

	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 61508-3
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 3
ICS 25.040.40; 35.080 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements (IEC 61508-3:1998 + corrigendum 1999); German version EN 61508-3:2001 Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 3: Prescriptions concernant les logiciels (CEI 61508-3:1998 + corrigendum 1999); Version allemande EN 61508-3:2001 Die Europäische Norm EN 61508-3:2001 hat den Status einer Deutschen Norm. Beginn der Gültigkeit Die EN 61508-3 wurde am 2001-07-03 angenommen. Anwendungsrichtlinie: DIN EN 61508-6 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/181/CDV (VDE 0801 Teil 3):1996-02. Die enthaltene IEC-Publikation wurde vom SC 65A „System aspects“ erarbeitet. Sie ist eine Sicherheits-Grundnorm, siehe hierzu auch Unterabschnitt 1.2. Fortsetzung Seite 2 und 3 und 52 Seiten EN DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

DIN EN 61508-3 (VDE 0803 Teil 3):2002-12

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 z. B. aus IEC 68 nun IEC 60068 geworden.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
EN 61508-1:2001	IEC 61508-1:1998	DIN EN 61508-1 (VDE 0803 Teil 1):2002-11	VDE 0803 Teil 1
EN 61508-2:2001	IEC 61508-2:2000	DIN EN 61508-2 (VDE 0803 Teil 2): in Vorbereitung	VDE 0803 Teil 2
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 61508-1 (VDE 0803 Teil 1), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen (IEC 61508-1:1998 + Corrigendum 1999); Deutsche Fassung EN 61508-1:2001.*

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 61508-4 (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 3: Anforderungen an Software**
(IEC 61508-3:1998 + Corrigendum 1999)

Functional safety of
electrical/electronic/programmable electronic
safety-related systems –
Part 3: Software requirements
(IEC 61508-3:1998 + corrigendum 1999)

Sécurité fonctionnelle des systèmes
électriques/électroniques/électroniques
programmables relatifs à la sécurité –
Partie 3: Prescriptions concernant les logiciels
(CEI 61508-3:1998 + 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 Modifikation 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 61508-3 einschließlich deren Corrigendum April 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 61508-3 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 sind Anhänge A, B und ZA normativ und ist Anhang 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 Systems, 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 61508-3:1998 einschließlich deren Corrigendum April 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	11
6 Qualitätsmanagementsystem der Software	11
6.1 Ziele	11
6.2 Anforderungen	12
7 Anforderungen an den Software-Sicherheitslebenszyklus	12
7.1 Allgemeines	12
7.2 Spezifikation der Software-Sicherheitsanforderungen	19
7.3 Planung der Validierung der Software bezüglich der Sicherheit	22
7.4 Softwareentwurf und Softwareentwicklung	23
7.5 Integration der programmierbaren Elektronik (Hardware und Software)	29
7.6 Software-Betriebs- und Modifikationsverfahren	31
7.7 Validierung der Software bezüglich der Sicherheit	31
7.8 Softwaremodifikation	32
7.9 Software-Verifikation	34
8 Beurteilung der funktionalen Sicherheit	38
Anhang A (normativ) Leitfaden für die Auswahl der Verfahren und Maßnahmen	39
Anhang B (normativ) Detailtabellen	46
Anhang C (informativ) Literaturhinweise	51
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	52
Bilder	
Bild 1 – Gesamtrahmen dieser Norm	10
Bild 2 – E/E/PES-Sicherheitslebenszyklus (in der Realisierungsphase)	14
Bild 3 – Software-Sicherheitslebenszyklus (in der Realisierungsphase)	14
Bild 4 – Beziehung zwischen der IEC 61508-2 und IEC 61508-3 und ihre Anwendungsbereiche	15
Bild 5 – Sicherheitsintegrität der Software und Entwicklungslebenszyklus (das V-Modell)	15
Bild 6 – Beziehung zwischen der Hardware- und Software-Architektur der programmierbaren Elektronik	20
Tabellen	
Tabelle 1 – Software-Sicherheitslebenszyklus: Überblick	16
Tabelle A.1 – Spezifikation der Software-Sicherheitsanforderung (siehe 7.2)	40
Tabelle A.2 – Softwareentwurf und Softwareentwicklung: Entwurf der Software-Architektur (siehe 7.4.3)	40
Tabelle A.3 – Softwareentwurf und Softwareentwicklung: Hilfswerkzeuge und Programmiersprachen (siehe 7.4.4)	41

