriftstücks 65A/549/FDIS, zukünftige 2. Ausgabe von IEC 61508-2, ausgearbeitet von dem SC 65A „System aspects“ des IEC/TC 65 „Industrial-process measurement, control and automation“, wurde der IEC-CENELEC Parallelen Abstimmung unterworfen und von CENELEC am 2010-05-01 als EN 61508-2 angenommen.

Diese Europäische Norm ersetzt EN 61508-2:2001.

Sie ist eine Sicherheits-Grundnorm nach IEC-Guide 104.

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

Nachstehende Daten wurden festgelegt:

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

Der Anhang ZA wurde von CENELEC hinzugefügt.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 61508-2:2010 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

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

[1] IEC 61511 Reihe	ANMERKUNG	Harmonisiert in der Reihe EN 61511 (nicht modifiziert).
[2] IEC 62061	ANMERKUNG	Harmonisiert als EN 62061.
[3] IEC 61800-5-2	ANMERKUNG	Harmonisiert als EN 61800-5-2.
[4] IEC 61508-5:2010	ANMERKUNG	Harmonisiert als EN 61508-5:2010 (nicht modifiziert).
[5] IEC 61508-6:2010	ANMERKUNG	Harmonisiert als EN 61508-6:2010 (nicht modifiziert).
[6] IEC 60601 Reihe	ANMERKUNG	Harmonisiert in der Reihe EN 60601 (teilweise modifiziert).
[7] IEC 61165	ANMERKUNG	Harmonisiert als EN 61165.
[8] IEC 61078	ANMERKUNG	Harmonisiert als EN 61078.
[9] IEC 61164	ANMERKUNG	Harmonisiert als EN 61164.
[10] IEC 62308	ANMERKUNG	Harmonisiert als EN 62308.
[11] IEC 61000-6-2	ANMERKUNG	Harmonisiert als EN 61000-6-2.
[12] ISO 14224	ANMERKUNG	Harmonisiert als EN ISO 14224.
[14] ISO 9000	ANMERKUNG	Harmonisiert als EN ISO 9000.
[15] IEC 60300-3-2	ANMERKUNG	Harmonisiert als EN 60300-3-2.

Inhalt

	Seite
Vorwort.....	2
Einleitung	6
1 Anwendungsbereich	8
2 Normative Verweisungen	11
3 Begriffe und Abkürzungen	11
4 Übereinstimmung mit dieser Norm	11
5 Dokumentation	11
6 Management der funktionalen Sicherheit	12
7 Anforderungen des Sicherheitslebenszyklus des E/E/PE-Systems	12
7.1 Allgemeines	12
7.2 Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems	16
7.3 Planung der Validierung der Sicherheit des E/E/PE-Systems	19
7.4 Entwurf und Entwicklung des E/E/PE-Systems	19
7.5 Integration des E/E/PE-Systems	41
7.6 Betriebs- und Instandhaltungsverfahren für das E/E/PE-System	42
7.7 Validierung der Sicherheit des E/E/PE-Systems	44
7.8 Modifikation des E/E/PE-Systems	45
7.9 Verifikation des E/E/PE-Systems	46
8 Beurteilung der funktionalen Sicherheit	47
Anhang A (normativ) Verfahren und Maßnahmen für sicherheitsbezogene E/E/PE-Systeme – Beherrschung von Ausfällen während des Betriebs	48
A.1 Allgemeines	48
A.2 Sicherheitsintegrität der Hardware	49
A.3 Systematische Sicherheitsintegrität	61
Anhang B (normativ) Verfahren und Maßnahmen für sicherheitsbezogene E/E/PE-Systeme – Vermeidung von systematischen Ausfällen während der verschiedenen Phasen des Lebenszyklus	66
Anhang C (normativ) Diagnosedeckungsgrad und Anteil sicherer Ausfälle	75
C.1 Berechnung des Diagnosedeckungsgrads und des Anteils sicherer Ausfälle eines Hardwareelements	75
C.2 Bestimmung von Diagnosedeckungsfaktoren	76
Anhang D (normativ) Sicherheitshandbuch für konforme Objekte	78
D.1 Allgemeines	78
D.2 Inhalte	78
Anhang E (normativ) Besondere Architektur Anforderungen an integrierte Schaltkreise (ICs) mit On- Chip-Redundanz	80
E.1 Allgemeines	80
E.2 Zusätzliche Anforderungen an On-Chip-Redundanz bei SIL 3	83

	Seite
E.3 β -Faktor.....	83
Anhang F (informativ) Verfahren und Maßnahmen für ASICs – Vermeidung von systematischen Ausfällen	86
F.1 Allgemeines	86
F.2 Hinweise: Verfahren und Maßnahmen	87
Literaturhinweise	95
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen.....	97
Bilder	
Bild 1 – Gesamtrahmen der Normenreihe IEC 61508	10
Bild 2 – Sicherheitslebenszyklus des E/E/PE-Systems (in der Realisierungsphase).....	13
Bild 3 – ASIC-Entwicklungslebenszyklus (V-Modell)	14
Bild 4 – Beziehung zwischen und Anwendungsbereich von IEC 61508-2 und IEC 61508-3.....	14
Bild 5 – Bestimmung des maximalen SIL für eine festgelegte Architektur (sicherheitsbezogenes E/E/PE-Teilsystem, das aus einer Anzahl hintereinandergeschalteter Elemente besteht, siehe 7.4.4.2.3)	28
Bild 6 – Bestimmung des maximalen SIL für eine festgelegte Architektur (sicherheitsbezogenes E/E/PE-Teilsystem, das aus zwei Teilsystemen X und Y besteht, siehe 7.4.4.2.4).....	30
Bild 7 – Architekturen für Datenkommunikation.....	41
Tabellen	
Tabelle 1 – Überblick – Realisierungsphase des Sicherheitslebenszyklus des E/E/PE-Systems	15
Tabelle 2 – Maximal zulässiger Sicherheits-Integritätslevel für eine Sicherheitsfunktion, die von einem sicherheitsbezogenen Typ A-Element oder Teilsystem ausgeführt wird.....	26
Tabelle 3 – Maximal zulässiger Sicherheits-Integritätslevel für eine Sicherheitsfunktion, die von einem sicherheitsbezogenen Typ B-Element oder Teilsystem ausgeführt wird.....	27
Tabelle A.1 – Fehler oder Ausfälle, die bei der Quantifizierung der Auswirkungen zufälliger Hardwareausfälle angenommen werden müssen oder bei der Bestimmung des Anteils sicherer Ausfälle berücksichtigt werden müssen.....	49
Tabelle A.2 – Elektrische Bauteile	52
Tabelle A.3 – Elektronische Bauteile	53
Tabelle A.4 – Verarbeitungseinheiten.....	54
Tabelle A.5 – Unveränderliche Speicherbereiche.....	55
Tabelle A.6 – Veränderliche Speicherbereiche.....	56
Tabelle A.7 – E/A-Einheiten und Schnittstellen (externe Kommunikation).....	57
Tabelle A.8 – Datenwege (interne Kommunikation)	57
Tabelle A.9 – Energieversorgung	58
Tabelle A.10 – Programmablauf (Watchdog).....	58
Tabelle A.11 – Takt	59
Tabelle A.12 – Kommunikation und Massenspeicher.....	59
Tabelle A.13 – Sensoren.....	60
Tabelle A.14 – Stellglieder (Aktoren)	60

Tabelle A.15 – Verfahren und Maßnahmen zur Beherrschung von durch den Hardwareentwurf verursachten systematischen Ausfällen	62
Tabelle A.16 – Verfahren und Maßnahmen zur Beherrschung von durch umgebungsbedingte Beanspruchung oder Einflüsse verursachten systematischen Ausfällen.....	62
Tabelle A.17 – Verfahren und Maßnahmen zur Beherrschung von systematischen Ausfällen während des Betriebs.....	64
Tabelle A.18 – Wirksamkeit von Verfahren und Maßnahmen zur Beherrschung von systematischen Ausfällen.....	64
Tabelle B.1 – Verfahren und Maßnahmen zur Vermeidung von Irrtümern während der Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems (siehe 7.2).....	67
Tabelle B.2 – Verfahren und Maßnahmen zur Vermeidung von Fehlern während Entwurf und Entwicklung des E/E/PE-Systems (siehe 7.4).....	68
Tabelle B.3 – Verfahren und Maßnahmen zur Vermeidung von Fehlern während der Integration des E/E/PE-Systems (siehe 7.5).....	69
Tabelle B.4 – Verfahren und Maßnahmen zur Vermeidung von Fehlern und Ausfällen während der Betriebs- und Instandhaltungsverfahren für das E/E/PE-System (siehe 7.6)	70
Tabelle B.5 – Verfahren und Maßnahmen zur Vermeidung von Fehlern während der Validierung der Sicherheit des E/E/PE-Systems (siehe 7.7)	70
Tabelle B.6 – Wirksamkeit von Verfahren und Maßnahmen zur Vermeidung von systematischen Ausfällen.....	72

Einleitung

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

Diese Internationale Norm beschreibt einen allgemeinen Lösungsweg für alle Tätigkeiten während des Sicherheitslebenszyklus für Systeme, die aus elektrischen und/oder elektronischen und/oder programmierbaren elektronischen (E/E/PE) Elementen bestehen und die eingesetzt werden, um Sicherheitsfunktionen auszuführen. Dieser allgemeine Lösungsweg wurde gewählt, um ein sinnvolles und konsistentes technisches Verfahren für alle elektrischen Sicherheitssysteme zu entwickeln. Ein Hauptziel ist es, die Entwicklung von produkt- und anwendungsspezifischen internationalen Normen, die auf der Normenreihe IEC 61508 basieren, zu erleichtern.

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

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

Es ist beachtet worden, dass eine große Vielfalt von Anwendungen in vielfältigen Anwendungsbereichen vorliegt, die sicherheitsbezogene E/E/PE-Systeme verwenden, und diese einen weiten Bereich in Bezug auf Komplexität, Gefährdungs- und Risikopotentiale abdecken. In jeder speziellen Anwendung sind die erforderlichen Sicherheitsmaßnahmen von vielen anwendungsspezifischen Faktoren abhängig. Dadurch, dass diese Internationale Norm allgemein gehalten ist, wird die Formulierung solcher Maßnahmen in zukünftigen produkt- und anwendungsspezifischen internationalen Normen und in Überarbeitungen der bereits bestehenden Normen ermöglicht.

