

	Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/programmierbarer elektronischer Systeme Teil 1: Allgemeine Anforderungen (IEC 61508-1:1998 + Corrigendum 1999) Deutsche Fassung EN 61508-1:2001	<u>DIN</u> EN 61508-1
VDE	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Vorstand beschlossenen Genehmigungsverfahrens unter nebenstehenden Nummern in das VDE-Vorschriftenwerk aufgenommen und in der etz Elektrotechnische Zeitschrift bekannt gegeben worden.	Klassifikation VDE 0803 Teil 1
ICS 25.040.40 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements (IEC 61508-1:1998 + corrigendum 1999); German version EN 61508-1:2001 Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Prescriptions générales (CEI 61508-1:1998 + corrigendum 1999); Version allemande EN 61508-1:2001 Die Europäische Norm EN 61508-1:2001 hat den Status einer Deutschen Norm. Beginn der Gültigkeit Die EN 61508-1 wurde am 2001-07-03 angenommen. Nationales Vorwort Für die vorliegende 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 zuständig. Norm-Inhalt war veröffentlicht als E DIN IEC 65A/179/CDV (VDE 0801 Teil 1):1995-12. Die enthaltene IEC-Publikation wurde vom SC 65A „System aspects“ erarbeitet. Sie ist eine Sicherheits-Grundnorm, siehe hierzu auch Unterabschnitt 1.4. Fortsetzung Seite 2 und 3 und 59 Seiten EN DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

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

Die Vornormen

DIN V VDE 0801 (VDE 0801):1990-01 Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben

DIN V VDE 0801/A1 (VDE 0801/A1):1994-10 Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben;
Änderung 1:1994-10

DIN V 19250:1994-05 Leittechnik – Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen
und

DIN V 19251:1995-02 Leittechnik – MSR-Schutzeinrichtungen – Anforderungen und Maßnahmen zur
gesicherten Funktion

enthalten Festlegungen, die den Festlegungen in den Normen der Reihe DIN EN 61508 (VDE 0803)
entgegenstehen oder zu ihnen redundant sind.

Die DKE beabsichtigt daher, die oben genannten Vornormen zum 01. August 2004 zurückzuziehen.

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.

Der Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ist nachstehend wiedergegeben. Zum Zeitpunkt der Veröffentlichung dieser Norm waren die angegebenen Ausgaben gültig.

IEC hat 1997 die Benummerung der IEC-Publikationen geändert. Zu den bisher verwendeten Normnummern wird jeweils 60000 addiert. So ist zum Beispiel aus IEC 68 nun IEC 60068 geworden.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
EN 61508-2:2001	IEC 61508-2:2000	DIN EN 61508-2 (VDE 0803 Teil 2): in Vorbereitung	VDE 0803 Teil 2
EN 61508-3:2001	IEC 61508-3:1998	DIN EN 61508-3 (VDE 0803 Teil 3): in Vorbereitung	VDE 0803 Teil 3
EN 61508-4:2001	IEC 61508-4:1998	DIN EN 61508-4 (VDE 0803 Teil 4):2002-11	VDE 0803 Teil 4
EN 61508-5:2001	IEC 61508-5:1998	DIN EN 61508-5 (VDE 0803 Teil 5):2002-11	VDE 0803 Teil 5
EN 61508-6:2001	IEC 61508-6:2000	DIN EN 61508-6 (VDE 0803 Teil 6): in Vorbereitung	VDE 0803 Teil 6
EN 61508-7:2001	IEC 61508-7:2000	DIN EN 61508-7 (VDE 0803 Teil 7): in Vorbereitung	VDE 0803 Teil 7
–	IEC Guide 104:1997	–	–
–	ISO/IEC Guide 51: 1990	DIN 820-120:2001-10	–

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN 820-120, *Normungsarbeit – Teil 120: Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen (ISO/IEC-Guide 51:1999)*.

DIN EN 61508-2 (VDE 0803 Teil 2), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme.*

DIN EN 61508-3 (VDE 0803 Teil 3), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software (IEC 61508-3:1998 + Corrigendum 1999); Deutsche Fassung EN 61508-3:2001.*

DIN EN 61508-4 (VDE 0803 Teil 4), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen (IEC 61508-4:1998 + Corrigendum 1999); Deutsche Fassung EN 61508-4:2001.*

DIN EN 61508-5 (VDE 0803 Teil 5), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level) (IEC 61508-5:1998); Deutsche Fassung EN 61508-5:2001.*

DIN EN 61508-6 (VDE 0803 Teil 6), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für die IEC 61508-2 und IEC 61508-3.*

DIN EN 61508-7 (VDE 0803 Teil 7), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 7: Anwendungshinweise über Verfahren und Maßnahmen.*

