

	Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/programmierbarer elektronischer Systeme Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3 (IEC 61508-6:2000) Deutsche Fassung EN 61508-6:2001	<u>DIN</u> EN 61508-6
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 6
ICS 25.040.40 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3; (IEC 61508-6:2000); German version EN 61508-6:2001 Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3; (CEI 61508-6:2000); Version allemande EN 61508-6:2001 Die Europäische Norm EN 61508-6:2001 hat den Status einer Deutschen Norm. Beginn der Gültigkeit Die EN 61508-6 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/255/CDV:1998-08. Die enthaltene IEC-Publikation wurde vom SC 65A „System aspects“ erarbeitet. Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zum Jahr 2005 unverändert bleiben soll. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees die Publikation – bestätigt, – zurückgezogen, – durch eine Folgeausgabe ersetzt oder – geändert. Fortsetzung Seite 2 und 3 und 72 Seiten EN DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

DIN EN 61508-6 (VDE 0803 Teil 6):2003-06

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 2004-08-01 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 61508-1:2001	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):2002-12	VDE 0803 Teil 2
EN 61508-3:2001	IEC 61508-3:1998	DIN EN 61508-3 (VDE 0803 Teil 3):2002-12	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 61508-7:2001	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	–
EN 61131-3:1993-07	IEC 61131-3:1993	DIN EN 61131-3:1994-08	–

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
EN 61078:1993-10	IEC 61078:1991	DIN EN 61078:1994-10	–

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 (IEC 61508-2:2000); Deutsche Fassung EN 61508-2:2001.*

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 + Corrigendum 1999); Deutsche Fassung EN 61508-5:2001.*

DIN EN 61508-7 (VDE 0803 Teil 7), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 7: Anwendungshinweise über Verfahren und Maßnahmen (IEC 61508-7:1998 + Corrigendum 1999); Deutsche Fassung EN 61508-7:2001.*

DIN EN 61131-3:1994-08, *Speicherprogrammierbare Steuerungen – Teil 3: Programmiersprachen (IEC 61131-3:1993); Deutsche Fassung EN 61131-3:1993.*

DIN EN 61078:1994-10, *Techniken für die Analyse der Zuverlässigkeit – Verfahren mit Zuverlässigkeitsblockdiagramm (IEC 61078:1991); Deutsche Fassung EN 61078:1993.*

– Leerseite –

**Funktionale Sicherheit sicherheitsbezogener
elektrischer/elektronischer/programmierbarer elektronischer Systeme –
Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3
(IEC 61508-6:2000)**

Functional safety of
electrical/electronic/programmable electronic
safety-related systems –
Part 6: Guidelines on the application of IEC
61508-2 and IEC 61508-3
(IEC 61508-6:2000)

Sécurité fonctionnelle des systèmes
électriques/électroniques/électroniques
programmables relatifs à la sécurité –
Partie 6: Lignes directrices pour l'application de
la CEI 61508-2 et de la CEI 61508-3
(CEI 61508-6:2000)

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 61508-6:2000, 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 61508-6 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 bis E informativ.

Der Anhang ZA wurde von CENELEC hinzugefügt.

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

„Diese Internationale Norm behandelt diejenigen Gesichtspunkte, die zu betrachten sind, wenn elektrische/elektronische/programmierbare 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/programmierbaren elektronischen (E/E/PE) sicherheitsbezogenen Systems, für dessen Anwendungsgebiet noch keine Internationale Norm besteht, zu ermöglichen.“

Der CENELEC-Bericht ROBT-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).

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.

ANMERKUNG 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 61508-6:2000 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

Inhalt

	Seite
Einleitung.....	7
1 Anwendungsbereich	9
2 Normative Verweisungen.....	11
3 Begriffe und Abkürzungen	11
Anhang A (informativ) Anwendung der IEC 61508-2 und der IEC 61508-3	12
A.1 Allgemeines.....	12
A.2 Funktionale Schritte in der Anwendung der IEC 61508-2	14
A.3 Funktionale Schritte in der Anwendung der IEC 61508-3	17
Anhang B (informativ) Beispiel eines Verfahrens für die Bewertung von Ausfallwahrscheinlichkeiten der Hardware	20
B.1 Allgemeines.....	20
B.2 Mittlere Ausfallwahrscheinlichkeit bei Anforderung (für die Betriebsart mit niedriger Anforderungsrate)	24
B.3 Wahrscheinlichkeit eines Ausfalls je Stunde (für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung)	36
B.4 Verweisungen	45
Anhang C (informativ) Ausgearbeitetes Beispiel für die Berechnung des Diagnosedeckungsgrads und des Anteils ungefährlicher Ausfälle.....	46
Anhang D (informativ) Eine Methode zur Quantifizierung der Auswirkungen von hardwarebedingten Ausfällen infolge gemeinsamer Ursache in E/E/PE-Systemen	49
D.1 Allgemeines.....	49
D.2 Kurzer Überblick	49
D.3 Anwendungsbereich der Methode	52
D.4 Durch die Methode berücksichtigte Punkte	52
D.5 Verwendung des β -Faktor, um die Wahrscheinlichkeit eines Ausfalls eines sicherheitsbezogenen E/E/PE-Systems durch Ausfälle infolge gemeinsamer Ursache zu berechnen	53
D.6 Schätzung von β unter Verwendung der Tabellen	54
D.7 Beispiele für die Anwendung der Methode	59
D.8 Literaturhinweise	60
Anhang E (informativ) Beispiele für die Anwendung der Tabellen zur Sicherheitsintegrität der Software aus der IEC 61508-3.....	61
E.1 Allgemeines.....	61
E.2 Beispiel für den Sicherheits-Integritätslevel 2.....	61
E.3 Beispiel für den Sicherheits-Integritätslevel 3.....	66
Literaturhinweise	71
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen.....	72
 Bilder	
Bild 1 – Gesamtrahmen dieser Norm.....	10
Bild A.1 – Anwendung der IEC 61508-2	16