Diese Internationale Norm:

- betrachtet alle relevanten Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus (zum Beispiel vom anfänglichen Konzept über Entwurf, Implementierung, Betrieb und Instandhaltung bis zur Außerbetriebnahme), wenn E/E/PE-Systeme benutzt werden, um Sicherheitsfunktionen auszuführen;
- wurde unter Berücksichtigung einer sich schnell entwickelnden Technologie entworfen. Der Betrachtungsrahmen ist ausreichend robust und ausführlich genug, um auch für zukünftige Entwicklungen verwendbar zu sein;
- ermöglicht die Erstellung produkt- und anwendungsspezifischer Internationaler Normen, die sich mit sicherheitsbezogenen E/E/PE-Systemen befassen. Die Entwicklung produkt- und anwendungsspezifischer Internationaler Normen sollte innerhalb des Rahmens dieser Norm zu einem hohen Grad an Übereinstimmung (zum Beispiel von zugrunde liegenden Prinzipien, Terminologie usw.) führen sowohl innerhalb der Anwendungsbereiche als auch über die Anwendungsbereiche hinweg. Dies hat sowohl sicherheitstechnische als auch wirtschaftliche Vorteile;
- liefert eine Methode für die Entwicklung der Spezifikation der Anforderungen an die Sicherheit, die notwendig ist, um die erforderliche funktionale Sicherheit für sicherheitsbezogene E/E/PE-Systeme zu erreichen;
- verwendet einen auf dem Risiko basierenden Lösungsansatz, durch den die Anforderungen an die Sicherheitsintegrität bestimmt werden können;

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

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

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

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

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

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

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme

1 Anwendungsbereich

1.1 Dieser Teil der Normenreihe IEC 61508:

- a) ist dazu vorgesehen, nur nach einem gründlichen Verständnis der IEC 61508-1 angewendet zu werden, die den Gesamtrahmen für das Erreichen der funktionalen Sicherheit bereitstellt;
- b) ist für jedes sicherheitsbezogene System, wie durch IEC 61508-1 definiert, anwendbar, das mindestens ein elektrisches, elektronisches oder programmierbares elektronisches Element enthält;
- c) ist auf alle Elemente innerhalb eines sicherheitsbezogenen E/E/PE-Systems anwendbar (einschließlich Sensoren, Aktoren und die Bedienerschnittstelle);
- d) legt fest, wie die in Übereinstimmung mit IEC 61508-1 entwickelte Spezifikation der Anforderungen an die Sicherheit des E/E/PE-Systems (welche die Spezifikation der Anforderungen an die Sicherheitsfunktionen des E/E/PE-Systems und die Spezifikation der Anforderungen an die Sicherheitsintegrität des E/E/PE-Systems einschließt) in die Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems verfeinert wird;
- e) legt die Anforderungen für Tätigkeiten fest, die während des Entwurfs und der Herstellung der sicherheitsbezogenen E/E/PE-Systeme anzuwenden sind (d. h. legt das Modell des Sicherheitslebenszyklus des E/E/PE-Systems fest), außer für Software, die in IEC 61508-3 behandelt wird (siehe [Bilder 2 bis 4](#)). Diese Anforderungen schließen die Anwendung von Verfahren und Maßnahmen zur Vermeidung und Beherrschung von Fehlern und Ausfällen ein, die dem Sicherheits-Integritätslevel entsprechend abgestuft sind;
- f) legt die notwendigen Informationen zur Ausführung der Installation, Inbetriebnahme und der abschließenden Validierung der Sicherheit der sicherheitsbezogenen E/E/PE-Systeme fest;
- g) gilt nicht für die Betriebs- und Instandhaltungsphase der sicherheitsbezogenen E/E/PE-Systeme – diese wird in IEC 61508-1 behandelt – jedoch stellt die IEC 61508-2 Anforderungen für die Vorbereitung von Informationen und Verfahren bereit, die vom Anwender für den Betrieb und die Instandhaltung der sicherheitsbezogenen E/E/PE-Systeme benötigt werden;
- h) legt Anforderungen fest, die durch die Organisation zu erfüllen sind, die irgendeine Modifikation der sicherheitsbezogenen E/E/PE-Systeme ausführt;

ANMERKUNG 1 Dieser Teil der IEC 61508 ist hauptsächlich an Lieferanten und/oder an firmeneigene Konstruktionsabteilungen gerichtet, deswegen sind Anforderungen zur Modifikation eingeschlossen.

ANMERKUNG 2 [Bild 4](#) zeigt die Beziehung zwischen der IEC 61508-2 und der IEC 61508-3.

- i) trifft nicht auf medizinische Einrichtungen gemäß der Normenreihe IEC 60601 zu.

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

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

ANMERKUNG Die funktionale Sicherheit eines sicherheitsbezogenen E/E/PE-Systems kann nur erreicht werden, wenn alle zutreffenden Anforderungen erfüllt werden. Daher ist es wichtig, dass alle zutreffenden Anforderungen sorgfältig betrachtet und angemessen in Bezug genommen werden.

1.4 [Bild 1](#) zeigt den Gesamtrahmen für die Normenreihe IEC 61508 und zeigt die Rolle, welche die IEC 61508-2 beim Erreichen der funktionalen Sicherheit für sicherheitsbezogene E/E/PE-Systeme spielt. IEC 61508-6, Anhang A beschreibt die Anwendung der IEC 61508-2 und der IEC 61508-3.

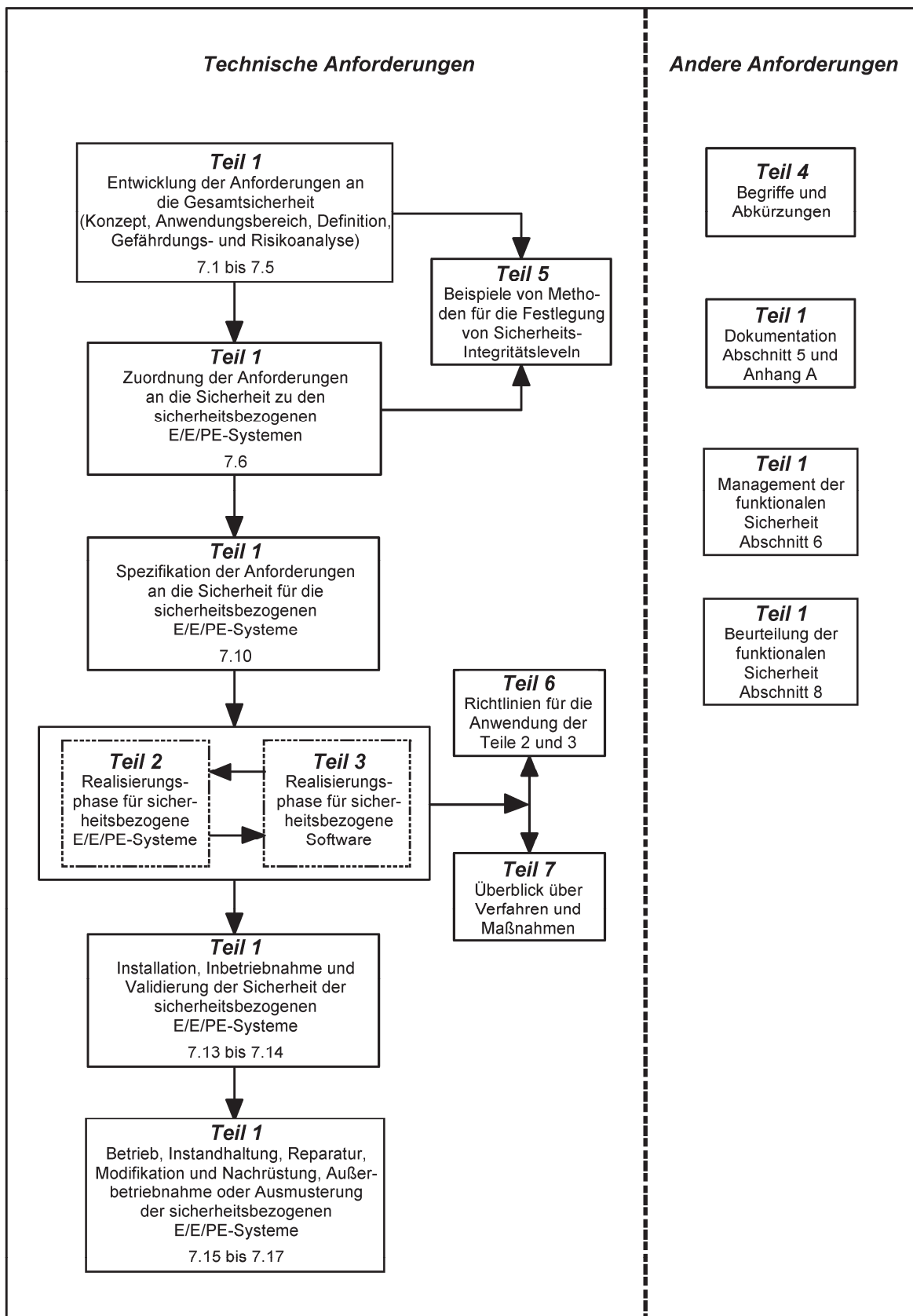


Bild 1 – Gesamttrahmen der Normenreihe IEC 61508

2 Normative Verweisungen

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

IEC 60947-5-1, *Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices*

IEC/TS 61000-1-2, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena*

IEC 61326-3-1, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – General industrial applications*

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

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

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

IEC 61508-7:2010, *Functional safety of electrical/electronic/programmable electronic safety related systems – Part 7: Overview of techniques and measures*

IEC 61784-3, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 62280-1, *Railway applications – Communication, signalling and processing systems – Part 1: Safety-related communication in closed transmission systems*

IEC 62280-2, *Railway applications – Communication, signalling and processing systems – Part 2: Safety-related communication in open transmission systems*

IEC Guide 104:1997, *The preparation of safety publications and the use of basic safety publications and group safety publications*

ISO/IEC Guide 51:1999, *Safety aspects – Guidelines for their inclusion in standards*

EN 50205, *Relays with forcibly guided (mechanically linked) contacts*

3 Begriffe und Abkürzungen

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

4 Übereinstimmung mit dieser Norm

Die Anforderungen zur Übereinstimmung mit dieser Norm sind in IEC 61508-1, Abschnitt 4 ausführlich beschrieben.

5 Dokumentation

Die Anforderungen zur Dokumentation sind in IEC 61508-1, Abschnitt 5 ausführlich beschrieben.

6 Management der funktionalen Sicherheit

Die Anforderungen für das Management der funktionalen Sicherheit sind in IEC 61508-1, Abschnitt 6 ausführlich beschrieben.

7 Anforderungen des Sicherheitslebenszyklus des E/E/PE-Systems

7.1 Allgemeines

7.1.1 Ziele und Anforderungen – Allgemeines

7.1.1.1 Dieser Unterabschnitt enthält die Ziele und Anforderungen für die Phasen des Sicherheitslebenszyklus des E/E/PE-Systems.

ANMERKUNG Die Ziele und Anforderungen für den Gesamt-Sicherheitslebenszyklus werden zusammen mit einer allgemeinen Einführung in die Struktur der Norm in IEC 61508-1 angegeben.

7.1.1.2 Für alle Phasen des Sicherheitslebenszyklus des E/E/PE-Systems zeigt [Tabelle 1](#):

- die zu erreichenden Ziele;
- den Anwendungsbereich der Phase;
- einen Bezug zum Unterabschnitt, der die Anforderungen enthält;
- die erforderlichen Eingaben für die Phase;
- die erforderlichen Ergebnisse (Ausgaben), um mit dem Unterabschnitt übereinzustimmen.

