

	DIN EN 61508-1 (VDE 0803-1)	
	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 61508-1 (VDE 0803-1):2002-11 Siehe Anwendungsbeginn Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen (IEC 61508-1:2010); Deutsche Fassung EN 61508-1:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements (IEC 61508-1:2010); German version EN 61508-1:2010 Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales (CEI 61508-1:2010); Version allemande EN 61508-1:2010 Gesamtumfang 74 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 61508-1 (VDE 0803-1):2002-11 noch bis 2013-05-01 angewendet werden.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 61508-1 (VDE 0803-1):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 61508-1 (VDE 0803-1):2002-11 wurden folgende Änderungen vorgenommen:

- a) Hinweis auf die IT-Sicherheit zum Erreichen der funktionalen Sicherheit im Rahmen der Gefährdungs- und Risikoanalyse;
- b) Anhang B „Kompetenz von Personen“ wurde mit Änderungen in den Abschnitt 6 „Management der funktionalen Sicherheit“ verschoben;
- c) Ersatz von „Sicherheitsbezogenes System anderer Technologie“ und „externe Einrichtung zur Risikominderung“ durch „andere risikoreduzierende Maßnahmen“;
- d) Aufnahme der neuen Lebenszyklusphase „Spezifikation der Anforderungen an die Sicherheit des E/E/PE-Systems“;
- e) Ausschluss von Medizingeräten (IEC 60601) im Anwendungsbereich (gilt für die Teile 1 bis 3).

Frühere Ausgaben

DIN EN 61508-1 (VDE 0803-1): 2002-11

Nationaler Anhang NA (informativ)

Zusammenhang mit Europäischen und Internationalen Normen

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

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

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

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
EN 60300-3-1:2004	IEC 60300-3-1:2003	DIN EN 60300-3-1:2005-05	–
–	IEC 60300-3-9:1995	–	–
EN 60601 (alle Teile)	IEC 60601 (alle Teile)	DIN EN 60601 (VDE 0750-1) (alle Teile)	VDE 0750-1
EN 61326-3-1	IEC 61326-3-1	DIN EN 61326-3-1 (VDE 0843-20-3-1)	VDE 0843-20-3-1
EN 61355-1 (alle Teile)	IEC 61355 (alle Teile)	DIN EN 61355 (VDE 0040-3) (alle Teile)	VDE 0040-3
EN 61508-2:2010	IEC 61508-2:2010	DIN EN 61508-2 (VDE 0803-2):2011-02	VDE 0803-2
EN 61508-3:2010	IEC 61508-3:2010	DIN EN 61508-3 (VDE 0803-3):2011-02	VDE 0803-3
EN 61508-4:2010	IEC 61508-4:2010	DIN EN 61508-4 (VDE 0803-4):2011-02	VDE 0803-4
EN 61508-5:2010	IEC 61508-5:2010	DIN EN 61508-5 (VDE 0803-5):2011-02	VDE 0803-5
EN 61508-6:2010	IEC 61508-6:2010	DIN EN 61508-6 (VDE 0803-6):2011-02	VDE 0803-6
EN 61508-7:2010	IEC 61508-7:2010	DIN EN 61508-7 (VDE 0803-7):2011-02	VDE 0803-7
EN 61511 (alle Teile)	IEC 61511 (alle Teile)	DIN EN 61511 (VDE 0810-1) (alle Teile)	VDE 0810-1
EN 61800-5-2	IEC 61800-5-2	DIN EN 61800-5-2 (VDE 0160-105-2)	VDE 0160-105-2
EN 62061	IEC 62061	DIN EN 62061 (VDE 0113-50)	VDE 0113-50
–	IEC 62443 (alle Teile)	–	–
–	IEC 61506:1997	–	–

Tabelle NA.1 (fortgesetzt)

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
–	IEC 61882:2001	–	–
–	IEC Guide 104:1997	–	–
–	IEC/TR 61508-0:2005	DIN EN 61508 Beiblatt 1 (VDE 0803 Beiblatt 1):2005-10	VDE 0803 Beiblatt 1
–	IEC/TS 61000-1-2	–	–
–	ISO 8613-1:1994	–	–
–	ISO/IEC Guide 51:1999	–	–
–	ISO/IEC/TR 19791	–	–

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN 60300-3-1:2005-05, *Zuverlässigkeitsmanagement – Teil 3-1: Anwendungsleitfaden – Verfahren zur Analyse der Zuverlässigkeit – Leitfaden zur Methodik (IEC 60300-3-1:2003); Deutsche Fassung EN 60300-3-1:2004*

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

DIN EN 61326-3-1 (VDE 0843-20-3-1), *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*

DIN EN 61355-1 (VDE 0040-3) (alle Teile), *Klassifikation und Kennzeichnung von Dokumenten für Anlagen, Systeme und Ausrüstungen*

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

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

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

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

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

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

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

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

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

DIN EN 61508 Beiblatt 1 (VDE 0803 Beiblatt 1):2005-10, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 0: Funktionale Sicherheit und die IEC 61508 (IEC/TR 61508-0:2005)*

– Leerseite –

Funktionale Sicherheit sicherheitsbezogener
elektrischer/elektronischer/programmierbarer elektronischer Systeme –
Teil 1: Allgemeine Anforderungen
(IEC 61508-1:2010)

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

Sécurité fonctionnelle des systèmes
électriques/électroniques/électroniques
programmables relatifs à la sécurité –
Partie 1: Exigences générales
(CEI 61508-1:2010)

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 61508-1:2010 D

Vorwort

Der Text des Schriftstücks 65A/548/FDIS, zukünftige 2. Ausgabe von IEC 61508-1, 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 61508-1 angenommen.

Diese Europäische Norm ersetzt EN 61508-1:2001.

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 61508-1:2010 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.
[5] IEC 61508-6:2010	ANMERKUNG	Harmonisiert als EN 61508-6:2010 (nicht modifiziert).
[6] IEC 61508-7:2010	ANMERKUNG	Harmonisiert als EN 61508-7:2010 (nicht modifiziert).
[10] IEC 60300-3-1:2003	ANMERKUNG	Harmonisiert als EN 60300-3-1:2004 (nicht modifiziert).
[15] IEC 61326-3-1	ANMERKUNG	Harmonisiert als EN 61326-3-1.
[17] IEC 61355 Reihe	ANMERKUNG	Harmonisiert in der Reihe EN 61355 (nicht modifiziert).
[18] IEC 60601 Reihe	ANMERKUNG	Harmonisiert in der Reihe EN 60601 (teilweise modifiziert).
[20] IEC 61508-5:2010	ANMERKUNG	Harmonisiert als EN 61508-5:2010 (nicht modifiziert).