– Leerseite –

**Funktionale Sicherheit sicherheitsbezogener
elektrischer/elektronischer/programmierbarer elektronischer Systeme –
Teil 1: Allgemeine Anforderungen**
(IEC 61508-1:1998 + Corrigendum 1999)

Functional safety of
electrical/electronic/programmable electronic
safety-related systems –
Part 1: General requirements
(IEC 61508-1:1998 + corrigendum 1999)

Sécurité fonctionnelle des systèmes
électriques/électroniques/électroniques
programmables relatifs à la sécurité –
Partie 1: Prescriptions générales
(CEI 61508-1:1998 + corrigendum 1999)

Diese Europäische Norm wurde von CENELEC am 2001-07-03 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, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Portugal, Schweden, Schweiz, Spanien, der Tschechischen Republik und dem Vereinigten Königreich.

CENELEC

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

Zentralsekretariat: rue de Stassart 35, B-1050 Brüssel

Vorwort

Der Text der Internationalen Norm IEC 61508-1 einschließlich deren Corrigendum Mai 1999, ausgearbeitet von dem SC 65A "System aspects" des IEC TC 65 "Industrial-process measurement and control", wurde dem Einstufigen Annahmeverfahren unterworfen und von CENELEC am 2001-07-03 ohne irgendeine Abänderung als EN 61508-1 angenommen.

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): 2002-08-01
- spätestes Datum, zu dem nationale Normen, die der EN entgegenstehen, zurückgezogen werden müssen (dow): 2004-08-01

Anhänge, die als "normativ" bezeichnet sind, gehören zum Norminhalt.

Anhänge, die als "informativ" bezeichnet sind, enthalten nur Informationen.

In dieser Norm ist Anhang ZA normativ und sind die Anhänge A, B und C informativ.

Der Anhang ZA wurde von CENELEC hinzugefügt.

Die IEC 61508 ist eine Sicherheitsgrundnorm zur funktionalen Sicherheit von elektrischen, elektronischen und programmierbar elektronischen sicherheitsbezogenen Systemen. Der Anwendungsbereich lautet :

„Diese Internationale Norm behandelt diejenigen Gesichtspunkte, die zu betrachten sind, wenn elektrische/elektronische/programmierbar elektronische Systeme (E/E/PES) zur Ausführung von Sicherheitsfunktionen eingesetzt werden. Ein Hauptziel dieser Norm ist es, für ein bestimmtes Anwendungsgebiet die Entwicklung einer entsprechenden Internationalen Norm durch das jeweils verantwortliche Komitee zu ermöglichen. Dies wird es erlauben, alle wichtigen Einflussgrößen dieses Anwendungsgebietes vollständig zu berücksichtigen und damit dessen besonderen Erfordernissen nachzukommen. Ein zweites Ziel dieser Norm ist es, die Entwicklung eines elektrischen/ elektronischen/programmierbar elektronischen (E/E/PE) sicherheitsbezogenen Systemes für dessen Anwendungsgebiet noch keine Internationale Norm besteht, zu ermöglichen.“

Der CENELEC-Bericht R0BT-004, der auf der 103. Sitzung des technischen Büros im März 2000 angenommen wurde, geht davon aus, dass einige IEC-Normen, die bereits veröffentlicht sind oder gerade erarbeitet werden, Implementierung der IEC 61508 für ein bestimmtes Anwendungsgebiet darstellen, z. B.:

- IEC 61511, Functional safety – Safety instrumented systems for the process industry sector;
- IEC 62061, Safety of machinery – Functional safety of electrical, electronic and programmable electronic control systems;
- IEC 61513, Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems.

Für das Anwendungsgebiet des Eisenbahnwesens wurde ebenfalls eine Reihe Europäischer Normen erstellt (EN 50126; EN 50128 und prEN 50129).

ANMERKUNG EN 50126 und EN 50128 beruhen auf früheren Entwürfen der IEC 61508. prEN 50129 beruht auf den Grundsätzen der jetzt gültigen Fassung der IEC 61508.

Diese Aufzählung schließt nicht aus, dass weitere Implementierungen der IEC 61508 für bestimmte Anwendungsgebiete, die sich gerade in der Erarbeitung oder Veröffentlichung innerhalb IEC oder CENELEC befinden, erscheinen.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 61508-1:1998 einschließlich deren Corrigendum Mai 1999 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