7.1.2 Ziele

7.1.2.1 Das erste Ziel der Anforderungen dieses Unterabschnittes ist es, die Phasen in dem Sicherheitslebenszyklus des E/E/PE-Systems, die betrachtet werden müssen, in einer systematischen Art zu strukturieren, um die erforderliche funktionale Sicherheit der sicherheitsbezogenen E/E/PE-Systeme zu erreichen.

7.1.2.2 Das zweite Ziel der Anforderungen dieses Unterabschnittes ist es, alle Informationen, die für die funktionale Sicherheit der sicherheitsbezogenen E/E/PE-Systeme relevant sind, während des Sicherheitslebenszyklus des E/E/PE-Systems zu dokumentieren.

7.1.3 Anforderungen

7.1.3.1 Der Sicherheitslebenszyklus des E/E/PE-Systems, der für die Übereinstimmung mit dieser Norm verwendet werden muss, ist der in [Bild 2](#) festgelegte. [Bild 3](#) zeigt ein detailliertes V-Modell des ASIC-Entwicklungslebenszyklus für den Entwurf von ASICs (siehe IEC 61508-4, 3.2.15). Falls ein anderer Sicherheitslebenszyklus des E/E/PE-Systems oder des ASIC-Entwicklungslebenszyklus verwendet wird, muss dieser als Teil der Tätigkeiten des Managements der funktionalen Sicherheit (siehe IEC 61508-1, Abschnitt 6) festgelegt werden, und alle Ziele und Anforderungen jedes Unterabschnitts der IEC 61508-2 müssen erfüllt werden.

ANMERKUNG 1 [Bild 4](#) zeigt die Beziehung zwischen IEC 61508-2 und IEC 61508-3 und den Anwendungsbereich dieser Normen.

ANMERKUNG 2 Es gibt bedeutende Ähnlichkeiten zwischen den Entwurfsprozessen für ASICs und für Software. IEC 61508-3 empfiehlt das V-Modell für den Entwurf von sicherheitsbezogener Software. Das V-Modell erfordert zur Vermeidung und Beherrschung systematischer Fehler einen klar strukturierten Entwurfsprozess und eine modulare Softwarestruktur. Der ASIC-Entwicklungslebenszyklus für den Entwurf von ASICs in [Bild 3](#) folgt diesem Modell. Zunächst werden die Anforderungen für die ASIC-Spezifikation von den Systemanforderungen abgeleitet, ASIC-Architektur, ASIC-Entwurf und Modulentwurf folgen. Die Ergebnisse jeder Stufe auf der linken Seite des V werden Eingabe zur nächsten Stufe und werden weiterhin, wo erforderlich, auf die vorherige Stufe zur Iteration zurückgekoppelt, bis der endgültige Code erzeugt wird. Dieser Code wird gegen den entsprechenden Entwurf durch Post-Layout-Simulation, Modultest, Modulintegrationstest und Verifikation des gesamten ASIC verifiziert. Die Ergebnisse irgendeiner Stufe können eine Überar-

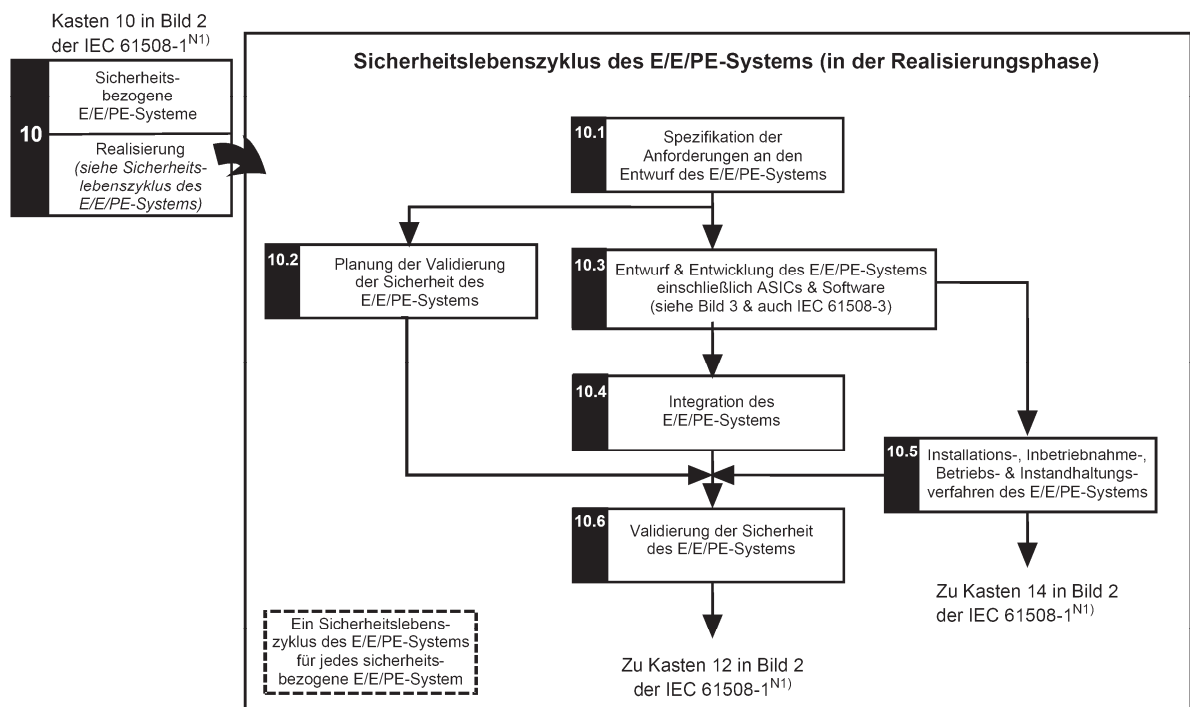
beutung irgendeiner der vorherigen Stufen erfordern. Zum Schluss wird der ASIC nach seiner Integration in das sicherheitsbezogene E/E/PE-System validiert.

7.1.3.2 Die Verfahren für das Management der funktionalen Sicherheit (siehe IEC 61508-1, Abschnitt 6) müssen parallel mit den Phasen des Sicherheitslebenszyklus des E/E/PE-Systems laufen.

7.1.3.3 Jede Phase des Sicherheitslebenszyklus des E/E/PE-Systems muss in elementare Tätigkeiten unterteilt werden mit dem Anwendungsbereich, den Eingaben und den Ergebnissen (Ausgaben) für jede Phase (siehe [Tabelle 1](#)).

7.1.3.4 Außer wenn als Teil der Tätigkeiten des Managements der funktionalen Sicherheit (siehe IEC 61508-1, Abschnitt 6) begründet, müssen die Ergebnisse jeder Phase des Sicherheitslebenszyklus des E/E/PE-Systems dokumentiert werden (siehe IEC 61508-1, Abschnitt 5).

7.1.3.5 Die Ergebnisse für jede Phase des Sicherheitslebenszyklus des E/E/PE-Systems müssen die Ziele und Anforderungen erfüllen, die für jede Phase festgelegt sind (siehe [7.2 bis 7.9](#)).



ANMERKUNG 1 Siehe auch IEC 61508-6, A.2 b).

ANMERKUNG 2 Dieses Bild zeigt nur jene Phasen des Sicherheitslebenszyklus des E/E/PE-Systems, die innerhalb der Realisierungsphase des Gesamt-Sicherheitslebenszyklus liegen. Der vollständige Sicherheitslebenszyklus des E/E/PE-Systems wird auch Aspekte der nachfolgenden Phasen des Gesamt-Sicherheitslebenszyklus (Kästen 12 bis 16 in Bild 2 von IEC 61508-1) enthalten, die spezifisch für das sicherheitsbezogene E/E/PE-System sind.

Bild 2 – Sicherheitslebenszyklus des E/E/PE-Systems (in der Realisierungsphase)

^{N1)} Nationale Fußnote: In der IEC 61508-2:2010 fehlt der Verweis auf IEC 61508-1.

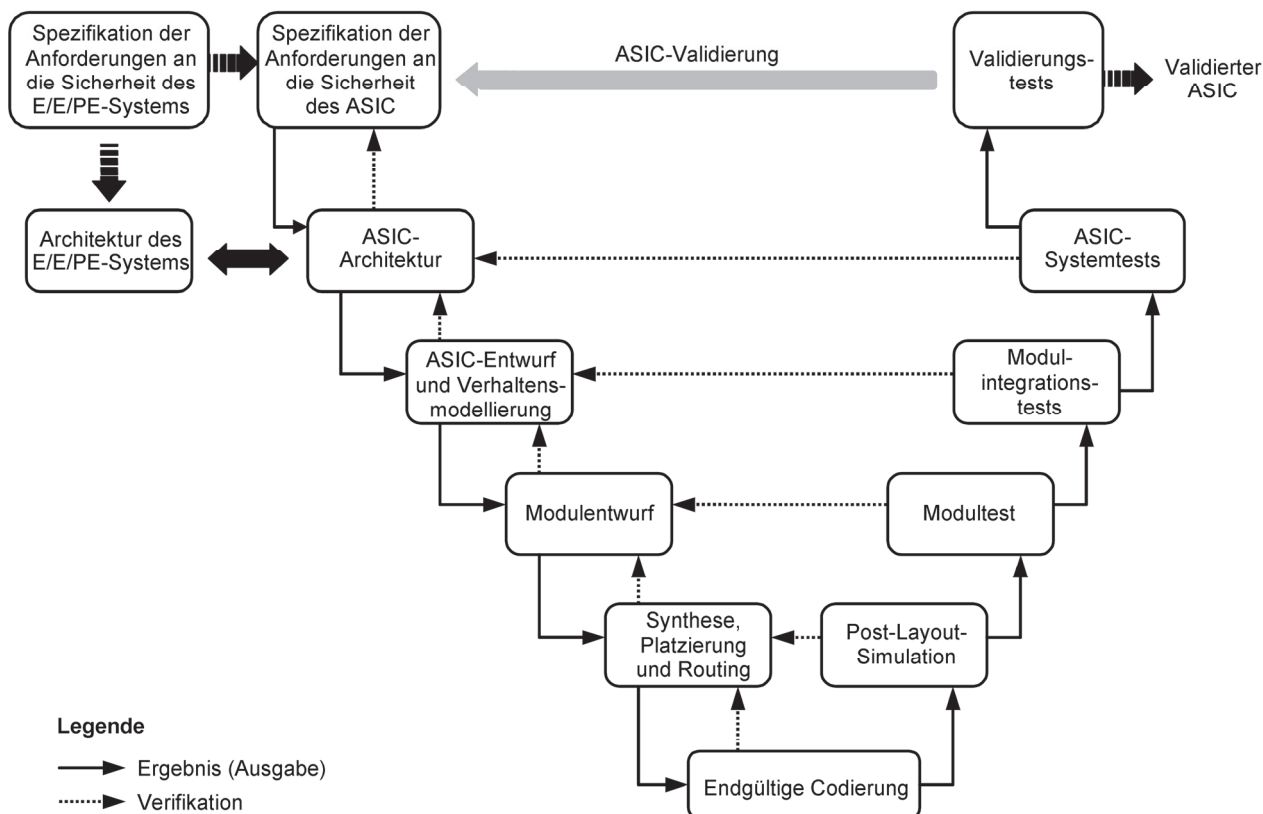


Bild 3 – ASIC-Entwicklungslebenszyklus (V-Modell)