Inhalt

	Seite
Vorwort.....	2
Einleitung	5
1 Anwendungsbereich	7
2 Normative Verweisungen	10
3 Begriffe und Abkürzungen	10
4 Übereinstimmung mit dieser Norm	10
5 Dokumentation	11
5.1 Ziele	11
5.2 Anforderungen	11
6 Management der funktionalen Sicherheit.....	12
6.1 Ziele	12
6.2 Anforderungen	12
7 Anforderungen an den Gesamt-Sicherheitslebenszyklus	15
7.1 Allgemeines	15
7.2 Konzept.....	27
7.3 Definition des gesamten Anwendungsbereiches	28
7.4 Gefährdungs- und Risikoanalyse	28
7.5 Anforderungen an die Gesamtsicherheit.....	31
7.6 Zuordnung der Anforderungen an die Gesamtsicherheit	33
7.7 Planung des Gesamtbetriebs und der Gesamtinstandhaltung.....	38
7.8 Planung der Validierung der Gesamtsicherheit.....	40
7.9 Planung der Gesamtinstallation und Gesamtinbetriebnahme	41
7.10 Spezifikation der Anforderungen an die Sicherheit des E/E/PE-Systems	42
7.11 Sicherheitsbezogene E/E/PE-Systeme – Realisierung	45
7.12 Andere risikomindernde Maßnahmen – Spezifikation und Realisierung	45
7.13 Gesamtinstallation und Gesamtinbetriebnahme	45
7.14 Validierung der Gesamtsicherheit	46
7.15 Gesamtbetrieb, Gesamtinstandhaltung und Gesamtreparatur	47
7.16 Gesamtmodifikation und Gesamtnachrüstung	50
7.17 Außerbetriebnahme oder Ausmusterung	53
7.18 Verifikation	54
8 Beurteilung der funktionalen Sicherheit.....	54
8.1 Ziel	54
8.2 Anforderungen	54
Anhang A (informativ) Beispiel einer Dokumentationsstruktur	59
A.1 Allgemeines	59
A.2 Dokumentenstruktur für den Sicherheitslebenszyklus	60

	Seite
A.3 Physikalische Dokumentenstruktur.....	64
A.4 Liste der Dokumente.....	65
Literaturhinweise	66
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen.....	68
 Bilder	
Bild 1 – Gesamtrahmen der Normenreihe IEC 61508	9
Bild 2 – Gesamt-Sicherheitslebenszyklus.....	17
Bild 3 – Sicherheitslebenszyklus des E/E/PE-Systems (in der Realisierungsphase).....	18
Bild 4 – Software-Sicherheitslebenszyklus (in der Realisierungsphase)	18
Bild 5 – Verhältnis des Gesamt-Sicherheitslebenszyklus zu dem Sicherheitslebenszyklus des E/E/PE-Systems und dem Software-Sicherheitslebenszyklus	19
Bild 6 – Zuordnung der Anforderungen an die Gesamtsicherheit zu den sicherheitsbezogenen E/E/PE-Systemen und anderen risikomindernden Maßnahmen	35
Bild 7 – Beispiel eines Modells der Betriebs- und Instandhaltungstätigkeiten.....	49
Bild 8 – Beispiel eines Modells des Betriebs- und Instandhaltungsmanagements.....	50
Bild 9 – Beispiel eines Modells eines Modifikationsverfahrens.....	52
Bild A.1 – Strukturierung von Informationen für Anwendergruppen in Sätze von Dokumenten	64
 Tabellen	
Tabelle 1 – Gesamt-Sicherheitslebenszyklus – Übersicht.....	20
Tabelle 2 – Sicherheits-Integritätslevel – Ausfallgrenzwerte für eine Sicherheitsfunktion, die in der Betriebsart mit niedriger Anforderungsrate betrieben wird	36
Tabelle 3 – Sicherheits-Integritätslevel – Ausfallgrenzwerte für eine Sicherheitsfunktion, die in der Betriebsart mit hoher Anforderungsrate oder in der Betriebsart mit kontinuierlicher Anforderung betrieben wird	37
Tabelle 4 – Minimale Unabhängigkeitsgrade derjenigen Personen, die die Beurteilung der funktionalen Sicherheit ausführen (Phasen 1 bis 8 und 12 bis einschließlich 16 des Gesamt- Sicherheitslebenszyklus (siehe Bild 2))	58
Tabelle 5 – Minimale Unabhängigkeitsgrade derjenigen Personen, die die Beurteilung der funktionalen Sicherheit ausführen (Phasen 9 und 10 des Gesamt-Sicherheitslebenszyklus einschließlich aller Phasen des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus (siehe Bilder 2, 3 und 4))	58
Tabelle A.1 – Beispiel einer Dokumentationsstruktur für Informationen mit Bezug auf den Gesamt- Sicherheitslebenszyklus	61
Tabelle A.2 – Beispiel einer Dokumentationsstruktur für Informationen mit Bezug auf den Sicherheitslebenszyklus des E/E/PE-Systems	62
Tabelle A.3 – Beispiel einer Dokumentationsstruktur für Informationen mit Bezug auf den Software- Sicherheitslebenszyklus	63

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 einkanale 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 1: Allgemeine Anforderungen

1 Anwendungsbereich

1.1 Diese Internationale Norm behandelt diejenigen Gesichtspunkte, die zu betrachten sind, wenn elektrische/elektronische/programmierbare elektronische (E/E/PE) Systeme zur Ausführung von Sicherheitsfunktionen eingesetzt werden. Ein Hauptziel dieser Norm ist es, die Entwicklung produkt- und anwendungsspezifischer Internationaler Normen durch die für ein Produkt- und Anwendungsgebiet verantwortlichen Technischen Komitees zu unterstützen. Dies wird es erlauben, alle wichtigen, mit dem Produkt oder der Anwendung verbundenen Einflussgrößen vollständig zu berücksichtigen und damit den speziellen Erfordernissen der Produktanwender und des Anwendungsgebietes nachzukommen. Ein zweites Ziel dieser Norm ist es, die Entwicklung sicherheitsbezogener E/E/PE-Systeme zu ermöglichen, für die keine produkt- oder anwendungsspezifischen Internationalen Normen bestehen.