Inhalt

	Seite
Einleitung	6
1 Anwendungsbereich	8
2 Normative Verweisungen	11
3 Begriffe und Abkürzungen	11
4 Übereinstimmung mit dieser Norm	11
5 Dokumentation	12
5.1 Ziele	12
5.2 Anforderungen	12
6 Management der funktionalen Sicherheit	13
6.1 Ziele	13
6.2 Anforderungen	14
7 Anforderungen zum gesamten Sicherheitslebenszyklus	15
7.1 Allgemeines	15
7.2 Konzept	25
7.3 Definition des gesamten Anwendungsbereiches	26
7.4 Gefährdungs- und Risikoanalyse	26
7.5 Gesamte Sicherheitsanforderungen	28
7.6 Zuordnung der Sicherheitsanforderungen	30
7.7 Planung des Gesamtbetriebs und der gesamten Instandhaltung	35
7.8 Planung der Sicherheits-Gesamtvalidierung	36
7.9 Planung der Gesamtinstallation und Gesamtinbetriebnahme	37
7.10 Realisierung: E/E/PES	38
7.11 Realisierung: Sicherheitsbezogene Systeme anderer Technologie	38
7.12 Realisierung: Externe Einrichtungen zur Risikominderung	38
7.13 Gesamtinstallation und Gesamtinbetriebnahme	39
7.14 Sicherheits-Gesamtvalidierung	39
7.15 Gesamtbetrieb, gesamte Instandhaltung und Reparatur	40
7.16 Gesamtmodifikation und gesamte Nachrüstung	43
7.17 Außerbetriebnahme oder Ausmusterung	45
7.18 Verifikation	46
8 Beurteilung der funktionalen Sicherheit	47
8.1 Ziel	47
8.2 Anforderungen	47
Anhang A (informativ) Beispiel einer Dokumentationsstruktur	50
A.1 Allgemeines	50
A.2 Dokumentenstruktur des Sicherheitslebenszyklus	51
A.3 Physikalische Dokumentenstruktur	54
A.4 Liste der Dokumente	55

	Seite
Anhang B (informativ) Kompetenz von Personen.....	57
B.1 Ziel	57
B.2 Allgemeine Überlegungen.....	57
Anhang C (informativ) Literaturhinweise	58
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen.....	59
Bilder	
Bild 1 – Gesamtrahmen dieser Norm.....	10
Bild 2 – Gesamter Sicherheitslebenszyklus	17
Bild 3 – E/E/PES-Sicherheitslebenszyklus (in der Realisierungsphase)	18
Bild 4 – Software-Sicherheitslebenszyklus (in der Realisierungsphase)	18
Bild 5 – Verhältnis des gesamten Sicherheitslebenszyklus zu den E/E/PES- und Software- Sicherheitslebenszyklen	19
Bild 6 – Zuordnung der Sicherheitsanforderungen zu den sicherheitsbezogenen E/E/PE-Systemen, sicherheitsbezogenen Systemen anderer Technologie und externen Einrichtungen zur Risikominderung	32
Bild 7 – Beispiel eines Modells der Betriebs- und Instandhaltungstätigkeiten.....	42
Bild 8 – Beispiel eines Modells des Betriebs- und Instandhaltungsmanagements.....	43
Bild 9 – Beispiel eines Modells der Modifikationsverfahren	45
Bild A.1 – Strukturierung von Informationen für Anwendergruppen in Sätze von Dokumenten	55
Bild A.2 – Strukturierung von Informationen großer komplexer Systeme und kleiner einfacher Systeme	55
Tabellen	
Tabelle 1 – Gesamter Sicherheitslebenszyklus: Übersicht.....	19
Tabelle 2 – Sicherheits-Integritätslevel: Ausfallgrenzwerte für eine Sicherheitsfunktion, die in der Betriebsart mit niedriger Anforderungsrate betrieben wird	33
Tabelle 3 – Sicherheits-Integritätslevel: Ausfallgrenzwerte für eine Sicherheitsfunktion, die in der Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung betrieben wird	33
Tabelle 4 – Minimale Unabhängigkeitsgrade der Personen, die die Beurteilung der funktionalen Sicherheit ausführen (Phasen 1 bis 8 und 12 bis einschließlich 16 des gesamten Sicherheitslebenszyklus (siehe Bild 2))	49
Tabelle 5 – Minimale Unabhängigkeitsgrade der Personen, die die Beurteilung der funktionalen Sicherheit ausführen (Phase 9 des gesamten Sicherheitslebenszyklus einschließlich aller Phasen des E/E/PES-Sicherheitslebenszyklus und des Software-Sicherheitslebenszyklus (siehe Bilder 2, 3 und 4)).....	49
Tabelle A.1 – Beispiel einer Dokumentationsstruktur für Informationen bezüglich des gesamten Sicherheitslebenszyklus.....	52
Tabelle A.2 – Beispiel einer Dokumentationsstruktur für Informationen bezüglich des E/E/PES- Sicherheitslebenszyklus.....	53
Tabelle A.3 – Beispiel einer Dokumentationsstruktur für Informationen bezüglich des Software- Sicherheitslebenszyklus.....	54