Tabelle A.4 – Softwareentwurf und Softwareentwicklung: detaillierter Entwurf (siehe 7.4.5 and 7.4.6) (Dies beinhaltet Software-Systementwurf, Entwurf der Softwaremodule und Codierung).....	41
Tabelle A.5 – Softwareentwurf und Softwareentwicklung: Test der Softwaremodule und Integration (siehe 7.4.7 und 7.4.8)	42
Tabelle A.6 – Integration der programmierbaren Elektronik (Hardware und Software) (siehe 7.5)	43
Tabelle A.7 – Validierung der Software bezüglich der Sicherheit (siehe 7.7).....	43
Tabelle A.8 – Modifikation (siehe 7.8).....	43
Tabelle A.9 – Software-Verifikation (siehe 7.9).....	44
Tabelle A.10 – Beurteilung der funktionalen Sicherheit (siehe Abschnitt 8).....	45
Tabelle B.1 – Entwurfs- und Codierungs-Richtlinien (Verweisungen aus Tabelle A.4).....	46
Tabelle B.2 – Dynamische Analyse und Test (Verweisung aus den Tabellen A.5 und A.9)	46
Tabelle B.3 – Funktionstest und Black-Box-Test (Verweisung aus den Tabellen A.5, A.6 und A7)	47
Tabelle B.4 – Ausfall-/Versagensanalyse (Verweisung aus der Tabelle A.10)	47
Tabelle B.5 – Modellierung (Verweisung aus der Tabelle A.7).....	48
Tabelle B.6 – Leistungstest (Verweisung aus den Tabellen A.5 und A.6).....	48
Tabelle B.7 – Semi-formale Methoden (Verweisung aus den Tabellen A.1, A.2 und A.4).....	49
Tabelle B.8 – Statische Analyse (Verweisung aus der Tabelle A.9).....	49
Tabelle B.9 – Modularisierung (Verweisung aus der Tabelle A.4).....	50

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 programmierbare 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 des 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 3: Anforderungen an Software

1 Anwendungsbereich

1.1 Dieser Teil der IEC 61508:

- a) ist dazu vorgesehen, nur nach einem gründlichen Verständnis der **IEC 61508-1** und **IEC 61508-2** angewendet zu werden;
- b) trifft auf jede Software zu, die einen Teil eines sicherheitsbezogenes Systems bildet oder verwendet wird, um ein sicherheitsbezogenes System im Anwendungsbereich der **IEC 61508-1** und **IEC 61508-2** zu entwickeln. Diese Software wird dann sicherheitsbezogene Software genannt;
 - sicherheitsbezogene Software beinhaltet Betriebssysteme, Systemsoftware, Software in Netzwerken, Funktionen für Mensch-Maschine-Schnittstellen, Hilfswerkzeuge und Firmware sowie Anwenderprogramme;
 - Anwenderprogramme beinhalten Hochsprachenprogramme, maschinennahe Programme und Programme für spezielle Anwendungen in einer Programmiersprache mit eingeschränktem Sprachumfang (siehe **3.2.7 der IEC 61508-4**);
- c) fordert, dass die Sicherheitsfunktionen der Software und die Software-Sicherheits-Integritätslevel spezifiziert werden;

ANMERKUNG 1 Sollte dies bereits als Teil der Spezifikation des E/E/PE-sicherheitsbezogenen Systems (siehe **7.2 der IEC 61508-2**) gemacht worden sein, so muss es an dieser Stelle nicht noch einmal wiederholt werden.

ANMERKUNG 2 Das Spezifizieren der Sicherheitsfunktionen der Software und der Software-Sicherheits-Integritätslevel ist ein iterativer Prozess; siehe **Bilder 2** und **6**.