1.2 Insbesondere:

- a) gilt diese Norm für sicherheitsbezogene Systeme, wenn eines oder mehrere dieser Systeme elektrische/elektronische/programmierbare elektronische Elemente enthalten;

ANMERKUNG 1 Für einfache sicherheitsbezogene E/E/PE-Systeme können bestimmte, in dieser Norm festgelegte Anforderungen unnötig sein, und eine Befreiung von der Normerfüllung in Bezug auf solche Anforderungen ist möglich (siehe 4.2 und Definition eines einfachen sicherheitsbezogenen E/E/PE-Systems in IEC 61508-4, 3.4.3).

ANMERKUNG 2 Obwohl eine Person ein Teil eines sicherheitsbezogenen Systems sein kann (siehe IEC 61508-4, 3.4.1), werden Anforderungen an menschliche Faktoren in Bezug auf den Entwurf der sicherheitsbezogenen E/E/PE-Systeme in dieser Norm nicht im Detail betrachtet.

- b) ist diese Norm allgemeingültig und auf alle sicherheitsbezogenen E/E/PE-Systeme, unabhängig von der Anwendung, anwendbar;
- c) behandelt diese Norm das Erreichen eines tolerierbaren Risikos durch Anwendung sicherheitsbezogener E/E/PE-Systeme, aber sie behandelt nicht Gefährdungen, die von der E/E/PE-Einrichtung selbst ausgehen (zum Beispiel elektrischer Schlag);
- d) gilt diese Norm für alle Typen sicherheitsbezogener E/E/PE-Systeme, einschließlich Schutzsysteme und Leit- oder Steuerungssysteme;
- e) behandelt diese Norm nicht E/E/PE-Systeme, bei denen:
- ein einzelnes E/E/PE-System allein fähig ist, das tolerierbare Risiko zu erreichen; und
 - die erforderliche Sicherheitsintegrität der Sicherheitsfunktionen des einzelnen E/E/PE-Systems geringer als die Sicherheitsintegrität ist, die für den Sicherheits-Integritätslevel 1 (den geringsten Sicherheits-Integritätslevel in dieser Norm) festgelegt ist;
- f) befasst sich diese Norm hauptsächlich mit den sicherheitsbezogenen E/E/PE-Systemen, deren Ausfall einen Einfluss auf die Sicherheit von Personen und/oder die Umwelt haben könnte – es ist jedoch bekannt, dass die Auswirkungen von Ausfällen auch ernsthafte wirtschaftliche Auswirkungen haben können. In solchen Fällen kann diese Norm verwendet werden, um ein beliebiges E/E/PE-System, das zum Schutz von Einrichtungen oder Produkten verwendet wird, festzulegen;

ANMERKUNG 3 Siehe IEC 61508-4, 3.1.1.

- g) betrachtet diese Norm sicherheitsbezogene E/E/PE-Systeme und andere risikomindernde Maßnahmen, damit die Spezifikation der Anforderungen an die Sicherheit für die sicherheitsbezogenen E/E/PE-Systeme in einer systematischen, risikoorientierten Art und Weise festgelegt werden kann;
- h) verwendet diese Norm als technischen Rahmen das Modell eines Gesamt-Sicherheitslebenszyklus, um diejenigen Tätigkeiten systematisch zu behandeln, die für die Sicherstellung der funktionalen Sicherheit der sicherheitsbezogenen E/E/PE-Systeme notwendig sind;

ANMERKUNG 4 Obwohl der Gesamt-Sicherheitslebenszyklus vornehmlich mit sicherheitsbezogenen E/E/PE-Systemen befasst ist, kann er auch einen technischen Rahmen für die Betrachtung eines beliebigen sicherheitsbezogenen Systems liefern ungeachtet der Technologie dieses Systems (zum Beispiel Mechanik, Hydraulik oder Pneumatik).

- i) legt diese Norm nicht die Sicherheits-Integritätslevel für spezifische Anwendungen (welche sich auf ausführliche Informationen und Kenntnis über die spezifische Anwendung stützen müssen) fest. Die für die spezifischen Anwendungen verantwortlichen technischen Komitees müssen, wenn dies angebracht ist, die Sicherheits-Integritätslevel in anwendungsspezifischen Normen festlegen;
- j) liefert diese Norm allgemeine Anforderungen für sicherheitsbezogene E/E/PE-Systeme, für die keine produkt- oder anwendungsspezifischen Internationale Normen vorhanden sind;
- k) fordert diese Norm, dass boshafte und nicht autorisierte Handlungen während der Gefährdungs- und Risikoanalyse zu betrachten sind. Der Anwendungsbereich der Analyse schließt alle relevanten Phasen des Sicherheitslebenszyklus ein;

ANMERKUNG 5 Andere IEC/ISO-Normen betrachten dieses Thema gründlich, siehe ISO/IEC TR 19791 und die Normenreihe IEC 62443.

- l) enthält diese Norm nicht die Vorsichtsmaßnahmen, die notwendig sein können, um zu verhindern, dass unberechtigte Personen die funktionale Sicherheit von sicherheitsbezogenen E/E/PE-Systemen schädigen und/oder anderweitig ungünstig beeinflussen (siehe k) oben);
- m) legt diese Norm keine Anforderungen an Entwicklung, Ausführung, Pflege und/oder Anwendung von IT-Sicherheitsregeln oder IT-Sicherheitsdiensten fest, die benötigt werden, um eine IT-Sicherheitsregel zu erfüllen, die von dem sicherheitsbezogenen E/E/PE-System gefordert sein könnte;
- n) trifft diese Norm nicht auf medizinische Einrichtungen gemäß der Normenreihe IEC 60601 zu.

1.3 Dieser Teil der Normenreihe IEC 61508 beinhaltet die allgemeinen Anforderungen, die auf alle Teile anwendbar sind. Andere Teile der Normenreihe IEC 61508 konzentrieren sich mehr auf spezifische Themen:

- Die Teile 2 und 3 enthalten zusätzliche und besondere Anforderungen für sicherheitsbezogene E/E/PE-Systeme (für Hardware und Software);
- Teil 4 enthält Begriffe und Abkürzungen, die in der ganzen Norm verwendet werden;
- Teil 5 liefert anhand von Beispielen Hinweise für die Anwendung von Teil 1 zur Festlegung von Sicherheits-Integritätsleveln;
- Teil 6 liefert Hinweise für die Anwendung der Teile 2 und 3;
- Teil 7 enthält einen Überblick über Verfahren und Maßnahmen.

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

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

1.5 Bild 1 zeigt den Gesamtrahmen für die Normenreihe IEC 61508 und zeigt die Rolle, welche die IEC 61508-1 beim Erreichen der funktionalen Sicherheit für sicherheitsbezogene E/E/PE-Systeme spielt.