	Seite
Bild A.2 – Anwendung der IEC 61508-2 (Fortsetzung)	17
Bild A.3 – Anwendung der IEC 61508-3.....	19
Bild B.1 – Beispielkonfiguration für zwei Kanäle mit Sensoren.....	22
Bild B.2 – Struktur mit Teilsystemen	24
Bild B.3 – Blockschaltbild für 1oo1	25
Bild B.4 – Zuverlässigkeits-Blockdiagramm für 1oo1.....	25
Bild B.5 – Blockschaltbild für 1oo2	26
Bild B.6 – Zuverlässigkeits-Blockdiagramm für 1oo2.....	27
Bild B.7 – Blockschaltbild für 2oo2	27
Bild B.8 – Zuverlässigkeits-Blockdiagramm für 2oo2.....	27
Bild B.9 – Blockschaltbild für 1oo2D	28
Bild B.10 – Zuverlässigkeits-Blockdiagramm für 1oo2D	28
Bild B.11 – Blockschaltbild für 2oo3	29
Bild B.12 – Zuverlässigkeits-Blockdiagramm für 2oo3.....	29
Bild B.13 – Architektur des Beispiels für die Betriebsart mit niedriger Anforderungsrate	34
Bild B.14 – Architektur des Beispiels für die Betriebsart mit hoher oder kontinuierlicher Anforderung	43
Bild D.1 – Beziehung zwischen Ausfällen infolge gemeinsamer Ursache und Ausfällen einzelner Kanäle	51

Tabellen

Tabelle B.1 – In diesem Anhang verwendete Benennungen und ihre zugehörigen Parameterbereiche.....	23
Tabelle B.2 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für ein Wiederholungsprüfungsintervall von 6 Monaten und eine mittlere Zeit zur Wiederherstellung von 8 h.....	30
Tabelle B.3 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für ein Wiederholungsprüfungsintervall von einem Jahr und eine mittlere Zeit zur Wiederherstellung von 8 h.....	31
Tabelle B.4 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für ein Wiederholungsprüfungsintervall von zwei Jahren und eine mittlere Zeit zur Wiederherstellung von 8 h.....	32
Tabelle B.5 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für ein Wiederholungsprüfungsintervall von 10 Jahren und eine mittlere Zeit zur Wiederherstellung von 8 h.....	33
Tabelle B.6 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für das Eingangs-Teilsystem in dem Beispiel für die Betriebsart mit niedriger Anforderungsrate (ein Jahr Wiederholungsprüfungsintervall und 8 h MTTR)	34
Tabelle B.7 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für das Logik-Teilsystem in dem Beispiel für die Betriebsart mit niedriger Anforderungsrate (ein Jahr Wiederholungsprüfungsintervall und 8 h MTTR)	34
Tabelle B.8 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für das Ausgangs-Teilsystem in dem Beispiel für die Betriebsart mit niedriger Anforderungsrate (ein Jahr Wiederholungsprüfungsintervall und 8 h MTTR)	35
Tabelle B.9 – Beispiel für eine nicht ausreichende Wiederholungsprüfung.....	36
Tabelle B.10 – Wahrscheinlichkeit eines Ausfalls je Stunde (für die Betriebsart mit hoher oder kontinuierlicher Anforderungsrate) für ein Wiederholungsprüfungsintervall von einem Monat	