ANMERKUNG 3 Zur Struktur der Dokumentation siehe **Abschnitt 5** und **Anhang A der IEC 61508-1**. Die Struktur der Dokumentation kann die Prozesse des Unternehmens berücksichtigen und ebenso die Arbeitserfahrung für das spezielle Anwendungsgebiet.

- d) legt Anforderungen und Tätigkeiten fest, die in den Phasen des Lebenszyklus während des Entwurfs und der Entwicklung der sicherheitsbezogenen Software (das Modell des Software-Sicherheitslebenszyklus) angewendet werden müssen. Diese Anforderungen beinhalten den Einsatz von Maßnahmen und Techniken in der Software, die zur Vermeidung und Beherrschung von Fehlern und Versagensfällen dem Sicherheits-Integritätslevel entsprechend abgestuft sind;
- e) liefert Anforderungen an die Informationen zur Software-Sicherheits-Validierung, die an die Organisation, die die E/E/PES-Integration durchführt, weitergeleitet werden;
- f) liefert Anforderungen zur Vorbereitung von Informationen und Prozeduren, die die Software betreffen und die vom Anwender für den Betrieb und die Instandhaltung des sicherheitsbezogenen Systems benötigt werden;
- g) liefert Anforderungen, die von der Organisation, die Modifikationen an der sicherheitsbezogenen Software durchführt, zu erfüllen sind;
- h) liefert, im Zusammenwirken mit der **IEC 61508-1** und **IEC 61508-2**, Anforderungen an Hilfswerkzeuge, wie Werkzeuge zur Entwicklung und zum Entwurf, Übersetzer, Werkzeuge für Test und Debugging und Werkzeuge für das Konfigurationsmanagement.

ANMERKUNG 4 Die **Bilder 4** und **6** zeigen die Beziehung zwischen der **IEC 61508-2** und IEC 61508-3.

1.2 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 existierende nationale Sicherheitsnormen für den Bereich der Prozessindustrie auf der Basis der IEC 61508 (d. h. ANSI/ISA S84.01-1996) anstelle der IEC 61508 so lange angewendet werden, bis die vorgeschlagene spezifische Umsetzung der IEC 61508 für die Prozessindustrie (d. h. IEC 61511) in den USA und Kanada als Internationale Norm veröffentlicht wurde.

1.3 [Bild 1](#) zeigt den gesamten Rahmen für die Teile 1 bis 7 der IEC 61508 und zeigt die Rolle, die die IEC 61508-3 zum Erreichen der funktionalen Sicherheit der sicherheitsbezogenen E/E/PE-Systeme spielt. [Anhang A der IEC 61508-6](#) beschreibt die Anwendung der [IEC 61508-2](#) und IEC-61508-3.