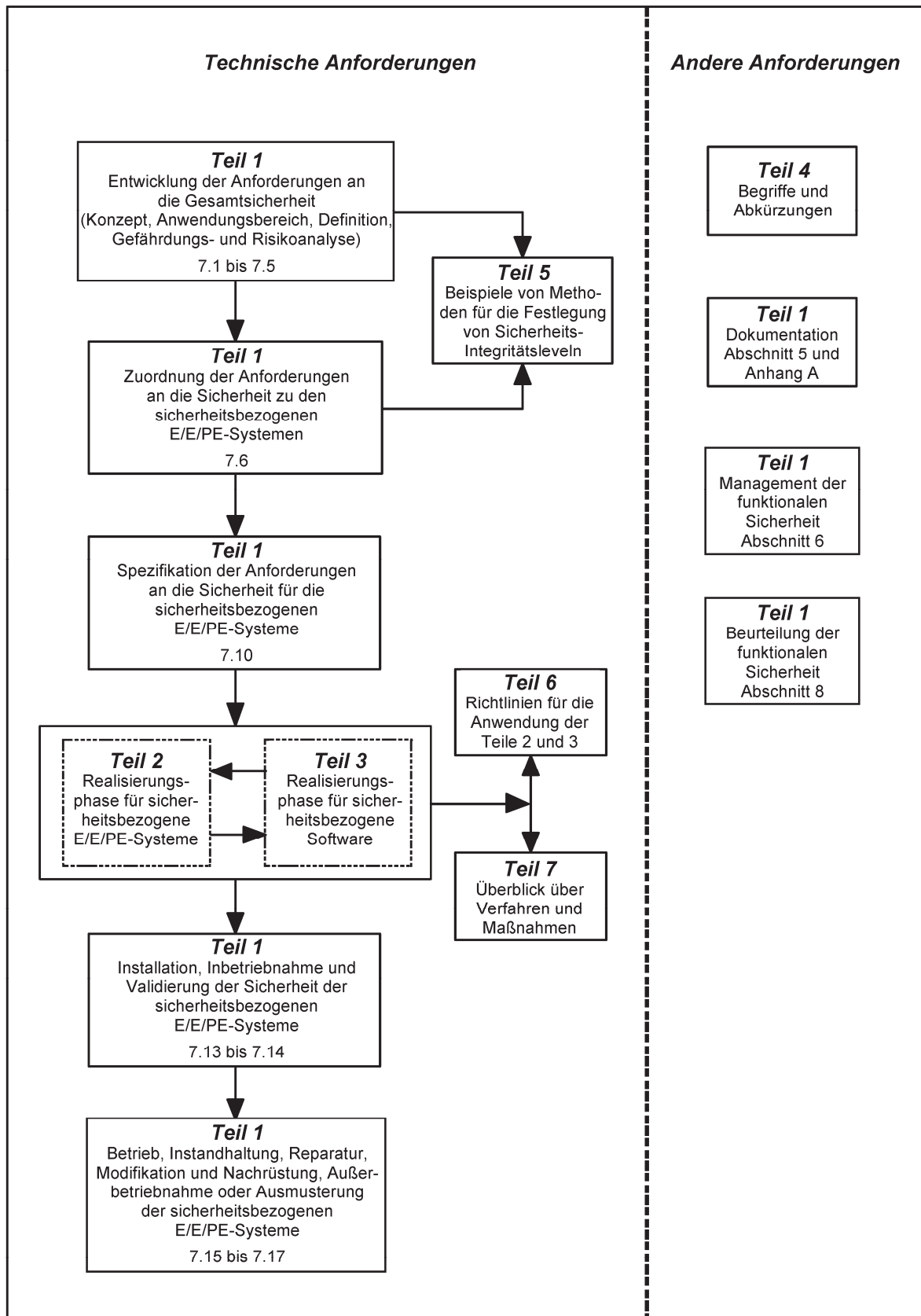


Bild 1 – Gesamtrahmen der Normenreihe IEC 61508

2 Normative Verweisungen

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

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

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

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

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*

3 Begriffe und Abkürzungen

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

4 Übereinstimmung mit dieser Norm

4.1 Um Übereinstimmung mit dieser Norm zu erreichen, muss dargelegt werden, dass alle relevanten Anforderungen entsprechend den erforderlichen festgelegten Kriterien (zum Beispiel der Sicherheits-Integritätslevel) erfüllt worden sind und somit die Ziele jedes Abschnitts oder Unterabschnitts erreicht worden sind.

4.2 Diese Norm legt die Anforderungen für sicherheitsbezogene E/E/PE-Systeme fest und ist erstellt worden, um den gesamten Komplexitätsbereich, der mit solchen Systemen verbunden ist, zu umfassen. Für einfache sicherheitsbezogene E/E/PE-Systeme (siehe IEC 61508-4, 3.4.3), für die verlässliche Felderfahrungen vorliegen, die das notwendige Vertrauen ergeben, dass die erforderliche Sicherheitsintegrität erreicht werden kann, sind jedoch die folgenden Alternativen vorhanden:

- in produkt- und anwendungsspezifischen Internationalen Normen, welche die Anforderungen von IEC 61508-1 bis IEC 61508-7 umsetzen, können bestimmte Anforderungen unnötig sein, und eine Befreiung von der Normerfüllung in Bezug auf solche Anforderungen ist akzeptabel;
- wird diese Norm in solchen Situationen, in denen keine produkt- oder anwendungsspezifische Internationale Norm vorhanden ist, direkt angewendet, so können bestimmte in dieser Norm festgelegte Anforderungen unnötig sein, und eine Befreiung von der Normerfüllung in Bezug auf solche Anforderungen ist akzeptabel, vorausgesetzt, dass diese begründet ist.

4.3 Produkt- und anwendungsspezifische Internationale Normen für sicherheitsbezogene E/E/PE-Systeme, die innerhalb des Rahmens dieser Norm entwickelt werden, müssen die Anforderungen von ISO/IEC Guide 51 und IEC Guide 104 berücksichtigen.

5 Dokumentation

5.1 Ziele

5.1.1 Das erste Ziel der Anforderungen dieses Abschnitts ist es, die notwendigen Informationen festzulegen, die dokumentiert werden müssen, damit alle Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus wirkungsvoll ausgeführt werden können.

5.1.2 Das zweite Ziel der Anforderungen dieses Abschnitts ist es, die zu dokumentierenden Informationen festzulegen, damit das Management der funktionalen Sicherheit (siehe [Abschnitt 6](#)), die Verifikation (siehe [7.18](#)) und die Beurteilung der funktionalen Sicherheit (siehe [Abschnitt 8](#)) wirkungsvoll ausgeführt werden können.