	Seite
und eine mittlere Zeit zur Wiederherstellung von 8 h	39
Tabelle B.11 – Wahrscheinlichkeit eines Ausfalls je Stunde (für die Betriebsart mit hoher oder kontinuierlicher Anforderungsrate) für ein Wiederholungsprüfungsintervall von drei Monaten und eine mittlere Zeit zur Wiederherstellung von 8 h	40
Tabelle B.12 – Wahrscheinlichkeit eines Ausfalls je Stunde (für die Betriebsart mit hoher oder kontinuierlicher Anforderungsrate) für ein Wiederholungsprüfungsintervall von 6 Monaten und eine mittlere Zeit zur Wiederherstellung von 8 h	41
Tabelle B.13 – Wahrscheinlichkeit eines Ausfalls je Stunde (für die Betriebsart mit hoher oder kontinuierlicher Anforderungsrate) für ein Wiederholungsprüfungsintervall von einem Jahr und eine mittlere Zeit zur Wiederherstellung von 8 h	42
Tabelle B.14 – Wahrscheinlichkeit eines Ausfalls je Stunde für das Eingangs-Teilsystem in dem Beispiel für die Betriebsart mit hoher oder kontinuierlicher Anforderung (sechs Monate Wiederholungsprüfungsintervall und 8 h MTTR)	43
Tabelle B.15 – Wahrscheinlichkeit eines Ausfalls je Stunde für das Logik-Teilsystem in dem Beispiel für die Betriebsart mit hoher oder kontinuierlicher Anforderung (sechs Monate Wiederholungsprüfungsintervall und 8 h MTTR)	43
Tabelle B.16 – Wahrscheinlichkeit eines Ausfalls je Stunde für das Ausgangs-Teilsystem in dem Beispiel für die Betriebsart mit hoher oder kontinuierlicher Anforderung (sechs Monate Wiederholungsprüfungsintervall und 8 h MTTR)	44
Tabelle C.1 – Beispielberechnung für den Diagnosedeckungsgrad und den Anteil ungefährlicher Ausfälle	47
Tabelle C.2 – Diagnosedeckungsgrad und Wirksamkeit für verschiedene Teilsysteme	48
Tabelle D.1 – Anrechnung programmierbarer Elektronik oder Sensoren/Stellglieder	56
Tabelle D.2 – Werte für Z: programmierbare Elektronik	58
Tabelle D.3 – Werte für Z: Sensoren oder Stellglieder	58
Tabelle D.4 – Berechnung von β oder β_D	59
Tabelle D.5 – Beispielwerte für programmierbare Elektroniken	60
Tabelle E.1 – Spezifikation der Software-Sicherheitsanforderungen (siehe 7.2 der IEC 61508-3)	62
Tabelle E.2 – Software-Entwurf und -Entwicklung: Entwurf der Software-Architektur (siehe 7.4.3 der IEC 61508-3)	63
Tabelle E.3 – Software-Entwurf und -Entwicklung: Hilfswerkzeuge und Programmiersprachen (siehe 7.4.4 der IEC 61508-3)	63
Tabelle E.4 – Software-Entwurf und -Entwicklung: Detaillierter Entwurf (siehe 7.4.5 und 7.4.6 der IEC 61508-3)	64
Tabelle E.5 – Software-Entwurf und -Entwicklung: Test der Software-Module und der Integration der Software (siehe 7.4.7 und 7.4.8 der IEC 61508-3)	64
Tabelle E.6 – Integration der programmierbaren Elektronik (Hardware und Software) (siehe 7.5 der IEC 61508-3)	64
Tabelle E.7 – Validierung der Software bezüglich der Sicherheit (siehe 7.7 der IEC 61508-3)	65
Tabelle E.8 – Software-Modifikation (siehe 7.8 der IEC 61508-3)	65
Tabelle E.9 – Software-Verifikation (siehe 7.9 der IEC 61508-3)	65
Tabelle E.10 – Beurteilung der funktionalen Sicherheit (siehe Abschnitt 8 der IEC 61508-3)	65
Tabelle E.11 – Spezifikation der Software-Sicherheitsanforderungen (siehe 7.2 der IEC 61508-3)	67
Tabelle E.12 – Software-Entwurf und -Entwicklung: Entwurf der Software-Architektur (siehe 7.4.3 der IEC 61508-3)	67
Tabelle E.13 – Software-Entwurf und -Entwicklung: Hilfswerkzeuge und Programmiersprachen	

	Seite
(siehe 7.4.4 der IEC 61508-3).....	68
Tabelle E.14 – Software-Entwurf und -Entwicklung: Detaillierter Entwurf (siehe 7.4.5 und 7.4.6 der IEC 61508-3).....	68
Tabelle E.15 – Software-Entwurf und -Entwicklung: Test der Software-Module und -Integration (siehe 7.4.7 und 7.4.8 der IEC 61508-3).....	69
Tabelle E.16 – Integration der programmierbaren Elektronik (Hardware und Software) (siehe 7.5 der IEC 61508-3).....	69
Tabelle E.17 – Validierung der Softwaresicherheit (siehe 7.7 der IEC 61508-3).....	69
Tabelle E.18 – Software-Modifikation (siehe 7.8 der IEC 61508-3).....	69
Tabelle E.19 – Software-Verifikation (siehe 7.9 der IEC 61508-3)	70
Tabelle E.20 – Beurteilung der funktionalen Sicherheit (siehe Abschnitt 8 der IEC 61508-3).....	70

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 programmierbaren 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} je 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 6: Richtlinien für die Anwendung der IEC 61508-2 und IEC 61508-3

1 Anwendungsbereich

1.1 Dieser Teil der IEC 61508 enthält Informationen und Richtlinien für die IEC 61508-2 und IEC 61508-3.

- Anhang A liefert einen kurzen Überblick über die Anforderungen der IEC 61508-2 und der IEC 61508-3 und zeigt die funktionalen Schritte zu ihrer Anwendung.
- Anhang B zeigt ein Beispiel für die Verfahren zur Berechnung der Wahrscheinlichkeiten von Hardwareausfällen und sollte in Verbindung mit 7.4.3 und Anhang C und D der IEC 61508-2 gelesen werden.
- Anhang C zeigt ein ausgearbeitetes Beispiel für die Berechnung des Diagnosedeckungsgrads und sollte in Verbindung mit Anhang C der IEC 61508-2 gelesen werden.
- Anhang D zeigt eine Methode zur Quantifizierung der Auswirkungen von hardwarebezogenen Ausfällen infolge gemeinsamer Ursache auf die Ausfallwahrscheinlichkeit.
- Anhang E zeigt ausgearbeitete Beispiele für die Anwendung der Tabellen der Sicherheitsintegrität der Software, die im Anhang A der IEC 61508-3 für die Sicherheits-Integritätslevel 2 und 3 festgelegt sind.