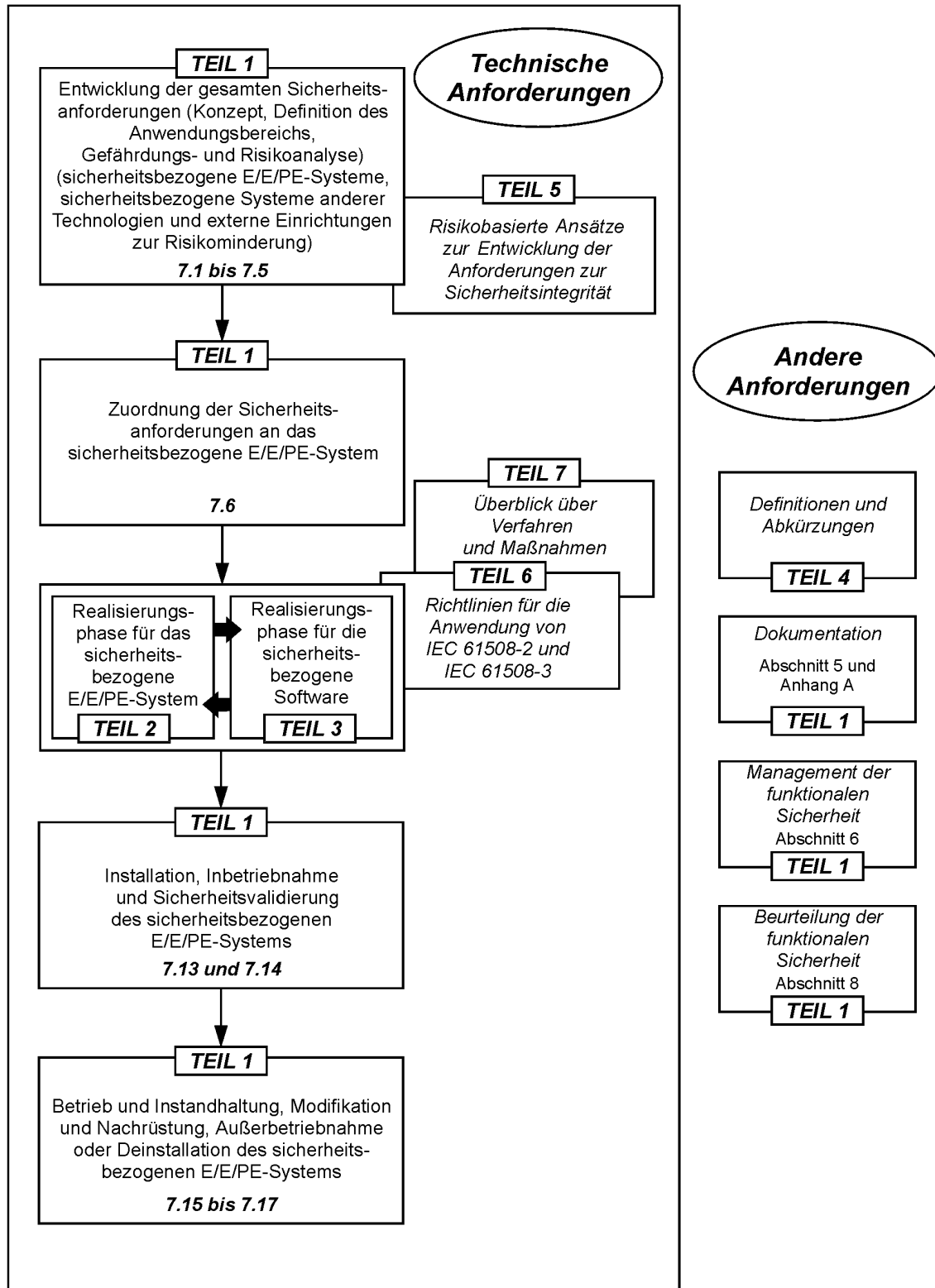


Bild 1 – Gesamtrahmen dieser Norm

2 Normative Verweisungen

Die folgenden Normen enthalten Festlegungen, die durch Verweisung in diesem Text Bestandteil dieses Teils der IEC 61508 sind. Zum Zeitpunkt der Veröffentlichung waren die angegebenen Ausgaben gültig. Alle Normen unterliegen der Überarbeitung, und Vertragspartner, deren Vereinbarungen auf diesen Teil der IEC 61508 basieren, werden gebeten, die Möglichkeit zu prüfen, ob die jeweils neuesten Ausgaben der im Folgenden genannten Normen angewendet werden können. Mitglieder von IEC und ISO führen Verzeichnisse der gültigen Internationalen Normen.

IEC 61508-1:1998, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 1: General requirements.*

IEC 61508-2:–, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 2: Requirements for electrical/electrical/programmable electronic safety-related system¹⁾.*

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

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

IEC 61508-6:–, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 6: Guidelines on the application of parts 2 and 3¹⁾.*

IEC 61508-7:–, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 7: Overview of techniques and measures¹⁾.*

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.*

3 Begriffe und Abkürzungen

Für die Anwendung dieser Norm gelten die in der **IEC 61508-4** aufgeführten Begriffe und Abkürzungen.

4 Übereinstimmung mit dieser Norm

Die Anforderungen zur Übereinstimmung mit dieser Norm befinden sich in **Abschnitt 4 der IEC 61508-1**.

5 Dokumentation

Die Ziele und Anforderungen zur Dokumentation befinden sich in **Abschnitt 5 der IEC 61508-1**.

6 Qualitätsmanagementsystem der Software

6.1 Ziele

Die Ziele sind die, die in **6.1 der IEC 61508-1** beschrieben sind.