Einleitung

Systeme, die aus elektrischen und/oder elektronischen Bauteilen bestehen, werden seit vielen Jahren verwendet, um Sicherheitsfunktionen in vielen Anwendungsbereichen auszuführen. Auf Rechnern basierende Systeme (allgemein ausgedrückt programmierbare elektronische Systeme (PES)) 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 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 programmierbar elektronischen Bauteilen bestehen (elektrische/elektronische/programmierbar elektronische Systeme (E/E/PES)) und die eingesetzt werden, um Sicherheitsfunktionen auszuführen. Dieser allgemeine Lösungsweg wurde gewählt, um ein sinnvolles und konsistentes technisches Verfahren für alle elektrischen Sicherheitssysteme zu entwickeln. Ein Hauptziel ist es, die Entwicklung von anwendungsspezifischen Normen zu erleichtern.

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

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

Diese Internationale Norm:

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

- setzt eine untere Grenze des Ausfallgrenzwertes für eine gefahrbringende Ausfallart, der für ein einzelnes sicherheitsbezogenes E/E/PE-System beansprucht werden kann. Für sicherheitsbezogene E/E/PE-Systeme, die:
 - in der Betriebsart mit einer niedrigen Anforderungsrate betrieben werden, ist die untere Grenze der mittleren Wahrscheinlichkeit, die entworfene Funktion auf Anforderung nicht auszuführen, auf 10^{-5} festgelegt;
 - in der Betriebsart mit einer hohen oder ununterbrochenen Anforderungsrate betrieben werden, ist die untere Grenze der Wahrscheinlichkeit eines gefahrbringenden Ausfalls auf 10^{-9} pro Stunde festgelegt;

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

- lässt einen weiten Bereich von Prinzipien, Techniken und Maßnahmen zu, um funktionale Sicherheit für sicherheitsbezogene E/E/PE-Systeme zu erreichen, verwendet aber nicht das Fail-safe-Konzept, das genutzt werden kann, wenn das Ausfallverhalten gut definiert und das Niveau der Komplexität verhältnismäßig niedrig ist. Das Fail-safe-Konzept wurde wegen des weiten Bereiches der Komplexität von sicherheitsbezogenen E/E/PE-Systemen, die im Rahmen der Norm behandelt werden, als ungeeignet betrachtet.

Funktionale Sicherheit elektrischer/elektronischer/programmierbar elektronischer sicherheitsbezogener Systeme

Teil 1: Allgemeine Anforderungen

1 Anwendungsbereich

1.1 Diese Internationale Norm behandelt diejenigen Gesichtspunkte, die zu betrachten sind, wenn elektrische/elektronische/programmierbar elektronische Systeme (E/E/PES) zur Ausführung von Sicherheitsfunktionen eingesetzt werden. Ein Hauptziel dieser Norm ist es, für ein bestimmtes Anwendungsgebiet die Entwicklung einer entsprechenden Internationalen Norm durch das jeweils verantwortliche Komitee zu ermöglichen. Dies wird es erlauben, alle wichtigen Einflussgrößen dieses Anwendungsgebietes vollständig zu berücksichtigen und damit dessen besonderen Erfordernissen nachzukommen. Ein zweites Ziel dieser Norm ist es, die Entwicklung eines elektrischen/elektronischen/programmierbar elektronischen (E/E/PE) sicherheitsbezogenen Systems, für dessen Anwendungsgebiet noch keine Internationale Norm besteht, zu ermöglichen.

1.2 Insbesondere:

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

ANMERKUNG 1 Für einfache sicherheitsbezogene E/E/PE-Systeme geringer Komplexität 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 3.4.4 von IEC 61508-4).

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

- b) ist diese Norm allgemein gültig und auf alle sicherheitsbezogenen E/E/PE-Systeme, unabhängig von der Anwendung, anwendbar;
- c) behandelt diese Norm mögliche Gefährdungen, die durch Ausfälle der durch die sicherheitsbezogenen E/E/PE-Systeme ausgeführten Sicherheitsfunktionen bedingt sind, diese sind verschieden von Gefährdungen, die von der E/E/PE-Einrichtung selbst ausgehen (zum Beispiel elektrischer Schlag usw.);
- d) behandelt diese Norm nicht E/E/PE-Systeme, bei denen:
- ein einzelnes E/E/PE-System fähig ist, die notwendige Risikominderung zu liefern, und
 - die erforderliche Sicherheitsintegrität des E/E/PE-Systems geringer als die Sicherheitsintegrität ist, die für den Sicherheits-Integritätslevel 1 (dem geringsten Sicherheits-Integritätslevel in dieser Norm) festgelegt ist;
- e) befasst sich diese Norm hauptsächlich mit den sicherheitsbezogenen E/E/PE-Systemen, deren Ausfall einen Einfluss auf die Sicherheit von Personen und/oder die Sicherheit der 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 Siehe 3.1.1 und 7.3.1.2 der IEC 61508-4.