ANMERKUNG 1 In dieser Norm befassen sich Anforderungen zur Dokumentation im Wesentlichen mit Informationen und nicht mit deren Gestalt und Aussehen. Die Informationen müssen nicht in physikalischen Dokumenten vorhanden sein, es sei denn, dass dies ausdrücklich in dem entsprechenden Unterabschnitt erwähnt wird.

ANMERKUNG 2 Dokumentation kann in verschiedenen Formen vorhanden sein (zum Beispiel auf Papier, Film oder jedem Datenmedium, das auf Bildschirmen oder Anzeigeeinrichtungen dargestellt werden kann).

ANMERKUNG 3 Siehe [Anhang A](#) bezüglich möglicher Dokumentationsstrukturen.

ANMERKUNG 4 Siehe Hinweis [\[7\]](#) in den Literaturhinweisen.

5.2 Anforderungen

5.2.1 Die Dokumentation muss hinreichende Informationen zu jeder abgeschlossenen Phase des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus enthalten, welche für eine wirkungsvolle Erfüllung nachfolgender Phasen und Verifikationsstätigkeiten notwendig sind.

ANMERKUNG Der Umfang ausreichender Informationen hängt von einer Anzahl von Faktoren ab, welche die Komplexität, den Umfang von sicherheitsbezogenen E/E/PE-Systemen und die Anforderungen bezüglich der speziellen Anwendung einschließen.

5.2.2 Die Dokumentation muss hinreichende Informationen, die für das Management der funktionalen Sicherheit ([Abschnitt 6](#)) erforderlich sind, enthalten.

ANMERKUNG Siehe Anmerkungen zu 5.1.2.

5.2.3 Die Dokumentation muss hinreichende Informationen, die für die Ausführung einer Beurteilung der funktionalen Sicherheit erforderlich sind, enthalten, zusammen mit den Informationen und den Ergebnissen, die aus jeder Beurteilung der funktionalen Sicherheit abgeleitet wurden.

ANMERKUNG Siehe Anmerkungen zu 5.1.2.

5.2.4 Die zu dokumentierenden Informationen müssen, außer wenn anders begründet, so sein, wie es in den verschiedenen Abschnitten dieser Norm festgelegt ist, oder sie müssen dem entsprechen, was in produkt- oder anwendungsspezifischen Internationalen Normen, die für die Anwendung zutreffend sind, festgelegt ist.

5.2.5 Die Verfügbarkeit der Dokumentation muss für die Aufgaben, die im Hinblick auf die Abschnitte dieser Norm ausgeführt werden müssen, ausreichend sein.

ANMERKUNG Jede betroffene Partei braucht nur die Informationen zu besitzen, die notwendig sind, um eine besondere, nach dieser Norm erforderliche Tätigkeit auszuführen.

5.2.6 Die Dokumentation muss:

- genau und knapp sein;
- von denjenigen Personen, die sie verwenden müssen, einfach zu verstehen zu sein;
- den Zweck erfüllen, wofür sie erstellt worden ist;
- verfügbar und pflegbar sein.

5.2.7 Die Dokumentation oder der Informationssatz muss Titel oder Namen haben, die auf den Anwendungsbereich des Inhalts hinweisen, und eine Art von Registereinteilung, die einen sofortigen Zugriff auf die nach dieser Norm erforderlichen Informationen erlaubt.

5.2.8 Die Struktur der Dokumentation darf firmeneigene Verfahren und die Arbeitspraxis von speziellen Produkt- und Anwendungsbereichen berücksichtigen.

5.2.9 Die Dokumentation oder der Informationssatz muss einen Revisionsindex (Versionsnummern) haben, um die Identifizierung der verschiedenen Versionen eines Dokuments zu ermöglichen.

5.2.10 Die Dokumentation oder der Informationssatz muss entsprechend gegliedert werden, um die Suche nach relevanten Informationen zu ermöglichen. Es muss möglich sein, die letzte Revision (Version) eines Dokuments oder Informationssatzes zu identifizieren.

ANMERKUNG Die physikalische Struktur der Dokumentation kann aufgrund mehrerer Faktoren variieren, wie zum Beispiel des Umfangs eines Systems, seiner Komplexität und organisatorischer Anforderungen.

5.2.11 Alle relevanten Dokumente müssen unter einem angemessenen System der Dokumentenlenkung überarbeitet, geändert, überprüft und genehmigt werden.

ANMERKUNG Werden automatische oder halbautomatische Werkzeuge für die Erstellung der Dokumentation verwendet, können spezielle Verfahren notwendig sein, um sicherzustellen, dass effektive Maßnahmen für das Versionsmanagement oder anderer Kontrollaspekte der Dokumente vorhanden sind.

6 Management der funktionalen Sicherheit

6.1 Ziele

6.1.1 Das erste Ziel der Anforderungen dieses Abschnitts ist es, die Verantwortlichkeiten im Management der funktionalen Sicherheit derjenigen Personen festzulegen, die Verantwortung für ein sicherheitsbezogenes E/E/PE-System oder für eine oder mehrere Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus haben.

6.1.2 Das zweite Ziel der Anforderungen dieses Abschnitts ist es, die Tätigkeiten festzulegen, die von den Personen mit Verantwortung im Management der funktionalen Sicherheit auszuführen sind.

ANMERKUNG Die in diesem Abschnitt behandelten organisatorischen Maßnahmen sind für die wirksame Implementierung der technischen Anforderungen vorgesehen und sind ausschließlich auf das Erreichen und Bewahren der funktionalen Sicherheit der sicherheitsbezogenen E/E/PE-Systeme ausgerichtet. Die technischen Anforderungen, die zum Erhalt der funktionalen Sicherheit notwendig sind, werden als Teil der vom Hersteller des sicherheitsbezogenen E/E/PE-Systems und seiner Elemente und Bauteile gelieferten Informationen festgelegt.