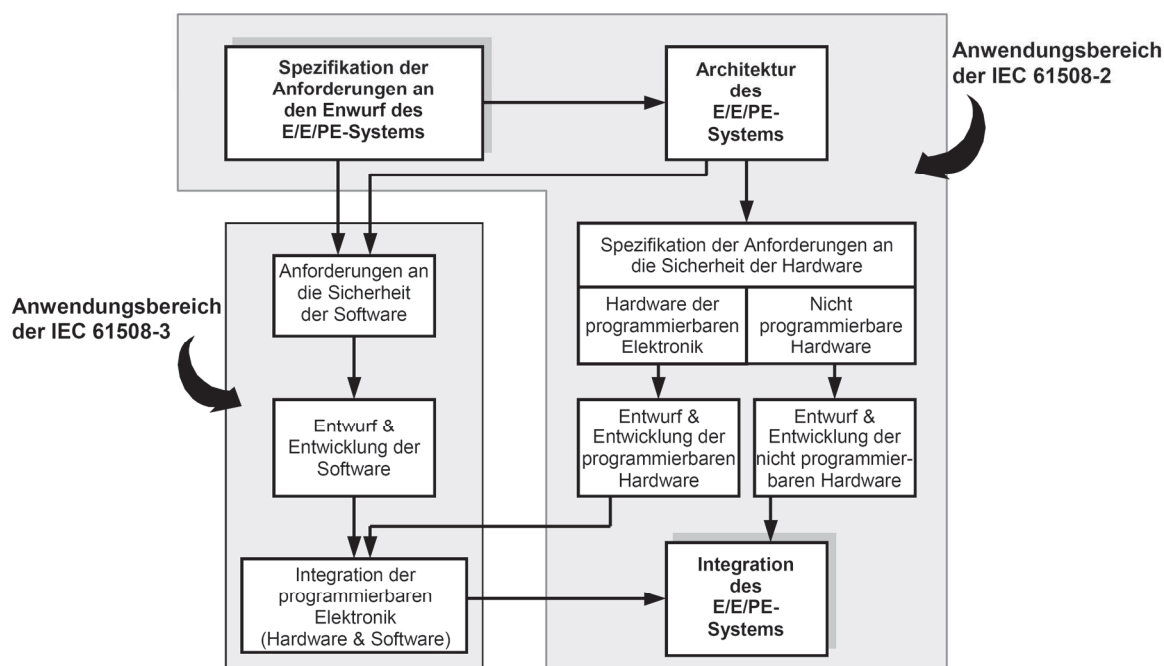


Bild 4 – Beziehung zwischen und Anwendungsbereich von IEC 61508-2 und IEC 61508-3

Tabelle 1 – Überblick – Realisierungsphase des Sicherheitslebenszyklus des E/E/PE-Systems

Phase des Sicherheitslebenszyklus		Ziele	Anwendungsbereich	Unterabschnitt mit den Anforderungen	Eingaben	Ergebnisse (Ausgaben)
Kastennummer in Bild 2	Titel					
10.1	Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems	Für jedes sicherheitsbezogene E/E/PE-System die Anforderungen an den Entwurf in Form von Teilsystemen und Elementen festlegen (siehe IEC 61508-1, 7.10.2).	Sicherheitsbezogenes E/E/PE-System	7.2.2	Spezifikation der Anforderungen an die Sicherheit des E/E/PE-Systems (siehe IEC 61508-1, 7.10)	Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems, welche die Betriebsmittel und Architekturen für das E/E/PE-System beschreibt
10.2	Planung der Validierung der Sicherheit des E/E/PE-Systems	Die Validierung der Sicherheit des sicherheitsbezogenen E/E/PE-Systems planen.	Sicherheitsbezogenes E/E/PE-System	7.3.2	Spezifikation der Anforderungen an die Sicherheit des E/E/PE-Systems und Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems	Plan für die Validierung der Sicherheit der sicherheitsbezogenen E/E/PE-Systeme
10.3	Entwurf und Entwicklung des E/E/PE-Systems einschließlich ASICs und Software (siehe Bild 3 und auch IEC 61508-3)	Das sicherheitsbezogene E/E/PE-System (einschließlich ASICs, wenn zutreffend) entwerfen und entwickeln, um die Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems (im Hinblick auf die Anforderungen an die Sicherheitsfunktionen und die Anforderungen an die Sicherheitsintegrität (siehe 7.2)) zu erfüllen.	Sicherheitsbezogenes E/E/PE-System	7.4.2 bis 7.4.11	Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems	Entwurf der sicherheitsbezogenen E/E/PE-Systeme in Übereinstimmung mit der Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems Plan für den Integrationstest des E/E/PE-Systems Informationen zur Architektur des PE-Systems als Eingabe für die Spezifikation der Anforderungen an die Software
10.4	Integration des E/E/PE-Systems	Das sicherheitsbezogene E/E/PE-System integrieren und testen.	Sicherheitsbezogenes E/E/PE-System	7.5.2	Entwurf des E/E/PE-Systems Plan der Integrationstests des E/E/PE-Systems Hardware und Software der programmierbaren Elektronik	Vollständig funktionierende sicherheitsbezogene E/E/PE-Systeme in Übereinstimmung mit dem Entwurf des E/E/PE-Systems Ergebnisse der Integrationstests des E/E/PE-Systems
10.5	Installations-, Inbetriebnahme-, Betriebs- und Instandhaltungsverfahren des E/E/PE-Systems	Verfahren entwickeln, um sicherzustellen, dass die erforderliche funktionale Sicherheit des sicherheitsbezogenen E/E/PE-Systems während des Betriebs und der Instandhaltung aufrechterhalten wird.	Sicherheitsbezogenes E/E/PE-System EUC	7.6.2	Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems Entwurf des E/E/PE-Systems	Installations-, Inbetriebnahme-, Betriebs- und Instandhaltungsverfahren des E/E/PE-Systems für jedes einzelne E/E/PE-System

Tabelle 1 (fortgesetzt)

Phase des Sicherheitslebenszyklus		Ziele	Anwendungsbereich	Unterabschnitt mit den Anforderungen	Eingaben	Ergebnisse (Ausgaben)
Kastennummer in Bild 2	Titel					
10.6	Validierung der Sicherheit des E/E/PE-Systems	Validieren, dass das sicherheitsbezogene E/E/PE-System in jeder Hinsicht den Anforderungen an die Sicherheit im Sinne der erforderlichen Sicherheitsfunktionen und der Sicherheitsintegrität entspricht.	Sicherheitsbezogenes E/E/PE-System	7.7.2	Spezifikation der Anforderungen an die Sicherheit des E/E/PE-Systems und Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems Plan für die Validierung der Sicherheit der sicherheitsbezogenen E/E/PE-Systeme	Vollständig in Bezug auf Sicherheit validierte sicherheitsbezogene E/E/PE-Systeme Ergebnisse der Validierung der Sicherheit des E/E/PE-Systems
–	Modifikation des E/E/PE-Systems	Korrekturen, Verbesserungen oder Anpassungen an dem sicherheitsbezogenen E/E/PE-System durchführen und dabei sicherstellen, dass die erforderliche Sicherheitsintegrität erreicht wird und aufrechterhalten bleibt.	Sicherheitsbezogenes E/E/PE-System	7.8.2	Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems	Ergebnisse der Modifikation des E/E/PE-Systems
–	Verifikation des E/E/PE-Systems	Die Ergebnisse einer gegebenen Phase testen und bewerten, um Korrektheit und Konsistenz hinsichtlich der Produkte und Normen sicherzustellen, welche die Eingabe zu dieser Phase bilden.	Sicherheitsbezogenes E/E/PE-System	7.9.2	Wie oben – hängt von der Phase ab Plan für die Verifikation der sicherheitsbezogenen E/E/PE-Systeme für jede Phase	Wie oben – hängt von der Phase ab Ergebnisse der Verifikation der sicherheitsbezogenen E/E/PE-Systeme für jede Phase
–	Beurteilung der funktionalen Sicherheit des E/E/PE-Systems	Die Angemessenheit der durch das sicherheitsbezogene E/E/PE-System erreichten funktionalen Sicherheit untersuchen und ein Urteil dazu bilden.	Sicherheitsbezogenes E/E/PE-System	Abschnitt 8	Plan für die Beurteilung der funktionalen Sicherheit des E/E/PE-Systems	Ergebnisse der Beurteilung der funktionalen Sicherheit des E/E/PE-Systems

7.2 Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems

ANMERKUNG Diese Phase entspricht Kasten 10.1 von Bild 2.

7.2.1 Ziel

Das Ziel der Anforderungen dieses Unterabschnittes ist es, für jedes sicherheitsbezogene E/E/PE-System die Anforderungen an den Entwurf in Form von Teilsystemen und Elementen festzulegen.

ANMERKUNG 1 Die Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems wird normalerweise von der Spezifikation der Anforderungen an die Sicherheit des E/E/PE-Systems durch Zerlegung der Sicherheitsfunktionen und Zuordnung von Teilen der Sicherheitsfunktion zu Teilsystemen (zum Beispiel Gruppen von Sensoren, Logiksystemen oder Aktoren) abgeleitet. Die Anforderungen an die Teilsysteme können in der Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems enthalten sein oder können separat vorliegen und von der Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems aus referenziert werden. Teilsysteme können weiter in Elemente und Architekturen zerlegt werden, um die Anforderungen an den Entwurf und die Entwicklung nach 7.4 zu erfüllen. Die Anforderungen an diese Elemente können in den Anforderungen an die Teilsysteme enthalten sein oder können separat vorliegen und von den Anforderungen an die Teilsysteme aus referenziert werden.

7.2.2 Allgemeines

7.2.2.1 Die Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems muss von den in IEC 61508-1, 7.10 spezifizierten Anforderungen an die Sicherheit des E/E/PE-Systems abgeleitet werden.

ANMERKUNG Vorsicht ist angebracht, falls Nichtsicherheitsfunktionen und Sicherheitsfunktionen im selben sicherheitsbezogenen E/E/PE-System implementiert werden. Obwohl dieses nach der Norm erlaubt ist, kann es zu größerer Komplexität führen und es schwieriger machen, die Tätigkeiten des Sicherheitslebenszyklus des E/E/PE-Systems auszuführen (zum Beispiel Entwurf, Validierung, Beurteilung der funktionalen Sicherheit und Instandhaltung). Siehe auch 7.4.2.3.

7.2.2.2 Die Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems muss in einer Art und Weise ausgedrückt und strukturiert werden, so dass sie wie folgt ist:

- a) klar, genau, unzweideutig, nachprüfbar, testbar, pflegbar und ausführbar;
- b) geschrieben, um den Personen Unterstützung zu leisten, die wahrscheinlich die Informationen in irgendeiner Phase des Sicherheitslebenszyklus des E/E/PE-Systems verwenden; und
- c) zurückführbar auf die Spezifikation der Anforderungen an die Sicherheit des E/E/PE-Systems.