- f) betrachtet diese Norm sicherheitsbezogene E/E/PE-Systeme, sicherheitsbezogene Systeme anderer Technologie und externe Einrichtungen zur Risikominderung, damit die Spezifikation der Sicherheitsanforderungen für die sicherheitsbezogenen E/E/PE-Systeme in einer systematischen, risikoorientierten Art und Weise festgelegt werden kann;
- g) verwendet diese Norm als technischen Rahmen das Modell eines gesamten Sicherheitslebenszyklus, um diejenigen Tätigkeiten systematisch zu behandeln, die für die Sicherstellung der funktionalen Sicherheit der sicherheitsbezogenen E/E/PE-Systeme notwendig sind;

ANMERKUNG 3 Die frühen Phasen des gesamten Sicherheitslebenszyklus schließen notwendigerweise die Berücksichtigung anderer Technologien (wie auch die sicherheitsbezogenen E/E/PE-Systeme) und externe Einrichtungen zur Risi-

kominderung ein, damit die Spezifikation der Sicherheitsanforderungen für die sicherheitsbezogenen E/E/PE-Systeme in einer systematischen, risikoorientierten Art und Weise entwickelt werden kann.

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

- h) 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;
- i) liefert diese Norm allgemeine Anforderungen für sicherheitsbezogene E/E/PE-Systeme, für die keine anwendungsspezifischen Normen vorhanden sind;
- j) 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.

1.3 Dieser Teil von IEC 61508 legt die allgemeinen Anforderungen fest, die auf alle Teile anwendbar sind. Andere Teile von 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 Definitionen 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 Methoden und Maßnahmen.

1.4 Die Teile 1, 2, 3 und 4 dieser Norm sind Sicherheits-Grundnormen, dieser Status ist aber im Zusammenhang mit einfachen E/E/PE-sicherheitsbezogenen Systemen nicht anwendbar (siehe 3.4.4 von Teil 4). Als Sicherheits-Grundnormen sind sie zur Verwendung durch technische Komitees bei der Erstellung von Normen nach IEC Guide 104 und ISO/IEC Guide 51 vorgesehen. Die IEC 61508 ist ebenfalls zur Verwendung als eigenständige Norm vorgesehen.

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

ANMERKUNG In den USA und Kanada können vorhandene nationale Sicherheitsnormen für den Bereich der Prozessindustrie auf Basis der IEC 61508 (d. h. ANSI/ISA S84.01-1996) (siehe Hinweis [8] in Anhang C) anstelle der IEC 61508 verwendet werden, bis die beabsichtigte sektorspezifische Umsetzung der IEC 61508 als eine Internationale Norm in den USA und Kanada veröffentlicht wird.