6.2 Anforderungen

6.2.1 Eine Organisation mit Verantwortung für ein sicherheitsbezogenes E/E/PE-System oder für eine oder mehrere Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems oder des Software-Sicherheitslebenszyklus muss eine oder mehrere Personen bestimmen, die Gesamtverantwortung trägt/tragen für:

- das System und für seine Lebenszyklusphasen;
- die Koordination der sicherheitsbezogenen Tätigkeiten, die in diesen Phasen ausgeführt werden;

- die Schnittstellen zwischen diesen Phasen und anderen Phasen, die von anderen Organisationen ausgeführt werden;
- für die Umsetzung der Anforderungen aus 6.2.2 bis 6.2.11 und [6.2.13](#);
- die Koordination der Beurteilungen der funktionalen Sicherheit (siehe [6.2.12 b](#)) und [Abschnitt 8](#)) – insbesondere wo diejenigen Personen, die die Beurteilung der funktionalen Sicherheit ausführen, sich zwischen den Phasen unterscheiden – einschließlich Kommunikation, Planung und Integration der Dokumentation, der Beurteilungen und der Empfehlungen,
- die Sicherstellung, dass die funktionale Sicherheit in Übereinstimmung mit den Zielen und Anforderungen dieser Norm erreicht und aufgezeigt wird.

ANMERKUNG Verantwortung für sicherheitsbezogene Tätigkeiten oder für Phasen des Sicherheitslebenszyklus kann auf andere Personen, insbesondere auf solche mit relevantem Sachverstand, delegiert werden. Unterschiedliche Personen können für unterschiedliche Tätigkeiten und Anforderungen verantwortlich sein. Die Verantwortung für die Koordination und für die gesamte funktionale Sicherheit sollte jedoch bei einer Person oder einer geringen Anzahl von Personen liegen, die über genügend Managementautorität verfügen.

6.2.2 Die Vorgehensweise und die Strategie zum Erreichen der funktionalen Sicherheit müssen gemeinsam mit den Mitteln zur Bewertung ihrer Ausführung und den Mitteln, mit denen sie innerhalb der Organisation mitgeteilt werden, festgelegt werden.

6.2.3 Alle Personen, Abteilungen und Organisationen, die für die Ausführung von Tätigkeiten in den zutreffenden Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems oder des Software-Sicherheitslebenszyklus verantwortlich sind (einschließlich Personen, die für Verifikation und Beurteilung der funktionalen Sicherheit zuständig sind, und, wo zutreffend, Genehmigungsbehörden oder Sicherheitsüberwachungsorgane), müssen identifiziert werden und ihre Verantwortlichkeiten müssen ihnen vollständig und eindeutig mitgeteilt werden.

6.2.4 Es müssen Verfahren entwickelt werden zur Definition, welche Informationen zwischen relevanten Parteien mitgeteilt werden müssen und wie diese Kommunikation stattfindet.

ANMERKUNG Siehe [Abschnitt 5](#) zu Dokumentationsanforderungen.

6.2.5 Es müssen Verfahren entwickelt werden zur Sicherstellung einer unverzüglichen Verfolgung und zufriedenstellenden Lösung von Empfehlungen bezüglich der sicherheitsbezogenen E/E/PE-Systeme, einschließlich derer, die von Folgendem herrühren:

- a) Gefährdungs- und Risikoanalyse (siehe [7.4](#));
- b) Beurteilung der funktionalen Sicherheit (siehe [Abschnitt 8](#));
- c) Verifikationstätigkeiten (siehe [7.18](#));
- d) Validierungstätigkeiten (siehe [7.8](#) und [7.14](#));
- e) Konfigurationsmanagement (siehe [6.2.10](#), [7.16](#), IEC 61508-2 und IEC 61508-3);
- f) Bericht und Analyse von Zwischenfällen (siehe [6.2.6](#)).

6.2.6 Es müssen Verfahren entwickelt werden zur Sicherstellung, dass alle erkannten gefährlichen Vorfälle analysiert werden und dass Empfehlungen erfolgen, um die Wahrscheinlichkeit eines nochmaligen Auftretens zu minimieren.

6.2.7 Es müssen Anforderungen für wiederkehrende Audits der funktionalen Sicherheit festgelegt werden, einschließlich:

- a) der Häufigkeit der Audits der funktionalen Sicherheit;
- b) dem Grad der Unabhängigkeit derjenigen Personen, die die Audits durchführen;
- c) der notwendigen Dokumentation und nachfolgender Tätigkeiten.

6.2.8 Es müssen Verfahren entwickelt werden für:

- a) die Einleitung von Modifikationen der sicherheitsbezogenen E/E/PE-Systeme (siehe [7.16.2.2](#));
- b) den Erhalt von Zustimmung und Ermächtigung zu Modifikationen.

6.2.9 Es müssen Verfahren entwickelt werden für die Bewahrung genauer Informationen zu den Gefährdungen und gefährlichen Vorfällen, Sicherheitsfunktionen und sicherheitsbezogenen E/E/PE-Systemen.

6.2.10 Es müssen Verfahren entwickelt werden für das Konfigurationsmanagement der sicherheitsbezogenen E/E/PE-Systeme während der Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus, einschließlich insbesondere:

- a) dem Punkt, im Hinblick auf spezifische Phasen, an dem eine formale Konfigurationskontrolle ausgeführt werden muss;
- b) den Verfahren, die für eine eindeutige Identifikation aller Bestandteile eines Objekts (Hardware und Software) angewendet werden müssen;
- c) den Verfahren, um zu verhindern, dass nicht zugelassene Komponenten zum Einsatz kommen.

6.2.11 Wo angebracht müssen Training und Informationen für die Notfalldienste bereitgestellt werden.

6.2.12 Diejenigen Personen, die Verantwortung für eine oder mehrere Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems oder des Software-Sicherheitslebenszyklus haben, müssen im Hinblick auf diejenigen Phasen, für die sie Verantwortung haben, und in Übereinstimmung mit den in [6.2.1 bis 6.2.11](#) definierten Verfahren alle Managementtätigkeiten und technischen Tätigkeiten festlegen, die notwendig sind, um das Erreichen, das Darlegen und den Erhalt der funktionalen Sicherheit der sicherheitsbezogenen E/E/PE-Systeme sicherzustellen, einschließlich:

- a) der ausgewählten Maßnahmen und Methoden, die angewendet werden, um die Anforderungen eines speziellen Abschnitts oder Unterabschnitts zu erfüllen (siehe IEC 61508-2, IEC 61508-3 und IEC 61508-6);
- b) der Tätigkeiten zur Beurteilung der funktionalen Sicherheit und der Art und Weise, wie das Erreichen der funktionalen Sicherheit denjenigen Personen dargelegt wird, die die Beurteilung der funktionalen Sicherheit durchführen (siehe [Abschnitt 8](#));

ANMERKUNG Es sollten angemessene Verfahren für die Beurteilung der funktionalen Sicherheit verwendet werden, um Folgendes festzulegen:

- die Auswahl einer geeigneten Organisation, Person oder Personen mit einem angemessenen Grad von Unabhängigkeit;
 - das Entwerfen und das Ändern des Aufgabenbereiches für Beurteilungen der funktionalen Sicherheit;
 - die Auswechslung derjenigen Personen, die die Beurteilung der funktionalen Sicherheit ausführen, an irgendeinem Punkt des Lebenszyklus eines Systems;
 - die Lösung von Kontroversen bezogen auf diejenigen Personen, die die Beurteilungen der funktionalen Sicherheit ausführen.
- c) der Verfahren zur Analyse der Betriebs- und Instandhaltungsleistungsfähigkeit, insbesondere für:
- die Erkennung systematischer Fehler, welche die funktionale Sicherheit gefährden können, einschließlich der während routinemäßiger Instandhaltung verwendeten Verfahren, die wiederkehrende Fehler erkennen können;
 - die Beurteilung, ob die Anforderungsraten und die Ausfallraten während des Betriebs und der Instandhaltung mit den während des Entwurfs des Systems gemachten Annahmen übereinstimmen.