7.2.3 Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems

7.2.3.1 Die Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems muss Anforderungen an den Entwurf in Bezug auf die Sicherheitsfunktionen (siehe 7.2.3.2) und Anforderungen an den Entwurf in Bezug auf die Sicherheitsintegrität (siehe 7.2.3.3) enthalten.

7.2.3.2 Die Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems muss, wie durch die Spezifikation der Anforderungen an die Sicherheitsfunktionen des E/E/PE-Systems (siehe IEC 61508-1, 7.10.2.6) festgelegt, Einzelheiten der gesamten für die Implementierung der erforderlichen Sicherheitsfunktionen notwendigen Hardware und Software enthalten. Die Spezifikation muss für jede Sicherheitsfunktion beinhalten:

- a) Anforderungen an die Teilsysteme und Anforderungen an ihre Hardware- und Softwareelemente wie zutreffend;
- b) Anforderungen zur Integration der Teilsysteme und ihrer Hardware- und Softwareelemente, um die Spezifikation der Anforderungen an die Sicherheitsfunktionen des E/E/PE-Systems zu erfüllen;
- c) Durchsatzleistungsfähigkeit, die es ermöglicht, Anforderungen in Bezug auf die Reaktionszeit zu erfüllen;
- d) Anforderungen an die Genauigkeit und Widerstandsfähigkeit für Messungen und Steuerungen;
- e) Schnittstellen des sicherheitsbezogenen E/E/PE-Systems und Bedienerschnittstellen;
- f) Schnittstellen zwischen den sicherheitsbezogenen E/E/PE-Systemen und allen anderen Systemen (entweder innerhalb oder außerhalb der EUC);
- g) alle Verhaltensweisen der sicherheitsbezogenen E/E/PE-Systeme, insbesondere Ausfallverhalten und die erforderliche Reaktion (zum Beispiel Alarm, automatische Abschaltung) der sicherheitsbezogenen E/E/PE-Systeme;
- h) die Bedeutung aller Hardware-/Softwarewechselwirkungen und, wo zutreffend, alle erforderlichen Einschränkungen zwischen Hardware und Software;

ANMERKUNG Wo diese Wechselwirkungen vor Beendigung des Entwurfs nicht bekannt sind, können nur allgemeine Einschränkungen angegeben werden.

- i) alle Grenzbedingungen und Einschränkungen für die sicherheitsbezogenen E/E/PE-Systeme und ihre zugehörigen Elemente, zum Beispiel zeitliche Einschränkungen, oder Einschränkungen wegen möglicher Ausfälle infolge gemeinsamer Ursache;
- j) alle speziellen Anforderungen in Bezug auf die Verfahren für Anlauf und Wiederanlauf der sicherheitsbezogenen E/E/PE-Systeme.

7.2.3.3 Die Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems muss für den Entwurf relevante Einzelheiten enthalten, um den Sicherheits-Integritätslevel und den erforderlichen Ausfallgrenzwert für die Sicherheitsfunktion, wie durch die Spezifikation der Anforderungen an die Sicherheitsintegrität des E/E/PE-Systems festgelegt (siehe IEC 61508-1, 7.10.2.7), zu erreichen, einschließlich:

- a) der Architektur jedes Teilsystems, die erforderlich ist, um die Einschränkungen hinsichtlich der Architektur zur Sicherheitsintegrität der Hardware (siehe 7.4.4) zu erfüllen;
- b) aller relevanten Zuverlässigkeitsmodellierungsparameter, wie zum Beispiel der erforderlichen Häufigkeit von Wiederholungsprüfungen aller Hardwareelemente, die zum Erreichen des Ausfallgrenzwertes notwendig sind;

ANMERKUNG 1 Informationen zur speziellen Anwendung können nicht unberücksichtigt bleiben (siehe IEC 61508-1, 7.10.2.1). Dies ist insbesondere für die Instandhaltung wichtig, wo das festgelegte Intervall für die Wiederholungsprüfung nicht kleiner sein sollte, als vernünftigerweise für die jeweilige Anwendung erwartet werden kann. Zum Beispiel ist die Zeit zwischen Wartungen, die realistischerweise für allgemein verwendete Massenprodukte erreicht werden kann, wahrscheinlich größer als die Zeit für Produkte in einer besser überwachten Anwendung.

- c) der zu treffenden Maßnahmen im Falle eines durch Diagnosemaßnahmen erkannten gefahrbringenden Ausfalls;
- d) der Anforderungen, Einschränkungen, Funktionen und Betriebsmitteln, um die Durchführung der Wiederholungsprüfung der E/E/PE-Hardware zu ermöglichen;
- e) des Leistungsvermögens verwendeter Betriebsmittel, den Extremwerten aller Umgebungsbedingungen (z. B. Temperatur, Feuchte, mechanisch, elektrisch) zu entsprechen, die als während des Sicherheitslebenszyklus des E/E/PE-Systems erforderlich festgelegt sind, einschließlich Herstellung, Lagerung, Transport, Prüfung, Installation, Inbetriebnahme, Betrieb und Instandhaltung;
- f) der erforderlichen elektromagnetischen Störfestigkeit (siehe IEC/TS 61000-1-2:2008);

ANMERKUNG 2 Die Störfestigkeit kann sich für unterschiedliche Elemente des sicherheitsbezogenen Systems unterscheiden, abhängig vom physikalischen Ort und den Anordnungen der Energieversorgungen.

ANMERKUNG 3 Hilfestellung kann in EMV-Produktnormen gefunden werden. Es ist jedoch wichtig zu berücksichtigen, dass für besondere Einsatzorte oder wenn die Betriebsmittel für die Verwendung in rauer elektromagnetischer Umgebung vorgesehen sind, höhere Störfestigkeitspegel oder zusätzliche Störfestigkeitsanforderungen als die in solchen Normen festgelegten notwendig sein können.

- g) der Maßnahmen zur Qualitätssicherung/Qualitätskontrolle, die für das Sicherheitsmanagement (siehe IEC 61508-1, 6.2.5) notwendig sind.

7.2.3.4 Die Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems muss entsprechend dem Fortschritt des Entwurfs im Detail vervollständigt und nach Modifikation wie notwendig aktualisiert werden.

7.2.3.5 Zur Vermeidung von Irrtümern während der Entwicklung der Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems muss eine angemessene Gruppe von Verfahren und Maßnahmen nach [Tabelle B.1](#) verwendet werden.

7.2.3.6 Die durch die Anforderungen an den Entwurf des E/E/PE-Systems auferlegten Auswirkungen auf die Architektur müssen berücksichtigt werden.

ANMERKUNG Dies sollte die Überlegung der Einfachheit der Implementierung, um den erforderlichen Sicherheits-Integritätslevel zu erreichen, einschließen (einschließlich Überlegungen zur Architektur und zur Zuteilung von Funktionalität zu Konfigurationsdaten oder zum Embedded-System).

7.3 Planung der Validierung der Sicherheit des E/E/PE-Systems

ANMERKUNG Diese Phase entspricht Kasten 10.2 in [Bild 2](#). Sie wird üblicherweise parallel zum Entwurf und zur Entwicklung des E/E/PE-Systems (siehe 7.4) ausgeführt.

7.3.1 Ziel

Das Ziel der Anforderungen dieses Unterabschnittes ist es, die Validierung der Sicherheit des sicherheitsbezogenen E/E/PE-Systems zu planen.

7.3.2 Anforderungen

7.3.2.1 Es muss eine Planung durchgeführt werden, um die Schritte (sowohl verfahrensmäßige als auch technische) festzulegen, die für den Nachweis ausgeführt werden müssen, dass das sicherheitsbezogene E/E/PE-System die Spezifikation der Anforderungen an die Sicherheit des E/E/PE-Systems (siehe IEC 61508-1, 7.10) und die Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems (siehe [7.2](#)) erfüllt.

7.3.2.2 Die Planung der Validierung des sicherheitsbezogenen E/E/PE-Systems muss Folgendes betrachten:

- a) alle in der Spezifikation der Anforderungen an die Sicherheit des E/E/PE-Systems und der Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems definierten Anforderungen;
- b) die Verfahren, die anzuwenden sind, um zu validieren, dass jede Sicherheitsfunktion korrekt implementiert ist, und die Kriterien für bestanden/nicht bestanden für die Ausführung der Tests;
- c) die Verfahren, die anzuwenden sind, um zu validieren, dass jede Sicherheitsfunktion der erforderlichen Sicherheitsintegrität entspricht, und die Kriterien für bestanden/nicht bestanden für die Ausführung der Tests;
- d) die erforderliche Umgebung, in der die Tests stattzufinden haben, einschließlich aller notwendigen Werkzeuge und Betriebsmittel (ebenso die Planung, welche Werkzeuge und Betriebsmittel kalibriert sein sollten);
- e) Testbewertungsverfahren (mit Begründungen);
- f) die Testverfahren und Bewertungskriterien, die anzuwenden sind, um die festgelegten elektromagnetischen Störfestigkeitsgrenzwerte zu validieren;

ANMERKUNG Eine Anleitung zur Spezifikation der Prüfungen der elektromagnetischen Störfestigkeit für Elemente von sicherheitsbezogenen Systemen ist in IEC/TS 61000-1-2 enthalten.

- g) Grundsätze zur Behandlung von Ausfällen im Rahmen der Validierung.

7.4 Entwurf und Entwicklung des E/E/PE-Systems

ANMERKUNG Diese Phase entspricht Kasten 10.3 in [Bild 2](#). Sie wird üblicherweise parallel zur Planung der Validierung der Sicherheit des E/E/PE-Systems (siehe 7.3) ausgeführt.

7.4.1 Ziel

Das Ziel der Anforderungen dieses Unterabschnittes ist es, das sicherheitsbezogene E/E/PE-System (einschließlich ASICs, wenn zutreffend, siehe IEC 61508-4, 3.2.15) zu entwerfen und zu entwickeln, um die Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems (im Hinblick auf die Anforderungen an die Sicherheitsfunktionen und die Anforderungen an die Sicherheitsintegrität (siehe [7.2](#))) zu erfüllen.

7.4.2 Allgemeine Anforderungen

7.4.2.1 Der Entwurf des sicherheitsbezogenen E/E/PE-Systems muss in Übereinstimmung mit der Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems (siehe [7.2.3](#)) unter Berücksichtigung aller Anforderungen nach [7.2.3](#) erstellt werden.