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

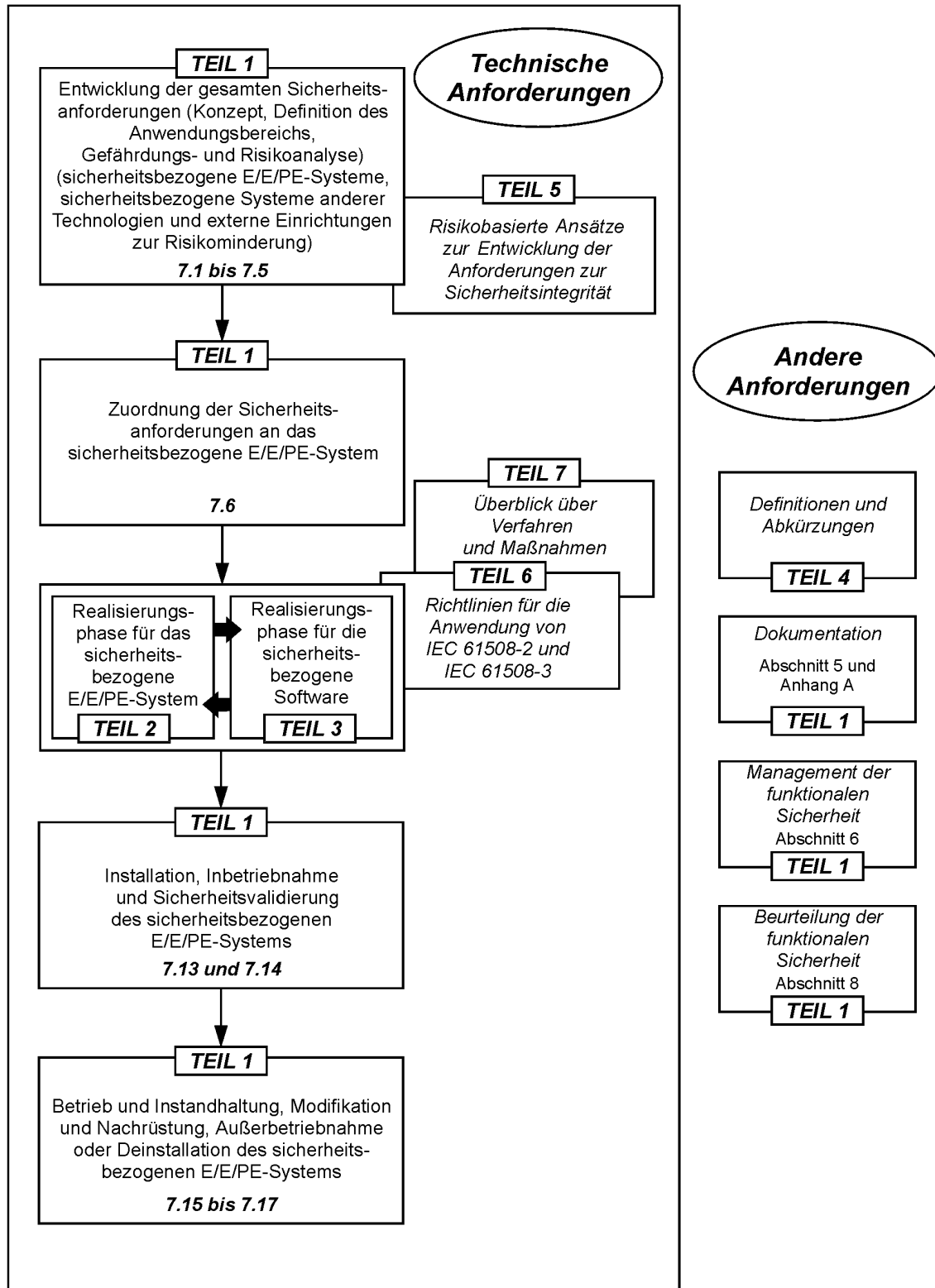


Bild 1 – Gesamtrahmen dieser Norm

2 Normative Verweisungen

Die folgenden normativen Dokumente enthalten Festlegungen, die durch Verweisung in diesem Text Bestandteil dieses Teils der IEC 61508 sind. Bei datierten Verweisungen gelten spätere Änderungen oder Überarbeitungen dieser Publikationen nicht. Vertragspartner, deren Vereinbarungen auf diesen Teil der IEC 61508 basieren, werden jedoch gebeten, die Möglichkeit zu prüfen, ob die jeweils neuesten Ausgaben der nachfolgend angegebenen normativen Dokumente angewendet werden können. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen normativen Dokuments. Die Mitglieder von ISO und IEC führen Verzeichnisse der gegenwärtig gültigen Internationalen Normen.

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

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

IEC 61508-2, – *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*¹⁾.

IEC 61508-3:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*.

IEC 61508-4:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*.

IEC 61508-5:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*.

IEC 61508-6, – *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of parts 2 and 3*¹⁾.

IEC 61508-7, – *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of the techniques and measures*¹⁾.

3 Begriffe und Abkürzungen

Für die Anwendung dieser Norm gelten die in **Teil 4** aufgeführten Begriffe und Abkürzungen.

4 Übereinstimmung mit dieser Norm

4.1 Um Übereinstimmung mit dieser Norm zu erreichen, muss dargelegt werden, dass die 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.

ANMERKUNG Es ist im Allgemeinen nicht möglich, jeden einzelnen Faktor zu bestimmen, der den Grad, mit dem eine Anforderung zu erfüllen ist, festlegt (Schärfegrad). Er hängt von einer Anzahl von Faktoren ab, die ihrerseits von der speziellen Phase und Tätigkeit des gesamten Sicherheitslebenszyklus, des E/E/PES-Sicherheitslebenszyklus oder des Software-Sicherheitslebenszyklus abhängen können. Diese Faktoren schließen ein:

- Art der Gefährdungen;
- Minderung der Auswirkungen und des Risikos;
- Sicherheits-Integritätslevel;
- Art der technologischen Ausführung;
- Größe des Systems;
- Anzahl der beteiligten Arbeitsgruppen;

¹⁾ wird veröffentlicht

- physikalische Verteilung;
- Neuheit des Entwurfs.

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 [3.4.4 von IEC 61508-4](#)), für die verlässliche Felderfahrungen vorliegen, die das notwendige Vertrauen ergeben, dass die erforderliche Sicherheitsintegrität erreicht werden kann, sind die folgenden Alternativen vorhanden:

- in anwendungsspezifischen Normen, die 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 Internationale anwendungsspezifische 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 dies begründet ist.