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

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

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) anstelle der IEC 61508 verwendet werden, bis die beabsichtigte sektorspezifische Umsetzung der IEC 61508 (d. h. IEC 61511) als eine Internationale Norm in den USA und Kanada veröffentlicht wird.

1.4 Bild 1 zeigt den Gesamtrahmen für die Teile 1 bis 7 der IEC 61508 und zeigt die Rolle, die die IEC 61508-2 beim Erreichen der funktionalen Sicherheit für sicherheitsbezogene E/E/PE-Systeme spielt. Anhang A der IEC 61508-6 beschreibt die Anwendung der IEC 61508-2 und der IEC 61508-3.

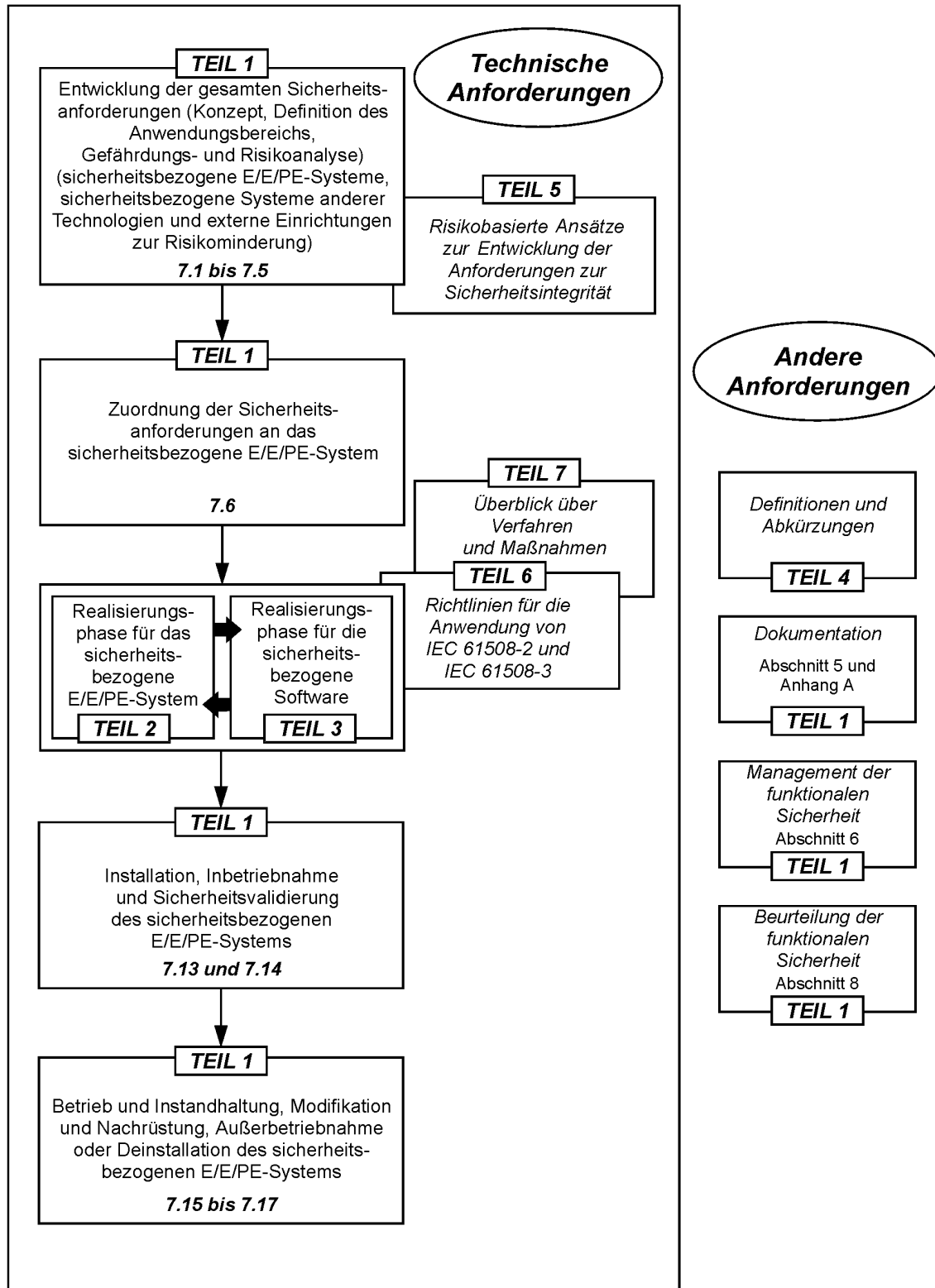


Bild 1 – Gesamtrahmen dieser Norm

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 Publikation nicht. Vertragspartner, deren Vereinbarungen auf diesem 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 IEC und ISO pflegen Verzeichnisse der gegenwärtig gültigen Internationalen Normen.