¹⁾ Wird veröffentlicht.

6.2 Anforderungen

6.2.1 Die Anforderungen sind die, die in **6.2 der IEC 61508-1** beschrieben sind, mit folgenden zusätzlichen Anforderungen.

6.2.2 Die Planung der funktionalen Sicherheit muss die Strategie für die Beschaffung, Entwicklung, Integration, Verifikation, Validierung und Modifikation der Software im Rahmen der Anforderungen des Sicherheits-Integritätslevels des E/E/PE-sicherheitsbezogenen Systems definieren.

ANMERKUNG Die Philosophie dieser Vorgehensweise ist die Verwendung der Planung der funktionalen Sicherheit als Möglichkeit, diese Norm unter Berücksichtigung der verschiedenen Sicherheitsintegritäten, die für die E/E/PE-sicherheitsbezogenen Systemkomponenten notwendig sind, anzupassen. **7.4.2.8** von Teil 3 sollte berücksichtigt werden, wenn E/E/PE-sicherheitsbezogene Systemkomponenten verschiedener Sicherheits-Integritätslevel gemeinsam verwendet werden.

6.2.3 Das Konfigurationsmanagement der Software sollte

- a) Verwaltungs- und technische Kontrollen während des Software-Sicherheitslebenszyklus verwenden, um Softwaremodifikationen zu verwalten und somit sicherzustellen, dass die spezifizierten Anforderungen an die Software bezüglich der Sicherheit weiterhin erfüllt werden;
- b) garantieren, dass alle notwendigen Tätigkeiten durchgeführt wurden, um zu zeigen, dass die erforderliche Sicherheitsintegrität der Software erreicht wurde;
- c) genau und mit gleicher Kennzeichnung alle Konfigurationsmerkmale behandeln, die notwendig sind, um die Integrität des E/E/PE-sicherheitsbezogenen Systems aufrecht zu erhalten. Konfigurationsmerkmale beinhalten mindestens Folgendes: die Sicherheitsanalyse und Sicherheitsanforderungen, Spezifikation der Software und Entwurfsdokumente, Softwaremodule im Source-code, Testpläne und Testergebnisse; bereits existierende Softwarekomponenten und Softwarepakete, die in das E/E/PE-sicherheitsbezogene System integriert werden, alle Werkzeuge und Entwicklungsumgebungen, die verwendet werden, um die Software zu erstellen oder zu testen, oder jedwede Arbeit an der Software des E/E/PE-sicherheitsbezogenen Systems durchzuführen;
- d) Verfahren anwenden, um nicht autorisierte Modifikationen zu verhindern, Modifikationsanforderungen zu dokumentieren, Einflüsse einer beabsichtigten Modifikation analysieren zu können und eine Aufforderung genehmigen oder zurückweisen zu können, die Einzelheiten der Modifikation und die Bevollmächtigung für die genehmigten Modifikationen zu dokumentieren, Mindestanforderungen an die Konfiguration zu bestimmten Punkten in der Softwareentwicklung festzulegen und die teilweisen Integrationstests zu dokumentieren, um die Mindestanforderung zu bestätigen (siehe **7.8**), die Zusammenstellung und den Aufbau aller Mindestanforderungen an die Software (mit den Modifikationen früherer Mindestanforderungen) garantieren zu können;

ANMERKUNG 1 Zur Anleitung zur Verwendung von Verwaltungs- und technischen Kontrollen und deren Durchsetzung ist die Entscheidung und Autorität des Managements notwendig.

- e) die folgenden Informationen dokumentieren, um ein nachfolgendes Audit zu ermöglichen: den Status der Konfiguration, Version, Begründung und Genehmigung der Modifikationen und deren Einzelheiten;
- f) die Version der sicherheitsbezogenen Software formal dokumentieren. Kopien der Software und alle zugehörige Dokumentation sollten aufbewahrt werden, um Pflege und Modifikation während der Betriebslebensdauer der Softwareversion zu ermöglichen.

ANMERKUNG 2 Für weitere Information zum Konfigurationsmanagement siehe ISO/IEC 12207.