4.3 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 gesamten Sicherheitslebenszyklus, des E/E/PES-Sicherheitslebenszyklus 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](#)), der Verifikation (siehe [7.18](#)) und der Beurteilung der funktionalen Sicherheit (siehe [Abschnitt 8](#)) wirkungsvoll ausgeführt werden kann.

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 [\[4\]](#) in Anhang C.

5.2 Anforderungen

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

ANMERKUNG Der Umfang ausreichender Informationen hängt von einer Anzahl von Faktoren ab, die 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 Wenn es nicht in der Planung der funktionalen Sicherheit begründet oder in anwendungsspezifischen Normen festgelegt ist, müssen die Informationen, die dokumentiert werden müssen, so sein, wie es in den verschiedenen Abschnitten dieser Norm 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 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 überarbeitet, geändert, überprüft und genehmigt werden und müssen einem angemessenen System der Dokumentenlenkung unterliegen.

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 Managementtätigkeiten und die technischen Tätigkeiten während der Phasen des gesamten Sicherheitslebenszyklus, des E/E/PES-Sicherheitslebenszyklus und des Software-Sicherheitslebenszyklus, die für das Erreichen der erforderlichen funktionalen Sicherheit der sicherheitsbezogenen E/E/PE-Systeme notwendig sind, festzulegen.

6.1.2 Das zweite Ziel der Anforderungen dieses Abschnitts ist es, die Verantwortlichkeiten der Personen, Abteilungen und Organisationen, die für jede Phase des gesamten Sicherheitslebenszyklus, des E/E/PES-Sicherheitslebenszyklus und des Software-Sicherheitslebenszyklus oder Tätigkeiten innerhalb jeder Phase verantwortlich sind, festzulegen.

ANMERKUNG Die organisatorischen Maßnahmen, die in diesem Abschnitt behandelt werden, liefern die effektive Ausführung der technischen Anforderungen und sind nur 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 im Allgemeinen als Teil der vom Hersteller des sicherheitsbezogenen E/E/PE-Systems gelieferten Informationen spezifiziert.

6.2 Anforderungen

6.2.1 Diejenigen Organisationen oder Personen, die Gesamtverantwortung für eine oder mehrere Phasen des gesamten Sicherheitslebenszyklus, des E/E/PES-Sicherheitslebenszyklus oder des Software-Sicherheitslebenszyklus haben, müssen im Hinblick auf diejenigen Phasen, für die sie Gesamtverantwortung haben, alle Managementtätigkeiten und technischen Tätigkeiten festlegen, die notwendig sind, um sicherzustellen, dass die sicherheitsbezogenen E/E/PE-Systeme die erforderliche funktionale Sicherheit erreichen und aufrechterhalten. Insbesondere sollten folgende Punkte betrachtet werden:

- a) die Vorgehensweise und die Strategie zum Erreichen der funktionalen Sicherheit, gemeinsam mit den Mitteln, das Erreichte zu bewerten, und den Mitteln, mit denen dieses innerhalb der Organisation kommuniziert wird, um eine "Kultur sicheren Arbeitens" zu gewährleisten;
- b) Festlegung der Personen, Abteilungen und Organisationen, die für die Ausführung und Überprüfung der zutreffenden Phasen des gesamten Sicherheitslebenszyklus, des E/E/PES-Sicherheitslebenszyklus oder des Software-Sicherheitslebenszyklus verantwortlich sind (einschließlich, wo zutreffend, Genehmigungsbehörden oder Sicherheitsüberwachungsorgane);
- c) die anzuwendenden Phasen des gesamten Sicherheitslebenszyklus, des E/E/PES-Sicherheitslebenszyklus oder des Software-Sicherheitslebenszyklus;
- d) die Art und Weise, wie Informationen strukturiert werden müssen, und der Umfang der zu dokumentierenden Informationen (siehe [Abschnitt 5](#));
- e) die 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](#));
- f) die Tätigkeiten zur Beurteilung der funktionalen Sicherheit (siehe [Abschnitt 8](#));
- g) die Verfahren zur Sicherstellung einer unverzüglichen Verfolgung und zufrieden stellenden Lösung von Anforderungen bezüglich der sicherheitsbezogenen E/E/PE-Systeme, die von Folgendem herrühren:
 - Gefährdungs- und Risikoanalyse (siehe [7.4](#));
 - Beurteilung der funktionalen Sicherheit (siehe [Abschnitt 8](#));
 - Verifikationstätigkeiten (siehe [7.18](#));
 - Validierungstätigkeiten (siehe [7.8](#) und [7.14](#));
 - Konfigurationsmanagement (siehe [6.2.1 o](#)), [7.16](#) und [IEC 61508-2](#) und [IEC 61508-3](#));
- h) die Verfahren zur Sicherstellung, dass die Gruppen, die an irgendeiner der Tätigkeiten des gesamten Sicherheitslebenszyklus, des E/E/PES-Sicherheitslebenszyklus oder des Software-Sicherheitslebenszyklus beteiligt sind, kompetent sind, die in ihrer Verantwortung liegenden Tätigkeiten auszuführen. Dabei sollte insbesondere Folgendes festgelegt sein:
 - die Ausbildung des Personals in der Diagnose und Reparatur von Fehlern und in der Prüfung eines Systems;
 - die Ausbildung des Betriebspersonals;
 - die Weiterbildung des Personals in regelmäßigen Abständen;