7.4.2.2 Der Entwurf des sicherheitsbezogenen E/E/PE-Systems (einschließlich der Gesamt-Hardwarearchitektur und Gesamt-Softwarearchitektur, Sensoren, Aktoren, programmierbarer Elektronik, ASICs, Embedded-Software, Anwendungssoftware, Daten usw.) muss alle Anforderungen von a) bis e) wie folgt erfüllen:

- a) die Anforderungen an die Sicherheitsintegrität der Hardware, bestehend aus:
 - den Einschränkungen der Sicherheitsintegrität der Hardware hinsichtlich der Architektur (siehe 7.4.4) und
 - den Anforderungen zur Quantifizierung der Auswirkung zufälliger Ausfälle (siehe 7.4.5);
- b) die besonderen Architektur Anforderungen an ICs mit On-Chip-Redundanz (siehe Anhang E), wo zutreffend, außer es kann begründet werden, dass der gleiche Grad von Unabhängigkeit zwischen verschiedenen Kanälen durch Anwendung eines anderen Maßnahmenkatalogs erreicht wird;
- c) die Anforderungen an die systematische Sicherheitsintegrität (systematische Eignung), die durch Ausführung einer der nachfolgenden Konformitätspfade erfüllt werden können:
 - Pfad 1_S: Übereinstimmung mit den Anforderungen zur Vermeidung von systematischen Fehlern (siehe 7.4.6 und IEC 61508-3) und den Anforderungen zur Beherrschung von systematischen Fehlern (siehe 7.4.7 und IEC 61508-3), oder
 - Pfad 2_S: Übereinstimmung mit den Anforderungen für den Nachweis, dass die Betriebsmittel betriebsbewährt sind (siehe 7.4.10), oder
 - Pfad 3_S (nur bereits existierende Softwareelemente): Übereinstimmung mit den Anforderungen von IEC 61508-3, 7.4.2.12;

ANMERKUNG Das tief gestellte „S“ in den oben aufgeführten Pfaden bezeichnet die systematische Sicherheitsintegrität zur Unterscheidung von Pfad 1_H und Pfad 2_H für die Sicherheitsintegrität der Hardware.

- d) die Anforderungen an das Systemverhalten bei Erkennung eines Fehlers (siehe 7.4.8);
- e) die Anforderungen an Datenkommunikationsprozesse (siehe 7.4.11).

7.4.2.3 Wenn ein sicherheitsbezogenes E/E/PE-System sowohl Sicherheitsfunktionen als auch Nichtsicherheitsfunktionen zu implementieren hat, muss die gesamte Hardware und Software als sicherheitsbezogen behandelt werden, es sei denn, es kann gezeigt werden, dass die Implementierung der Sicherheitsfunktionen und Nichtsicherheitsfunktionen ausreichend unabhängig voneinander ist (d. h., dass der Ausfall irgendeiner Nichtsicherheitsfunktion keinen gefährlichen Ausfall einer Sicherheitsfunktion verursachen kann).

ANMERKUNG 1 Eine ausreichende Unabhängigkeit der Implementierung liegt vor, wenn gezeigt wird, dass die Wahrscheinlichkeit eines abhängigen Ausfalls zwischen den nicht sicherheitsbezogenen und sicherheitsbezogenen Teilen im Vergleich zum höchsten Sicherheits-Integritätslevel, der mit den betroffenen Sicherheitsfunktionen verbunden ist, ausreichend gering ist.

ANMERKUNG 2 Vorsicht ist angebracht, falls Nichtsicherheitsfunktionen und Sicherheitsfunktionen im selben sicherheitsbezogenen E/E/PE-System implementiert werden. Obwohl dieses nach der Norm erlaubt ist, kann es zu größerer Komplexität führen und kann es schwieriger machen, die Tätigkeiten des Sicherheitslebenszyklus des E/E/PE-Systems auszuführen (zum Beispiel Entwurf, Validierung, Beurteilung der funktionalen Sicherheit und Instandhaltung).

7.4.2.4 Die Anforderungen an Hardware und Software müssen durch den Sicherheits-Integritätslevel der Sicherheitsfunktion mit dem höchsten Sicherheits-Integritätslevel bestimmt werden, es sei denn, es kann gezeigt werden, dass die Implementierung von Sicherheitsfunktionen verschiedener Sicherheits-Integritätslevel ausreichend unabhängig ist.

ANMERKUNG 1 Eine ausreichende Unabhängigkeit der Implementierung liegt vor, wenn gezeigt wird, dass die Wahrscheinlichkeit eines abhängigen Ausfalls zwischen den Teilen, die Sicherheitsfunktionen unterschiedlicher Sicherheits-Integritätslevel enthalten, im Vergleich zum höchsten Sicherheits-Integritätslevel, der mit den betroffenen Sicherheitsfunktionen verbunden ist, ausreichend gering ist.

ANMERKUNG 2 Wenn mehrere Sicherheitsfunktionen in einem sicherheitsbezogenen E/E/PE-System implementiert werden, ist es notwendig, die Möglichkeit zu betrachten, dass ein einzelner Fehler einen Ausfall mehrerer Sicherheitsfunktionen bedingt. In einer solchen Situation kann es angebracht sein, die Anforderungen an Hardware und Software auf der Basis eines höheren Sicherheits-Integritätslevels als dem mit irgendeiner der Sicherheitsfunktionen in Verbindung stehenden in Abhängigkeit von dem mit einem solchen Ausfall verbundenen Risiko festzulegen.

7.4.2.5 Ist Unabhängigkeit zwischen den Sicherheitsfunktionen gefordert (siehe 7.4.2.3 und 7.4.2.4), muss Folgendes während des Entwurfs dokumentiert werden:

- a) die Methode zum Erreichen der Unabhängigkeit;
- b) die Begründung der Methode.

BEISPIEL Behandlung vorhersehbarer Ausfallarten, die die Unabhängigkeit untergraben könnten, und ihrer Ausfallraten durch die Verwendung von FMECA oder Analyse abhängiger Ausfälle.

7.4.2.6 Die Anforderungen an sicherheitsbezogene Software (siehe IEC 61508-3) müssen dem Entwickler des sicherheitsbezogenen E/E/PE-Systems zur Verfügung gestellt werden.

7.4.2.7 Der Entwickler des sicherheitsbezogenen E/E/PE-Systems muss die Anforderungen an die sicherheitsbezogene Software und Hardware überprüfen, um sicherzustellen, dass die Anforderungen angemessen festgelegt sind. Insbesondere muss der Entwickler des E/E/PE-Systems Folgendes betrachten:

- a) Sicherheitsfunktionen;
- b) Anforderungen an die Sicherheitsintegrität des sicherheitsbezogenen E/E/PE-Systems;
- c) Betriebsmittel- und Bedienerschnittstellen.

7.4.2.8 Die Dokumentation des Entwurfs des sicherheitsbezogenen E/E/PE-Systems muss die Verfahren und Maßnahmen festlegen, die während der Phasen des Sicherheitslebenszyklus des E/E/PE-Systems notwendig sind, um den Sicherheits-Integritätslevel zu erreichen.

7.4.2.9 Die Dokumentation des Entwurfs des sicherheitsbezogenen E/E/PE-Systems muss die Begründung für die Verfahren und Maßnahmen enthalten, die gewählt worden sind, um eine geeignete Zusammenstellung zu bilden, die für den erforderlichen Sicherheits-Integritätslevel ausreichend ist.

ANMERKUNG Die Wahl eines gesamtheitlichen Lösungsansatzes mit Ausführung unabhängiger Typprüfungen der sicherheitsbezogenen E/E/PE-Systeme (einschließlich Sensoren, Aktoren usw.) für Hardware und Software, Diagnose-tests und Programmierwerkzeuge und, wo immer möglich, Verwendung angemessener Programmiersprachen für die Software bietet die Möglichkeit, die Komplexität des Anwendungs-Engineering des E/E/PE-Systems zu vermindern.

7.4.2.10 Während der Entwurfs- und Entwicklungstätigkeiten muss die Bedeutung (wo zutreffend) aller Hardware- und Software-Wechselwirkungen festgestellt, bewertet und dokumentiert werden.

7.4.2.11 Der Entwurf muss auf einer Aufteilung in Teilsysteme basieren, wobei jedes Teilsystem einen festgelegten Entwurf und eine Zusammenstellung von Integrationstests besitzt (siehe 7.5.2).

ANMERKUNG 1 Ein Teilsystem kann als aus einem einzigen Element oder einer Gruppe von Elementen bestehend betrachtet werden. Siehe IEC 61508-4 für Definitionen. Ein vollständiges sicherheitsbezogenes E/E/PE-System setzt sich aus einer Anzahl von identifizierbaren und separaten Teilsystemen zusammen, die, wenn sie zusammengefügt sind, die betrachtete Sicherheitsfunktion implementieren. Ein Teilsystem kann mehr als einen Kanal besitzen (siehe 7.4.9.3 und 7.4.9.4).

ANMERKUNG 2 Wann immer möglich, sollten vorhandene verifizierte Teilsysteme in der Implementierung verwendet werden. Diese Aussage ist nur gültig, wenn beinahe 100 % Übereinstimmung in Teilsystem- oder Elementfunktionalität, Kapazität und Leistungsfähigkeit mit den neuen Anforderungen besteht oder das verifizierte Teilsystem oder Element in einer solchen Art und Weise strukturiert ist, dass es dem Anwender möglich ist, nur die für die spezielle Anwendung erforderliche Funktion, Kapazität oder Leistungsfähigkeit auszuwählen. Eine übermäßige Funktionalität, Kapazität oder Leistungsfähigkeit kann schädlich für die Systemsicherheit sein, wenn das vorhandene Teilsystem oder Element übermäßig kompliziert ist oder nicht verwendete Bestandteile enthält, und wenn ein Schutz gegen unbeabsichtigte Funktionen nicht erreicht werden kann.

7.4.2.12 Wenn der einleitende Entwurf des sicherheitsbezogenen E/E/PE-Systems abgeschlossen worden ist, muss eine Analyse durchgeführt werden, um zu ermitteln, ob irgendein vernünftigerweise vorhersehbarer Ausfall des sicherheitsbezogenen E/E/PE-Systems eine Gefährdungssituation verursachen oder eine Anforderung an irgendeine andere Maßnahme zur Risikobeherrschung stellen könnte. Wenn irgendein vernünftigerweise vorhersehbarer Ausfall eine dieser Auswirkung haben könnte, muss die erste Priorität die Veränderung des Entwurfs des sicherheitsbezogenen E/E/PE-Systems sein um solche Ausfallarten zu vermeiden.

Wenn dies nicht erfolgen kann, müssen Maßnahmen gewählt werden, um die Wahrscheinlichkeit solcher Ausfallarten auf ein Maß zu vermindern, das angemessen zum Ausfallgrenzwert ist. Diese Maßnahmen müssen den Anforderungen dieser Norm unterliegen.

ANMERKUNG Es ist die Absicht dieses Abschnitts, Ausfallmodi des sicherheitsbezogenen E/E/PE-Systems zu identifizieren, die eine Anforderung an andere risikobeherrschende Maßnahmen stellen. Es können Fälle existieren, in denen die Ausfallrate der spezifizierten Ausfallmodi nicht reduziert werden kann und entweder eine neue Sicherheitsfunktion erforderlich wird oder der SIL der anderen Sicherheitsfunktionen unter Berücksichtigung der Ausfallrate nochmals zu überdenken ist.

7.4.2.13 Unterlastung (en: de-rating, siehe IEC 61508-7) sollte für alle Hardwarebauteile berücksichtigt werden. Die Begründung für den Betrieb irgendwelcher Hardwareelemente an ihren Grenzen muss dokumentiert werden (siehe IEC 61508-1, Abschnitt 5).