7 Anforderungen an den Software-Sicherheitslebenszyklus

7.1 Allgemeines

7.1.1 Ziel

Das Ziel der Anforderungen dieses Unterabschnitts ist es, die Entwicklung der Software in definierte Phasen und Tätigkeiten zu strukturieren (siehe **Tabelle 1** und **Bilder 2 bis 5**).

7.1.2 Anforderungen

7.1.2.1 Für die Entwicklung der Software muss während der Sicherheitsplanung ein Sicherheitslebenszyklus in Übereinstimmung mit [Abschnitt 6 der IEC 61508-1](#) ausgewählt und spezifiziert werden.

ANMERKUNG Ein Modell des Sicherheitslebenszyklus, das die Anforderungen des [Abschnitts 7 der IEC 61508-1](#) erfüllt, kann für die besonderen Bedürfnisse des Projekts oder der Organisation geeignet angepasst werden.

7.1.2.2 Verfahren zur Gewährleistung der Qualität und Sicherheit müssen in die Tätigkeiten des Sicherheitslebenszyklus integriert werden.

7.1.2.3 Jede Phase des Software-Sicherheitslebenszyklus muss in elementare Tätigkeiten aufgeteilt werden, wobei Anwendungsbereich, Eingaben und Ausgaben für jede Phase festgelegt werden.

ANMERKUNG 1 Für weitere Informationen zu den Phasen des Lebenszyklus siehe ISO/IEC 12207.

ANMERKUNG 2 [Abschnitt 5 der IEC 61508-1](#) betrachtet die Ausgaben der Phasen des Lebenszyklus. Bei der Entwicklung E/E/PE-sicherheitsbezogener Systeme darf das Ergebnis einiger Phasen des Lebenszyklus ein unterschiedliches Dokument sein, während die dokumentierten Ausgaben verschiedener Phasen in einem Dokument zusammengefasst werden dürfen. Die wesentliche Anforderung ist, dass die Ausgaben der Phase des Sicherheitslebenszyklus für die angestrebte Aufgabe ausreichend sind. In einfachen Entwicklungen können einige Phasen des Lebenszyklus ebenfalls zusammengefasst werden (siehe [7.4.5](#)).

7.1.2.4 Falls der Software-Sicherheitslebenszyklus die Anforderungen von [Bild 3](#) und [Tabelle 1](#) erfüllt, ist es möglich, die Tiefe, die Anzahl und die Arbeitsgröße der Phasen des V-Modells (siehe [Bild 5](#)) unter Berücksichtigung der Sicherheitsintegrität und Komplexität des Projekts zuzuschneiden.

ANMERKUNG Die gesamte Liste der Phasen des Lebenszyklus in [Tabelle 1](#) ist geeignet für große, neu entwickelte Systeme. Für kleine Systeme kann es zum Beispiel angemessen sein, die Phasen Entwurf des Softwaresystems und der Architektur zusammenzufassen.

7.1.2.5 Es ist möglich, das Softwareprojekt anders zu gliedern als nach dieser Norm (z. B. Verwendung eines anderen Modells des Software-Sicherheitslebenszyklus), wenn alle Ziele und Anforderungen dieses Abschnitts erfüllt werden.

7.1.2.6 Für jede Phase des Lebenszyklus müssen angemessene Techniken und Maßnahmen verwendet werden. Die [Anhänge A](#) und [B](#) (Leitfaden für die Auswahl der Techniken und Maßnahmen) geben entsprechende Empfehlungen. Die Auswahl von Techniken aus den [Anhängen A](#) und [B](#) gibt für sich allein keine Gewähr, dass die erforderliche Sicherheitsintegrität erreicht wird.

7.1.2.7 Die Ergebnisse der Tätigkeiten im Software-Sicherheitslebenszyklus müssen dokumentiert werden (siehe [Abschnitt 5](#)).

7.1.2.8 Wenn sich in irgendeinem Abschnitt des Software-Sicherheitslebenszyklus eine Modifikation auf eine frühere Phase des Lebenszyklus bezieht, müssen die frühere Phase des Lebenszyklus und die folgenden Phasen wiederholt werden.