6.2.13 Es müssen Verfahren entwickelt werden, um sicherzustellen, dass alle Personen mit Verantwortlichkeiten gemäß [6.2.1](#) und [6.2.3](#) (d. h. einschließlich aller Personen, die an irgendeiner Tätigkeit des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems oder des Software-Sicherheitslebenszyklus, einschließlich der Tätigkeiten zur Verifikation, zum Management der funktionalen Sicherheit und zur Beurteilung der funktionalen Sicherheit, beteiligt sind) eine angemessene Kompetenz haben müssen (d. h. Ausbildung, technisches Wissen, Erfahrung und Qualifikationen) in Bezug auf die speziellen, von ihnen auszuführenden Aufgaben. Solche Verfahren müssen Anforderungen zur Auffrischung, Aktualisierung und fortlaufenden Beurteilung der Kompetenz einschließen.

6.2.14 Die Angemessenheit der Kompetenz muss in Bezug auf die jeweilige Anwendung unter Beachtung aller relevanten Faktoren betrachtet werden, einschließlich:

- a) der Verantwortlichkeiten der Personen;
- b) dem erforderlichen Grad der Aufsicht;
- c) den möglichen Auswirkungen beim Auftreten eines Ausfalls der sicherheitsbezogenen E/E/PE-Systeme – je größer die Auswirkungen, desto strenger muss die Festlegung der Kompetenz sein;
- d) der Sicherheits-Integritätslevel der sicherheitsbezogenen E/E/PE-Systeme – je höher die Sicherheits-Integritätslevel, desto strenger muss die Festlegung der Kompetenz sein;
- e) der Neuartigkeit des Entwurfs, der Entwurfsverfahren oder der Anwendung – je neuer oder unerprobter diese sind, desto strenger muss die Festlegung der Kompetenz sein;
- f) früherer Erfahrungen und ihrer Relevanz in Bezug auf die speziellen auszuführenden Aufgaben und der verwendeten Technologie – je größer die erforderliche Kompetenz, desto besser müssen die Kompetenzen aus früheren Erfahrungen zu den für die speziellen auszuführenden Tätigkeiten erforderlichen Kompetenzen passen;
- g) der Art der Kompetenz passend zu den Umständen (zum Beispiel Qualifikationen, Erfahrungen, relevante Ausbildung und nachfolgende Praxis, Führungsverhalten und Entscheidungsfähigkeiten);
- h) angemessener technischer Kenntnis für Anwendungsbereich und Technologie;
- i) angemessener sicherheitstechnischer Kenntnis der Technologie;
- j) Kenntnis des Rahmens der gesetzlichen Bestimmungen und der Sicherheitsbestimmungen;
- k) Relevanz der Qualifikationen in Bezug auf die speziellen auszuführenden Tätigkeiten.

ANMERKUNG Hinweis [8] in den Literaturhinweisen enthält ein Beispiel für die Handhabung der Kompetenz für sicherheitsbezogene E/E/PE-Systeme.

6.2.15 Die Kompetenz und Befähigung aller Personen mit Verantwortlichkeiten nach 6.2.1 und 6.2.3 muss dokumentiert werden.

6.2.16 Die als Ergebnis von 6.2.2 bis 6.2.15 festgelegten Tätigkeiten müssen ausgeführt und überwacht werden.

6.2.17 Lieferanten, die Produkte an eine Organisation mit Gesamtverantwortung für eine oder mehrere Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems oder des Software-Sicherheitslebenszyklus (siehe 6.2.1) liefern oder Dienstleistungen für sie erbringen, müssen Produkte oder Dienstleistungen nach den Festlegungen dieser Organisation liefern oder erbringen und müssen ein angemessenes Qualitätsmanagementsystem besitzen.

6.2.18 Tätigkeiten in Bezug auf das Management der funktionalen Sicherheit müssen in den relevanten Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems oder des Software-Sicherheitslebenszyklus angewendet werden (siehe 7.1.1.5).

7 Anforderungen an den Gesamt-Sicherheitslebenszyklus

7.1 Allgemeines

7.1.1 Einleitung

7.1.1.1 Diese Norm verwendet als technischen Rahmen einen Gesamt-Sicherheitslebenszyklus (siehe Bild 2), um auf systematische Art und Weise alle Tätigkeiten zu behandeln, die zum Erreichen der erforderlichen Sicherheitsintegrität für die Sicherheitsfunktionen, die von den sicherheitsbezogenen E/E/PE-Systemen ausgeführt werden, notwendig sind.

ANMERKUNG Für den Anspruch auf Übereinstimmung mit dieser Norm sollte der Gesamt-Sicherheitslebenszyklus als Grundlage verwendet werden. Es kann jedoch ein von dem im [Bild 2](#) gezeigten verschiedener Gesamt-Sicherheitslebenszyklus verwendet werden, vorausgesetzt, die Ziele und Anforderungen jedes Abschnitts dieser Norm werden erfüllt.