ANMERKUNG Wo Unterlastung angebracht ist, ist ein Unterlastungsgrad von annähernd zwei Drittel typisch.

7.4.2.14 Wenn der Entwurf eines sicherheitsbezogenen E/E/PE-Systems ein oder mehrere ASICs zur Implementierung einer Sicherheitsfunktion einschließt, muss ein ASIC-Entwicklungslebenszyklus (siehe 7.1.3.1) angewendet werden.

7.4.3 Synthese von Elementen zum Erreichen der erforderlichen systematischen Eignung

7.4.3.1 Um die Anforderungen an die systematische Sicherheitsintegrität zu erfüllen, kann das vorgesehene sicherheitsbezogene E/E/PE-System unter den in diesem Abschnitt beschriebenen Umständen in Elemente unterschiedlicher systematischer Eignung aufgeteilt werden.

ANMERKUNG 1 Die systematische Eignung eines Elements bestimmt das Potenzial für systematische Fehler dieses Elements, das zu einem Ausfall der Sicherheitsfunktion führt. Das Konzept der systematischen Eignung eines Elements ist gleichermaßen auf Hardware- und Softwareelemente anwendbar.

ANMERKUNG 2 IEC 61508-1, 7.6.2.7 beachtet den Nutzen von Unabhängigkeit und Diversität auf der Ebene einer Sicherheitsfunktion und der sicherheitsbezogenen E/E/PE-Systeme, zu denen sie zugeordnet werden könnte. Diese Vorstellungen können auch auf der Ebene des detaillierten Entwurfs angewendet werden, wo eine Anordnung von Elementen, die eine Sicherheitsfunktion implementieren, potenziell eine bessere systematische Leistungsfähigkeit erreichen kann als einzelne Elemente.

7.4.3.2 Für ein Element mit der systematischen Eignung SC N ($N = 1, 2, 3$), bei dem ein systematischer Fehler dieses Elements nicht zu einem Ausfall der festgelegten Sicherheitsfunktion führt, dies jedoch nur in Kombination mit einem zweiten systematischen Fehler eines anderen Elements mit der systematischen Eignung SC N erfolgt, kann die systematische Eignung der Kombination der beiden Elemente als eine systematische Eignung von SC ($N + 1$) betrachtet werden, vorausgesetzt, dass zwischen den beiden Elementen eine ausreichende Unabhängigkeit besteht (siehe 7.4.3.4).

ANMERKUNG Die Unabhängigkeit der Elemente kann nur beurteilt werden, wenn die konkrete Anwendung der Elemente in Bezug auf die definierten Sicherheitsfunktionen bekannt ist.

7.4.3.3 Die systematische Eignung, die für eine Kombination von Elementen in Anspruch genommen werden kann, wenn jedes einzelne Element die systematische Eignung SC N besitzt, kann höchstens SC ($N + 1$) betragen. Ein Element von SC N kann nur einmal auf diese Weise verwendet werden. Es ist nicht gestattet, SC ($N + 2$) und besser durch aufeinanderfolgendes Zusammenfügen von Anordnungen aus SC N-Elementen zu erreichen.

7.4.3.4 Ausreichende Unabhängigkeit im Entwurf zwischen Elementen und in der Anwendung von Elementen muss durch eine Analyse gemeinsamer Ursachen begründet werden, um zu zeigen, dass die Wahrscheinlichkeit einer Beeinträchtigung zwischen Elementen und zwischen den Elementen und der Umgebung ausreichend gering im Vergleich zum Sicherheits-Integritätslevel der betrachteten Sicherheitsfunktion ist.

ANMERKUNG 1 Für die systematische Eignung schließen mögliche Ansätze zum Erreichen ausreichender Unabhängigkeit hinsichtlich Hardwareentwurf, Realisierung, Betrieb und Instandhaltung Folgendes ein:

- funktionale Diversität: Verwendung unterschiedlicher Methoden, um die gleichen Ergebnisse zu erreichen;
- diversitäre Technologien: Verwendung unterschiedlicher Arten von Betriebsmitteln, um die gleichen Ergebnisse zu erreichen;
- gemeinsame Teile/Dienste: Sicherstellen, dass es keine gemeinsamen Teile oder Dienste oder Hilfssysteme (zum Beispiel Stromversorgungen) gibt, deren Ausfall zu einem gefahrbringenden Ausfall aller Systeme führen kann;
- gemeinsame Verfahren: Sicherstellen, dass es keine gemeinsamen Betriebs-, Instandhaltungs- oder Prüfverfahren gibt.

ANMERKUNG 2 Unabhängigkeit von der Anwendung bedeutet, dass Elemente das Ausführungsverhalten untereinander nicht derart ungünstig beeinflussen, dass ein gefahrbringender Ausfall auftreten wird.

ANMERKUNG 3 Zur Unabhängigkeit von Softwareelementen siehe IEC 61508-3, 7.4.2.8 und 7.4.2.9.

7.4.4 Einschränkungen der Sicherheitsintegrität der Hardware hinsichtlich der Architektur

ANMERKUNG 1 Die Gleichung in Bezug auf Einschränkungen der Sicherheitsintegrität der Hardware ist in [Anhang C](#) beschrieben und die Einschränkungen der Sicherheitsintegrität sind in [Tabelle 2](#) und [Tabelle 3](#) zusammengefasst.

ANMERKUNG 2 IEC 61508-6, Abschnitt A.2 gibt einen Überblick über die notwendigen Schritte zum Erreichen der erforderlichen Sicherheitsintegrität der Hardware und zeigt, wie dieser Unterabschnitt zu anderen Anforderungen dieser Norm in Bezug steht.

Im Zusammenhang mit der Sicherheitsintegrität der Hardware ist der höchste Sicherheits-Integritätslevel, der für eine Sicherheitsfunktion beansprucht werden kann, durch die Einschränkungen der Sicherheitsintegrität der Hardware begrenzt, die durch die Implementierung einer der beiden möglichen Pfade (auf System- oder Teilsystemebene zu implementieren) erreicht werden müssen:

- Pfad 1_H basierend auf Vorstellungen der Hardwarefehlertoleranz und des Anteils sicherer Ausfälle; oder
- Pfad 2_H basierend auf Bauteilzuverlässigkeitsdaten, die aus der Rückmeldung von Endanwendern stammen, erhöhten Konfidenzniveaus und einer Hardwarefehlertoleranz für festgelegte Sicherheits-Integritätslevel.

Anwendungsspezifische Normen, die auf der Normenreihe IEC 61508 basieren, können auf einen bevorzugten Pfad hinweisen (d. h. Pfad 1_H oder Pfad 2_H).

ANMERKUNG 3 Das tief gestellte „H“ in den oben aufgeführten Pfaden bezeichnet die Sicherheitsintegrität der Hardware zur Unterscheidung von Pfad 1_S, Pfad 2_S und Pfad 3_S für die systematische Sicherheitsintegrität.

7.4.4.1 Allgemeine Anforderungen

7.4.4.1.1 Im Hinblick auf die Anforderungen zur Hardwarefehlertoleranz

- a) bedeutet eine Hardwarefehlertoleranz von N, dass N + 1 die minimale Anzahl von Fehlern ist, die zu einem Verlust der Sicherheitsfunktion führen können (für weitere Erläuterung siehe [Anmerkung 1](#) und [Tabelle 2](#) und [Tabelle 3](#)). Bei der Bestimmung der Hardwarefehlertoleranz darf keine Berücksichtigung von anderen Maßnahmen erfolgen, welche die Auswirkungen von Fehlern beherrschen können, wie zum Beispiel Diagnoseeinrichtungen; und
- b) werden, wo ein Fehler direkt zu einem oder mehreren nachfolgenden Fehlern führt, diese Fehler als ein Einzelfehler betrachtet;
- c) können bei der Bestimmung der erreichten Hardwarefehlertoleranz bestimmte Fehler unter der Voraussetzung ausgeschlossen werden, dass die Wahrscheinlichkeit ihres Auftretens sehr gering ist im Verhältnis zu den Anforderungen an die Sicherheitsintegrität des Teilsystems. Jeder einzelne Fehlerausschluss muss begründet und dokumentiert werden (siehe [Anmerkung 2](#)).

ANMERKUNG 1 Die Einschränkungen der Sicherheitsintegrität der Hardware wurden aufgenommen, um eine ausreichend robuste Architektur unter Berücksichtigung des Niveaus der Komplexität von Elementen und Teilsystemen (siehe

7.4.4.1.1 und 7.4.4.1.2) zu erreichen. Der höchste zulässige Sicherheits-Integritätslevel für die durch das sicherheitsbezogene E/E/PE-System implementierte Sicherheitsfunktion, der unter Anwendung dieser Anforderungen abgeleitet wird, ist der höchstens für die Sicherheitsfunktion in Anspruch nehmbar, auch wenn in einigen Fällen Zuverlässigkeitsberechnungen zeigen, dass ein höherer Sicherheits-Integritätslevel erreicht werden könnte. Es ist weiterhin anzumerken, dass, auch wenn die Hardwarefehlertoleranz für alle Teilsysteme erreicht wird, trotzdem eine Zuverlässigkeitsberechnung notwendig ist, um zu zeigen, dass der festgelegte Ausfallgrenzwert erreicht worden ist; dies kann erfordern, dass die Hardwarefehlertoleranz erhöht werden muss, um die Anforderungen an den Entwurf zu erfüllen.

ANMERKUNG 2 Die Anforderungen zur Hardwarefehlertoleranz beziehen sich auf die unter den normalen Betriebsbedingungen verwendete Teilsystemarchitektur. Die Anforderungen zur Hardwarefehlertoleranz können verringert werden, während das sicherheitsbezogene E/E/PE-System im Betrieb repariert wird. Jedoch sollten die Schlüsselp Parameter in Bezug auf jede Verringerung vorher bewertet worden sein (zum Beispiel MTTR im Vergleich zur Wahrscheinlichkeit einer Anforderung).

ANMERKUNG 3 Bestimmte Fehler können ausgeschlossen werden, weil, wenn ein Element eindeutig eine sehr geringe Ausfallwahrscheinlichkeit auf Grund von Eigenschaften besitzt, die durch seinen Entwurf und seine Konstruktion inhärent bedingt sind (zum Beispiel ein mechanisches Aktor-Verbindungssystem), es üblicherweise nicht als notwendig erachtet wird, die Sicherheitsintegrität irgendeiner Sicherheitsfunktion, die dieses Element verwendet, (auf Grund der Hardwarefehlertoleranz) einzuschränken.

ANMERKUNG 4 Die Wahl des Pfades ist anwendungs- und sektorabhängig, und das Folgende sollte berücksichtigt werden, wenn der Pfad ausgewählt wird:

- ein sicherer Zustand einer bestimmten Funktion könnte eine neue Gefährdung hervorrufen oder eine zusätzliche Ursache für eine bestehende Gefährdung sein;
- Redundanz könnte nicht für alle Funktionen umsetzbar sein;
- Reparatur ist nicht immer oder schnell möglich (z. B. nicht durchführbar innerhalb einer Zeit, die im Vergleich zum Intervall für die Wiederholungsprüfung unbedeutend ist).