IEC 61508 (alle Teile), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

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

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

3 Begriffe und Abkürzungen

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

Anhang A (informativ)

Anwendung der IEC 61508-2 und der IEC 61508-3

A.1 Allgemeines

Eine Maschine, eine Prozessanlage und andere Betriebsmittel können im Fall einer Fehlfunktion (z. B. aufgrund von Ausfällen elektromechanischer, elektronischer und/oder programmierbarer elektronischer Geräte) durch gefahrbringende Ereignisse wie Feuer, Explosion, Überdosis von Strahlung oder in eine Maschine eingeschlossen werden, Risiken für Personen und die Umwelt darstellen. Ausfälle können entweder durch physikalische Fehler im Gerät (die z. B. zufällige Hardwareausfälle verursachen), durch systematische Fehler (z. B. kann menschliches Versagen bei der Spezifikation oder beim Entwurf systematische Ausfälle bei einer besonderen Kombination von Eingaben verursachen) oder durch Umgebungsbedingungen entstehen.

Die IEC 61508-1 liefert mit einem risikobasiertem Ansatz den gesamten Rahmen zur Vermeidung und/oder Beherrschung von Ausfällen in elektromechanischen, elektronischen oder programmierbaren elektronischen Geräten.

Das Hauptziel ist es, sicherzustellen, dass die Anlage und die Betriebsmittel sicher automatisiert werden können. Ein zentrales Ziel dieser Norm ist die Verhinderung von Folgendem:

- Ausfälle von Steuerungssystemen, die andere Ereignisse auslösen, die wiederum zu Gefahren (z. B. Brand, Freisetzen giftiger Stoffe, Wiederanlauf einer Maschine usw.) führen können, und
- unerkannte Ausfälle in Schutzsystemen (z. B. in einem Notabschaltsystem), die die Systeme im Falle eines notwendigen Sicherheitseingriffs unverfügbar machen.

Die IEC 61508-1 fordert, dass eine Gefährdungs- und Risikoanalyse auf Prozess-/Maschinenebene durchgeführt wird, um den für die Risikokriterien der Anwendung notwendigen Betrag der Risikominderung zu bestimmen. Das Risiko basiert auf der Beurteilung sowohl der Auswirkung (oder Schwere) als auch der Häufigkeit (oder Wahrscheinlichkeit) des gefahrbringenden Ereignisses.

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

Die IEC 61508-2 und die IEC 61508-3 nehmen die Sicherheitsfunktionen und Anforderungen an die Sicherheitsintegrität auf, die jedem System zugeordnet sind, das durch die Anwendung der IEC 61508-1 als sicherheitsbezogenes E/E/PE-System *bezeichnet* wird und legen die Anforderungen an die Tätigkeiten im Sicherheitslebenszyklus fest, die

- während der Spezifikation, des Entwurfs und der Modifikation der Hardware und Software angewendet werden müssen; und
- sich auf Mittel zur Verhinderung und/oder Beherrschung zufälliger Hardware- und systematischer Ausfälle (des E/E/PE und Sicherheitslebenszyklus der Software³⁾) konzentrieren.

¹⁾ Systeme, die für die funktionale Sicherheit notwendig sind und ein oder mehrere elektrische (elektromechanische), elektronische oder programmierbare elektronische (E/E/PE) Geräte beinhalten, werden als E/E/PE-sicherheitsbezogenes System bezeichnet und schließen alle Betriebsmittel ein, die zur Ausführung der erforderlichen Sicherheitsfunktionen (siehe 3.4.1 der IEC 61508-4) notwendig sind.

²⁾ Die Sicherheitsintegrität wird als eine von vier diskreten Stufen festgelegt. Der Sicherheits-Integritätslevel 4 ist die höchste und 1 die niedrigste (siehe 7.6.2.9 der IEC 61508-1).

³⁾ Um den Anforderungen dieser Norm eine eindeutige Struktur zu geben, wurde die Entscheidung getroffen, die Anforderungen unter Verwendung eines Modells des Entwicklungsprozesses zu ordnen, in dem die Stufen in einer definierten Reihenfolge mit geringer Iteration (manchmal auch Wasserfallmodell genannt) aufeinander folgen. Es sei jedoch hervor gehoben, dass jeder Ansatz für einen Lebenszyklus verwendet werden kann, vorausgesetzt, dass eine Aussage zur Gleichwertigkeit im Sicherheitsplan für das Projekt (siehe Abschnitt 6 der IEC 61508-1) gemacht worden ist.

Die IEC 61508-2 und die IEC 61508-3 geben keine Anleitung, welches Sicherheits-Integritätslevel für ein gegebenes tolerierbares Risiko angemessen ist. Diese Entscheidung hängt von vielen Faktoren ab, einschließlich der Art der Anwendung, dem Maß, in dem andere Systeme Sicherheitsfunktionen ausführen, und von gesellschaftlichen und wirtschaftlichen Gegebenheiten (siehe IEC 61508-1 und IEC 61508-5).