ANMERKUNG 1 [Anhang B](#) enthält Leitfäden zu den Anforderungen an die Kompetenz für diejenigen, die an irgendeiner Tätigkeit des gesamten Sicherheitslebenszyklus, des E/E/PES-Sicherheitslebenszyklus oder des Software-Sicherheitslebenszyklus beteiligt sind.

- i) die Verfahren zur Sicherstellung, dass gefahrbringende Zwischenfälle (oder Zwischenfälle mit der Möglichkeit, Gefährdungen zu erzeugen) analysiert werden und dass Empfehlungen erfolgen, um die Wahrscheinlichkeit des wiederholten Auftretens zu minimieren;
- j) die Verfahren zur Analyse der Betriebs- und Instandhaltungsleistung, insbesondere Verfahren für:
 - die Erkennung systematischer Fehler, die 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;
- k) Anforderungen für periodische Audits der funktionalen Sicherheit in Übereinstimmung mit diesem Unterabschnitt einschließlich:
 - der Häufigkeit der Audits der funktionalen Sicherheit;
 - der Beachtung des erforderlichen Unabhängigkeitsgrades der für die Audits Verantwortlichen;
 - der Dokumentation und nachfolgender Tätigkeiten;
- l) die Verfahren für die Einleitung von Modifikationen der sicherheitsbezogenen Systeme (siehe 7.16.2.2);
- m) die erforderlichen Verfahren für die Zustimmung und die Ermächtigung zu Modifikationen;
- n) die Verfahren für die Bewahrung genauer Informationen zu möglichen Gefährdungen und den sicherheitsbezogenen Systemen;
- o) die Verfahren für das Konfigurationsmanagement der sicherheitsbezogenen E/E/PE-Systeme während aller Phasen des gesamten Sicherheitslebenszyklus, des E/E/PES-Sicherheitslebenszyklus und des Software-Sicherheitslebenszyklus. Insbesondere sollte Folgendes angegeben werden:
 - das Stadium, in dem eine formale Konfigurationskontrolle eingeführt werden muss;
 - die Verfahren, die für eine eindeutige Bestimmung aller Bestandteile eines Gegenstands (Hardware und Software) angewendet werden müssen;
 - die Verfahren, um zu verhindern, dass nicht zugelassene Komponente zum Einsatz kommen;

ANMERKUNG 2 Für weitere Details zum Konfigurationsmanagement siehe Hinweise [6] und [7] in Anhang C.

- p) wo angemessen, die Bestimmungen zur Ausbildung und Informationen für den Gefahrenfall.

6.2.2 Die als Ergebnis von 6.2.1 festgelegten Tätigkeiten müssen ausgeführt werden und der Fortschritt muss überwacht werden.

6.2.3 Die als Ergebnis von 6.2.1 entwickelten Anforderungen müssen formal durch die zuständigen Organisationen überprüft werden und es muss Übereinstimmung erzielt werden.

6.2.4 Alle, die als verantwortlich für das Management der Tätigkeiten der funktionalen Sicherheit festgelegt werden, müssen über die ihnen zugeordneten Verantwortlichkeiten informiert werden.

6.2.5 Hersteller, die Produkte an eine Organisation liefern oder Dienstleistungen für sie erbringen, wobei diese Organisation Gesamtverantwortung für eine oder mehrere Phasen des gesamten Sicherheitslebenszyklus, des E/E/PES-Sicherheitslebenszyklus oder des Software-Sicherheitslebenszyklus (siehe 6.2.1) hat, müssen Produkte oder Dienstleistungen nach den Festlegungen dieser Organisation liefern oder erbringen und sie müssen ein angemessenes Qualitätsmanagementsystem haben.

7 Anforderungen zum gesamten Sicherheitslebenszyklus

7.1 Allgemeines

7.1.1 Einleitung

7.1.1.1 Um auf systematische Art und Weise alle Tätigkeiten, die zum Erreichen des erforderlichen Sicherheits-Integritätslevels für die sicherheitsbezogenen E/E/PE-Systeme notwendig sind, abzuhandeln, verwendet diese Norm als technischen Rahmen einen gesamten Sicherheitslebenszyklus (siehe Bild 2).