ANMERKUNG 5 Besondere Architekturanforderungen an ICs mit On-Chip-Redundanz sind in [Anhang E](#) enthalten.

7.4.4.1.2 Ein Element kann als vom Typ A betrachtet werden, wenn für die Bauteile, die für das Erreichen der Sicherheitsfunktion erforderlich sind:

- a) das Ausfallverhalten aller eingesetzten Bauteile eindeutig definiert ist; und
- b) das Verhalten des Elements unter Fehlerbedingungen vollständig bestimmt werden kann; und
- c) ausreichend verlässliche Ausfalldaten existieren, um zu zeigen, dass die angenommenen Ausfallraten für erkannte und unerkannte gefahrbringende Ausfälle erreicht werden (siehe [7.4.9.3 bis 7.4.9.5](#)).

7.4.4.1.3 Ein Element muss als vom Typ B betrachtet werden, wenn für die Bauteile, die für das Erreichen der Sicherheitsfunktion erforderlich sind:

- a) das Ausfallverhalten von mindestens einem eingesetzten Bauteil nicht eindeutig definiert ist; oder
- b) das Verhalten des Elements unter Fehlerbedingungen nicht vollständig bestimmt werden kann; oder
- c) keine ausreichend zuverlässigen Ausfalldaten vorliegen, um die beanspruchten Ausfallraten für erkannte und unerkannte gefahrbringende Ausfälle zu unterstützen (siehe [7.4.9.3 bis 7.4.9.5](#)).

ANMERKUNG Dies bedeutet, dass, falls mindestens ein Bauteil eines Elements selbst die Bedingungen für ein Typ B-Element erfüllt, dieses Element eher als Typ B wie als Typ A betrachtet wird.

7.4.4.1.4 Bei der Abschätzung des Anteils sicherer Ausfälle eines Elements, das zur Verwendung in einem Teilsystem mit einer Hardwarefehlertoleranz von 0 vorgesehen ist und das eine Sicherheitsfunktion oder einen Teil einer Sicherheitsfunktion ausführt, die in der Betriebsart mit hoher Anforderungsrate oder bei kontinuierlicher Anforderung betrieben wird, darf die Diagnose nur angerechnet werden, wenn:

- die Summe von Diagnose-Testintervall und der Zeit, um die zum Erreichen oder Aufrechterhalten eines sicheren Zustands festgelegte Reaktion durchzuführen, kleiner als die Prozess-Sicherheitszeit ist; oder
- bei Betrieb in der Betriebsart mit hoher Anforderungsrate das Verhältnis der Diagnose-Testrate zur Anforderungsrate 100 gleicht oder übertrifft.

7.4.4.1.5 Bei der Abschätzung des Anteils sicherer Ausfälle eines Elements, das:

- eine Hardwarefehlertoleranz größer 0 besitzt und das eine Sicherheitsfunktion oder einen Teil einer Sicherheitsfunktion ausführt, die in der Betriebsart mit hoher Anforderungsrate oder bei kontinuierlicher Anforderung betrieben wird; oder
- eine Sicherheitsfunktion oder einen Teil einer Sicherheitsfunktion in der Betriebsart mit niedriger Anforderungsrate ausführt;

darf die Diagnose nur angerechnet werden, wenn die Summe von Diagnose-Testintervall und die Zeit zur Ausführung der Reparatur eines erkannten Ausfalls geringer ist, als die in der Berechnung zur Ermittlung der erreichten Sicherheitsintegrität für diese Sicherheitsfunktion verwendete MTTR.

7.4.4.2 Pfad 1_H

7.4.4.2.1 Um den maximalen Sicherheits-Integritätslevel zu bestimmen, der für eine Sicherheitsfunktion in Anspruch genommen werden kann, muss das folgende Verfahren befolgt werden:

- 1) Definition der Teilsysteme, aus denen das sicherheitsbezogene E/E/PE-System besteht.
- 2) Für jedes Teilsystem Bestimmung des Anteils sicherer Ausfälle separat für alle Elemente im Teilsystem (d. h. auf individueller Basis von Elementen mit jedem Element mit einer Hardwarefehlertoleranz von 0). Bei redundanter Konfiguration der Elemente kann die SFF unter Berücksichtigung der zusätzlichen Diagnose, die vorhanden sein kann (z. B. durch Vergleich von redundanten Elementen), berechnet werden.
- 3) Für jedes Element Berücksichtigung des erreichten Anteils sicherer Ausfälle und der Hardwarefehlertoleranz von 0 zur Bestimmung des maximalen Sicherheits-Integritätslevels, der aus [Tabelle 2](#), Spalte 2 (für Typ A-Elemente), und aus [Tabelle 3](#), Spalte 2 (für Typ B-Elemente), in Anspruch genommen werden kann.
- 4) Anwendung der Methode in [7.4.4.2.3](#) und [7.4.4.2.4](#) zur Bestimmung des maximalen Sicherheits-Integritätslevels, der für das Teilsystem in Anspruch genommen werden kann.
- 5) Der maximale Sicherheits-Integritätslevel, der für ein sicherheitsbezogenes E/E/PE-System in Anspruch genommen werden kann, muss durch das Teilsystem bestimmt werden, das den niedrigsten Sicherheits-Integritätslevel erreicht hat.

7.4.4.2.2 Zur Anwendung auf Teilsysteme, die Elemente enthalten, die die speziellen, unten detaillierten Anforderungen erfüllen, ist als Alternative zur Anwendung der Anforderungen nach 7.4.4.2.1 2) bis 7.4.4.2.1 4) Folgendes anwendbar:

- 1) das Teilsystem enthält mehr als ein Element, und
- 2) die Elemente sind gleichen Typs, und
- 3) alle Elemente haben Anteile sicherer Ausfälle erreicht, die in den gleichen Bereichen liegen (siehe Anmerkung 1 unten), die in den [Tabellen 2](#) und [3](#) angegeben sind; dann kann das folgende Verfahren verwendet werden:
 - a) Bestimmung des Anteils sicherer Ausfälle für alle einzelnen Elemente. Bei redundanter Konfiguration der Elemente kann die SFF unter Berücksichtigung der zusätzlichen Diagnose, die vorhanden sein kann (z. B. durch Vergleich von redundanten Elementen), berechnet werden;
 - b) Bestimmung der Hardwarefehlertoleranz des Teilsystems;
 - c) Bestimmung des maximalen Sicherheits-Integritätslevels, der für das Teilsystem in Anspruch genommen werden kann, aus [Tabelle 2](#), wenn die Elemente dem Typ A entsprechen;
 - d) Bestimmung des maximalen Sicherheits-Integritätslevels, der für das Teilsystem in Anspruch genommen werden kann, aus [Tabelle 3](#), wenn die Elemente dem Typ B entsprechen.

ANMERKUNG 1 Der Bereich, auf den in 3) oben hingewiesen ist, bezieht sich auf die Tabellen 2 und 3, in denen der Anteil sicherer Ausfälle in einen von vier Bereichen fällt (d. h. (< 60 %), (60 % bis < 90 %), (90 % bis < 99 %) und (≥ 99 %)). Alle SFF haben im gleichen Bereich zu liegen (z. B. alle im Bereich (90 % bis < 99 %)).

BEISPIEL 1 Um den maximal zulässigen Sicherheits-Integritätslevel zu bestimmen, der durch ein Teilsystem mit einer Hardwarefehlertoleranz von 1 für die festgelegte Sicherheitsfunktion erreicht worden ist, bei dem eine Element-Sicher-

heitsfunktion durch parallele Elemente ausgeführt wird, kann die folgende Methode angewendet werden, vorausgesetzt, das Teilsystem erfüllt die Anforderungen von 7.4.4.2.2. In diesem Beispiel sind alle Elemente vom Typ B, und die Anteile sicherer Ausfälle der Elemente liegen im Bereich von (90 % bis < 99 %).

Aus [Tabelle 3](#) ist ersichtlich, dass für eine Hardwarefehlertoleranz gleich 1, mit Anteilen sicherer Ausfälle für beide Elemente im Bereich von (90 % bis < 99 %), der maximal zulässige Sicherheits-Integritätslevel für die festgelegte Sicherheitsfunktion SIL 3 beträgt.

BEISPIEL 2 Um die erforderliche Hardwarefehlertoleranz für ein Teilsystem für die festgelegte Sicherheitsfunktion zu bestimmen, bei dem eine Element-Sicherheitsfunktion durch parallele Elemente ausgeführt wird, kann die folgende Methode angewendet werden, vorausgesetzt, das Teilsystem erfüllt die Anforderungen von 7.4.4.2.2. In diesem Beispiel sind alle Elemente vom Typ A, und die Anteile sicherer Ausfälle der Elemente liegen im Bereich von (60 % bis < 90 %). Der Sicherheits-Integritätslevel der Sicherheitsfunktion ist SIL 3.

Aus [Tabelle 2](#) ist ersichtlich, dass zum Erreichen der Anforderung von SIL 3 die erforderliche Hardwarefehlertoleranz gleich 1 sein muss. Dies bedeutet, dass zwei parallele Elemente notwendig sind.

Tabelle 2 – Maximal zulässiger Sicherheits-Integritätslevel für eine Sicherheitsfunktion, die von einem sicherheitsbezogenen Typ A-Element oder Teilsystem ausgeführt wird

Anteil sicherer Ausfälle eines Elements	Hardwarefehlertoleranz		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % – < 90 %	SIL 2	SIL 3	SIL 4
90 % – < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

ANMERKUNG 1 Diese Tabelle wird in Verbindung mit 7.4.4.2.1 und 7.4.4.2.2 für die Festlegung des maximalen SIL verwendet, der für ein Teilsystem bei gegebener Fehlertoleranz des Teilsystems und SFF der verwendeten Elemente in Anspruch genommen werden kann.

i Für allgemeine Anwendung auf irgendein Teilsystem siehe 7.4.4.2.1.

ii Für Anwendung auf Teilsysteme, die Elemente enthalten, die die speziellen Anforderungen von 7.4.4.2.2 erfüllen. Um zu beanspruchen, dass ein Teilsystem einen speziellen SIL direkt nach dieser Tabelle erfüllt, ist es notwendig, alle Anforderungen in 7.4.4.2.2 zu erfüllen.

ANMERKUNG 2 Die Tabelle kann in Verbindung mit 7.4.4.2.1 und 7.4.4.2.2 auch verwendet werden:

i für die Festlegung der Anforderungen an die Hardwarefehlertoleranz für ein Teilsystem bei gegebenem SIL der Sicherheitsfunktion und gegebenen SFFs der zu verwendenden Elemente;

ii für die Festlegung der SFF-Anforderungen an Elemente bei gegebenem erforderlichen SIL der Sicherheitsfunktion und gegebener Hardwarefehlertoleranz des Teilsystems.

ANMERKUNG 3 Die Anforderungen in 7.4.4.2.3 und 7.4.4.2.4 beruhen auf den in dieser Tabelle und [Tabelle 3](#) festgelegten Daten.

ANMERKUNG 4 Siehe [Anhang C](#) zu Einzelheiten bezüglich der Berechnung des Anteils sicherer Ausfälle.