Die Anforderungen der IEC 61508-2 und der IEC 61508-3 beinhalten:

- die Anwendung von Maßnahmen und Verfahren⁴⁾, abgestuft gegen den Sicherheits-Integritätslevel, zur Vermeidung systematischer Ausfälle⁵⁾ durch vermeidende Methoden und
- die Beherrschung systematischer Ausfälle (einschließlich Softwarefehler) und zufälliger Hardwareausfälle durch Entwurfsmerkmale wie Fehleraufdeckung, Redundanz und strukturelle Merkmale (z. B. Diversität).

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

- den Anforderungen zur Hardware-Fehlertoleranz (siehe Tabellen 2 und 3 der IEC 61508-2) und
- dem Diagnosedeckungsgrad und der Häufigkeit von Wiederholungsprüfungen von Teilsystemen und Bauteilen, indem eine Zuverlässigkeitsanalyse unter Verwendung angemessener Daten ausgeführt wird.

Sowohl in der IEC 61508-2 als auch in der IEC 61508-3 wird die Zusicherung, dass das Ziel der Sicherheitsintegrität für systematische Ausfälle erreicht worden ist, aufgrund

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

gegeben.

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

Die IEC 61508-2 ist entwickelt worden, um Anforderungen zum Erreichen der Sicherheitsintegrität der Hardware⁸⁾ des sicherheitsbezogenen E/E/PE-Systems einschließlich Sensoren und Stellgliedern zur Verfügung zu stellen. Verfahren und Maßnahmen werden sowohl gegen zufällige Hardwareausfälle als auch gegen systematische Hardwareausfälle gefordert. Diese beinhalten, wie oben dargelegt, eine angemessene Kombination von fehlervermeidenden und ausfallbeherrschenden Maßnahmen. Wird ein Bedienereingriff für die funktionale Sicherheit benötigt, werden Anforderungen an die Bedienerschnittstelle gestellt. In der IEC 61508-2 werden ebenfalls auf Software und Hardware (z. B. Diversität) basierende Diagnosetest-Verfahren und -Maßnahmen zur Aufdeckung zufälliger Hardwareausfälle festgelegt.

Die IEC 61508-3 ist entwickelt worden, um Anforderungen zum Erreichen der Sicherheitsintegrität der Software, und zwar sowohl der Embedded-Software (einschließlich Dienste für Diagnose und Fehleraufdeckung) als auch der Anwendungssoftware, zur Verfügung zu stellen. Die IEC 61508-3 fordert eine Kombination von Ansätzen zur Fehlervermeidung (Qualitätssicherung) und Fehlertoleranz (Softwarearchitektur), da es keinen bekannten Weg zum Nachweis der Fehlerfreiheit in einigermaßen komplexer sicherheitsbezogener Software, besonders der Freiheit von Spezifikations- und Entwurfsfehlern, gibt. Die IEC 61508-3 fordert die Anwendung

⁴⁾ Die für jeden Sicherheits-Integritätslevel geforderten Techniken und Maßnahmen werden in den Tabellen in den Anhängen A und B der IEC 61508-2 und IEC 61508-3 gezeigt.

⁵⁾ Systematische Ausfälle können gewöhnlich nicht quantifiziert werden. Ursachen hierfür sind u. a.: Spezifikations- und Entwurfsfehler in Hardware und Software; Ausfälle auf Grund der Umgebungsbedingungen (z. B. Temperatur) und betriebsbedingte Fehler (z. B. eine schlechte Schnittstelle).

⁶⁾ Andere als in dieser Norm festgelegte Maßnahmen sind ebenfalls annehmbar, wenn sie während der Sicherheitsplanung schriftlich begründet werden (siehe Abschnitt 6 der IEC 61508-1).

⁷⁾ Eine unabhängige Beurteilung bedeutet nicht unbedingt eine Beurteilung durch Dritte (siehe Abschnitt 8 der IEC 61508-1).

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

von Software-Entwurfsprinzipien wie Top-Down-Entwurf, Modularität, Verifikation jeder Phase des Entwicklungslebenszyklus, geprüfte Software-Module und Software-Modul-Bibliotheken und verständliche Dokumentation, um die Verifikation und Validierung zu erleichtern. Die verschiedenen Stufen der Software erfordern verschiedene Stufen an Zusicherung, dass diese und ähnliche Prinzipien richtig angewendet worden sind.

Der Softwareentwickler darf, muss aber nicht, unabhängig von der Organisation sein, die die gesamte E/E/PES-Entwicklung durchführt. In jedem Fall ist eine enge Zusammenarbeit notwendig, insbesondere bei der Entwicklung der Architektur der programmierbaren Elektronik, wo die Abwägungen zwischen Hardware- und Softwarearchitektur im Hinblick auf die Auswirkungen auf die Sicherheit (siehe **Bild 4 der IEC 61508-2**) durchgeführt werden müssen.

A.2 Funktionale Schritte in der Anwendung der IEC 61508-2

Die funktionalen Schritte zur Anwendung der IEC 61508-2 werden in den **Bildern A.1 und A.2** gezeigt, die zur Anwendung der IEC 61508-3 in **Bild A.3**.