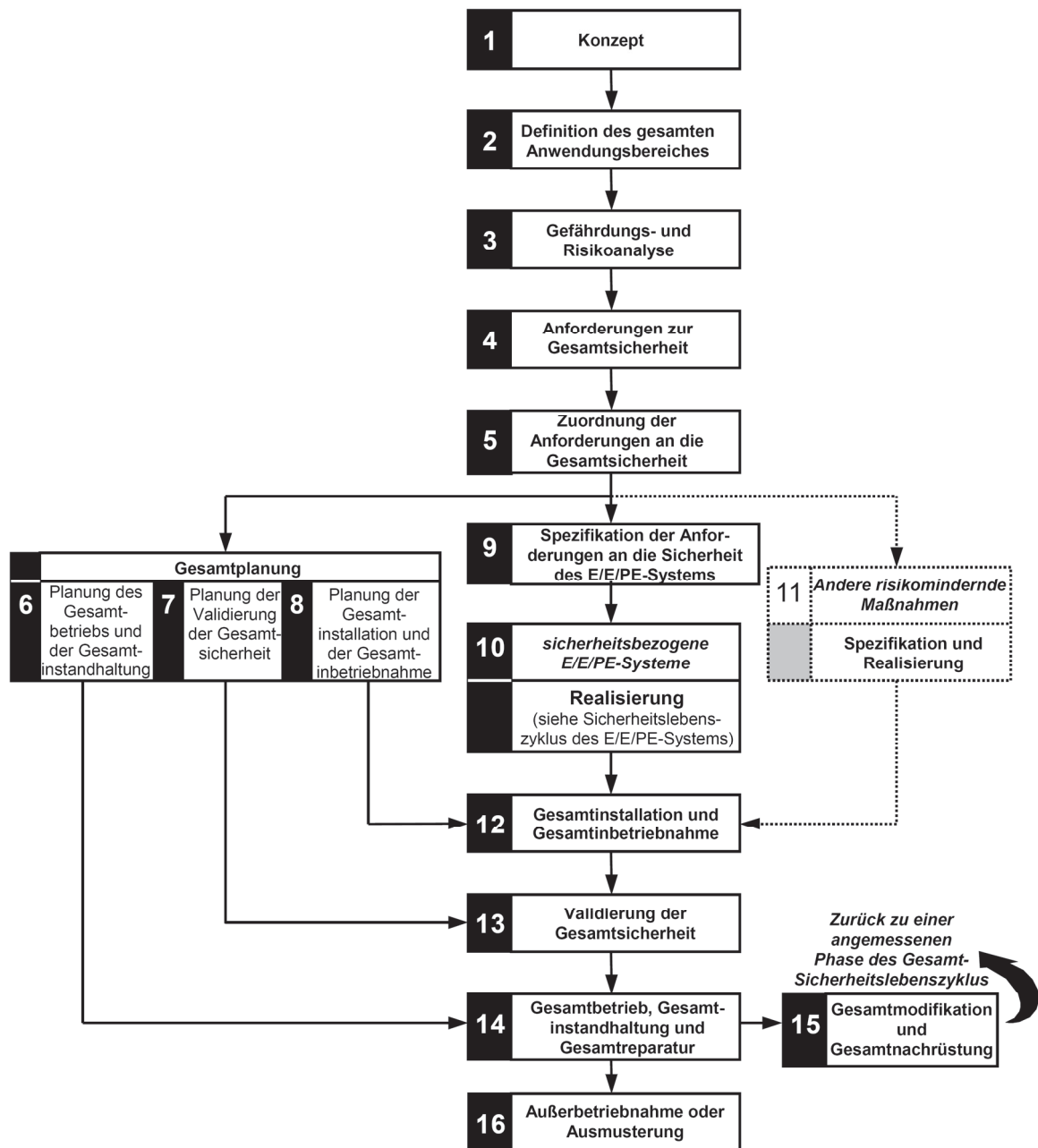
7.1.1.2 Der Gesamt-Sicherheitslebenszyklus enthält folgende Mittel zum Erreichen des tolerierbaren Risikos:

- sicherheitsbezogene E/E/PE-Systeme;
- andere risikomindernde Maßnahmen.

7.1.1.3 Die Realisierungsphase der sicherheitsbezogenen E/E/PE-Systeme aus dem Gesamt-Sicherheitslebenszyklus wird erweitert und in [Bild 3](#) gezeigt. Dieser Teil des Sicherheitslebenszyklus des E/E/PE-Systems bildet den technischen Gesamtrahmen für IEC 61508-2. Der in [Bild 4](#) gezeigte Teil des Software-Sicherheitslebenszyklus bildet den technischen Gesamtrahmen für IEC 61508-3. Die Beziehung des Gesamt-Sicherheitslebenszyklus zum Sicherheitslebenszyklus des E/E/PE-Systems und zum Software-Sicherheitslebenszyklus für sicherheitsbezogene Systeme wird in [Bild 5](#) gezeigt.

7.1.1.4 Die Abbildungen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus ([Bilder 2 bis 4](#)) sind vereinfachte Betrachtungen der Realität und zeigen als solche nicht alle Iterationen bezüglich der speziellen Phasen oder Zwischenphasen. Iterationen sind aber innerhalb des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus ein notwendiger und wichtiger Teil der Entwicklung.

7.1.1.5 Tätigkeiten in Bezug auf das Management der funktionalen Sicherheit ([Abschnitt 6](#)), Verifikation ([7.18](#)) und Beurteilung der funktionalen Sicherheit ([Abschnitt 8](#)) werden in dem Gesamt-Sicherheitslebenszyklus, dem Sicherheitslebenszyklus des E/E/PE-Systems oder dem Software-Sicherheitslebenszyklus nicht gezeigt. Dies erfolgte, um die Komplexität der Bilder der Sicherheitslebenszyklen zu reduzieren. Diese Tätigkeiten müssen, wo erforderlich, in den relevanten Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus ausgeführt werden.



ANMERKUNG 1 Tätigkeiten in Bezug auf **Verifikation, Management der funktionalen Sicherheit** und **Beurteilung der funktionalen Sicherheit** sind zur besseren Übersicht nicht gezeigt, gehören jedoch zu allen Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus.

ANMERKUNG 2 Die durch den Kasten 11 dargestellte Phase liegt außerhalb des Anwendungsbereiches dieser Norm.

ANMERKUNG 3 IEC 61508-2 und IEC 61508-3 behandeln Kasten 10 (Realisierung), sie beschäftigen sich jedoch auch, wo zutreffend, mit Aspekten der programmierbaren Elektronik (Hardware und Software) der Kästen 13, 14 und 15.

ANMERKUNG 4 Siehe [Tabelle 1](#) für eine Beschreibung der Ziele und des Anwendungsbereiches der durch jeden Kasten dargestellten Phase.

ANMERKUNG 5 Die zum Gesamtbetrieb, zur Gesamtinstandhaltung, Gesamtreparatur, Gesamtmodifikation, Gesamtnachrüstung und Außerbetriebnahme oder Ausmusterung notwendigen technischen Anforderungen werden als Teil der vom Hersteller des sicherheitsbezogenen E/E/PE-Systems und seiner Elemente und Bauteile gelieferten Informationen festgelegt.

Bild 2 – Gesamt-Sicherheitslebenszyklus