Die funktionalen Schritte der IEC 61508-2 (siehe **Bilder A.1 und A.2**) sind wie folgt:

- a) Erhalt der Zuordnung der Sicherheitsanforderungen (siehe **IEC 61508-1**). Angemessene Aktualisierung der Sicherheitsplanung während der E/E/PES-Entwicklung.
- b) Bestimmung der Anforderungen für die E/E/PES-Sicherheit, einschließlich der Anforderungen zur Sicherheitsintegrität für jede Sicherheitsfunktion (siehe **7.2 der IEC 61508-2**). Zuweisung der Anforderungen an die Software und Übergabe an die Softwarelieferanten und/oder Entwickler für die Anwendung der **IEC 61508-3**.

ANMERKUNG 1 An dieser Stelle ist es notwendig, die Möglichkeit gleichzeitiger Ausfälle im EUC-Leit- und Steuersystem und E/E/PE-sicherheitsbezogenen System(en) zu berücksichtigen (siehe **7.5.2.4 der IEC 61508-1**). Diese können aus Bauteilausfällen infolge gemeinsamer Ursache, z. B. gleichartigen Umgebungseinflüssen, herrühren. Bei ungenügender Berücksichtigung kann das Vorhandensein solcher Ausfälle zu einem höheren als dem erwarteten Restrisiko führen.

- c) Start der Phase für die Planung der Validierung bezüglich der Sicherheit des E/E/PES (siehe **7.3 der IEC 61508-2**).
- d) Spezifikation der Architektur (Konfiguration) für das Logik-Teilsystem des E/E/PES, Sensoren und Stellglieder. Überprüfung der Hardware- und Softwarearchitektur und der sicherheitstechnischen Auswirkungen der Abwägungen zwischen Hardware und Software (siehe **Bild 4 der IEC 61508-2**) mit dem Softwarelieferanten/Entwickler. Falls notwendig, Wiederholung dieses Schrittes.
- e) Entwicklung eines Modells für die Hardwarearchitektur des sicherheitsbezogenen E/E/PE-Systems. Entwicklung dieses Modell durch getrennten Test jeder Sicherheitsfunktion und Bestimmung jedes Teilsystems (Bauteils), das zur Ausführung dieser Funktion verwendet wird.
- f) Festlegung der Systemparameter für jedes der Teilsysteme (Bauteile), die in dem sicherheitsbezogenen E/E/PE-System verwendet werden. Für jedes wird Folgendes bestimmt:
 - das Wiederholungsprüfungsintervall für Ausfälle, die nicht automatisch aufgedeckt werden;
 - die mittlere Zeit zur Wiederherstellung;
 - der Diagnosedeckungsgrad (siehe **Anhang C der IEC 61508-2**).
 - die Ausfallwahrscheinlichkeit; und
 - der Anteil sicherer Ausfälle (siehe **Anhang C der IEC 61508-2**)
- g) Bestimmung der Einschränkungen auf Grund der Architektur (siehe **Tabellen 2 und 3 der IEC 61508-2**).
- h) Bildung eines Zuverlässigkeitsmodells für jede Sicherheitsfunktion, die das sicherheitsbezogene E/E/PE-System ausführen muss.

ANMERKUNG 2 Ein Zuverlässigkeitsmodell ist eine mathematische Gleichung, die die Beziehung zwischen der Verfügbarkeit und den relevanten Parametern der Einrichtung und der Einsatzbedingungen zeigt.

- i) Berechnung einer Zuverlässigkeitsvoraussage für jede Sicherheitsfunktion unter Verwendung eines angemessenen Verfahrens. Vergleich des Ergebnisses mit dem oben in b) festgelegten Ausfallgrenzwert und den Anforderungen der **Tabellen 2 und 3 der IEC 61508** (siehe **7.4.3.1 der IEC 61508-2**). Falls die vorausgesagte Zuverlässigkeit nicht den Ausfallgrenzwert erreicht und/oder nicht den Anforderungen der **Tabellen 2 und 3 der IEC 61508-2** entspricht, dann wird Folgendes geändert:

- wenn möglich, einen oder mehrere der Teilsystem-Parameter (zurückgehen zu f) oben) und/oder
- die Hardwarearchitektur (zurückgehen zu d) oben).

ANMERKUNG 3 Eine Anzahl von Methoden zur Modellierung steht zur Verfügung, und der Analytiker sollte wählen, welche die geeignetste ist (siehe 7.4.3.2.2, Anmerkung 9 der IEC 61508-2 für die Liste einiger Methoden, die verwendet werden können).

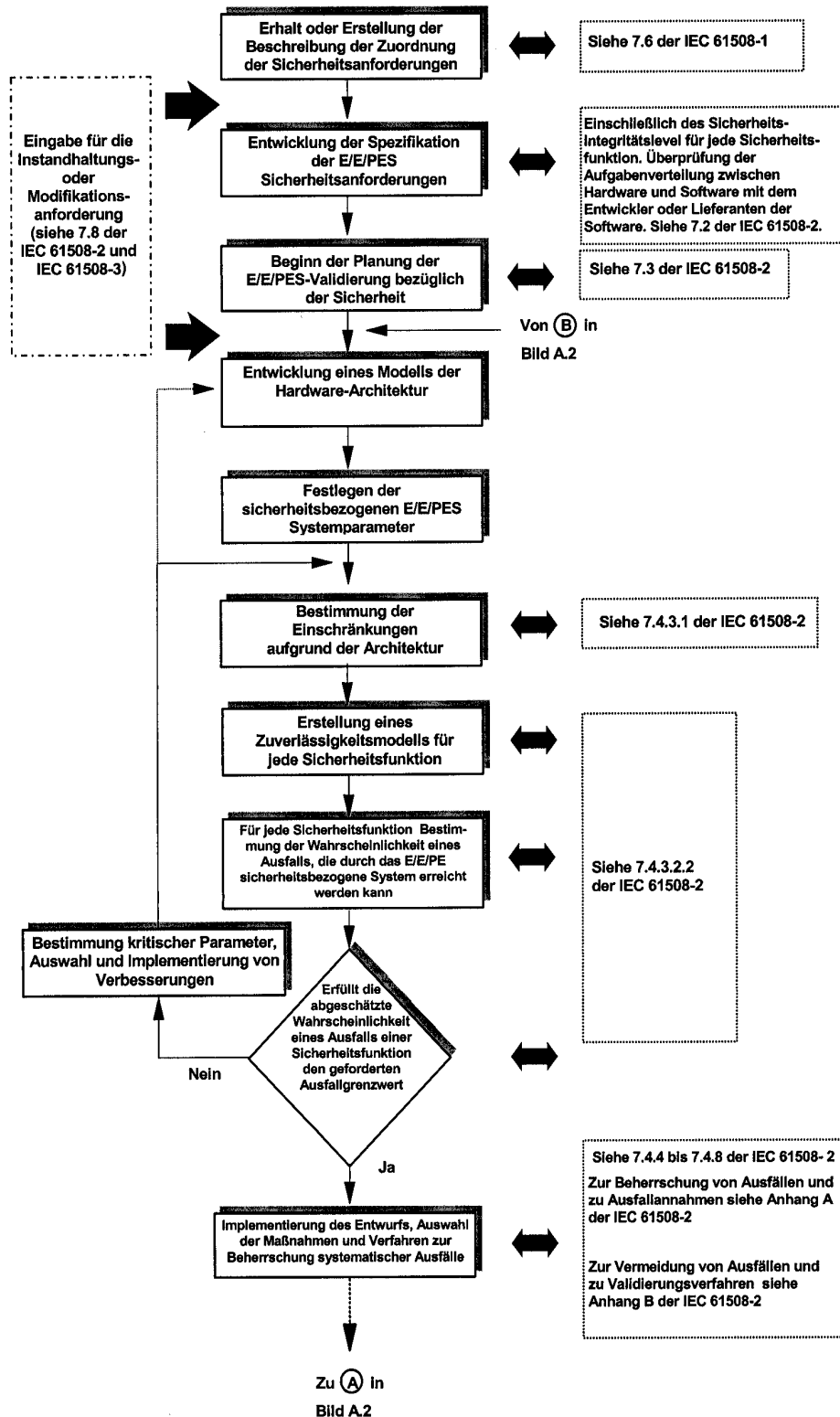
- j) Implementierung des Entwurfs des sicherheitsbezogenen E/E/PE-Systems. Auswahl von Maßnahmen und Verfahren, um systematische Hardwareausfälle, Ausfälle durch Umwelteinflüsse und Bedienungsfehler (siehe Anhang A der IEC 61508-2) zu beherrschen.
- k) Integration der verifizierten Software (siehe IEC 61508-3) in die Ziel-Hardware (siehe 7.5 der IEC 61508-2 und Anhang B der IEC 61508-2) und parallel dazu die Entwicklung der Verfahren, denen Anwender und Instandhaltungspersonal beim Betrieb des Systems zu folgen haben (siehe 7.6 der IEC 61508-2 und Anhang B der IEC 61508-2). Berücksichtigung der Softwareaspekte (siehe A.3 f)).
- l) Validierung des E/E/PES (siehe 7.7 der IEC 61508-2 und Anhang B der IEC 61508-2) zusammen mit dem Softwareentwickler (siehe 7.7 der IEC 61508-3).
- m) Übergabe der Hardware und Ergebnisse der Validierung des E/E/PES bezüglich der Sicherheit an die Systemingenieure für die weitere Integration in das Gesamtsystem.
- n) Falls eine Instandhaltung/Modifikation des E/E/PES während der Betriebszeit notwendig wird, erneute Anwendung der IEC 61508-2, sofern angebracht (siehe 7.8 der IEC 61508-2).

Einige Tätigkeiten finden im gesamten Sicherheitslebenszyklus des E/E/PES statt. Darunter sind die Verifikation (siehe 7.9 der IEC 61508-2) und die Beurteilung der funktionalen Sicherheit (siehe Abschnitt 8 der IEC 61508-1).

Durch Anwendung der obigen Schritte werden E/E/PES-Sicherheits-Verfahren und Maßnahmen im Hinblick auf das erforderliche Sicherheits-Integritätslevel ausgewählt. Zur Hilfestellung bei dieser Auswahl sind Tabellen mit der Einordnung der verschiedenen Verfahren/Maßnahmen unter die vier Sicherheits-Integritätslevel (siehe Anhang B der IEC 61508-2) formuliert worden. Aus den Tabellen wird für jedes Verfahren und jede Maßnahme auf eine Kurzbeschreibung mit Literaturhinweisen verwiesen (siehe Anhang A und B der IEC 61508-7).

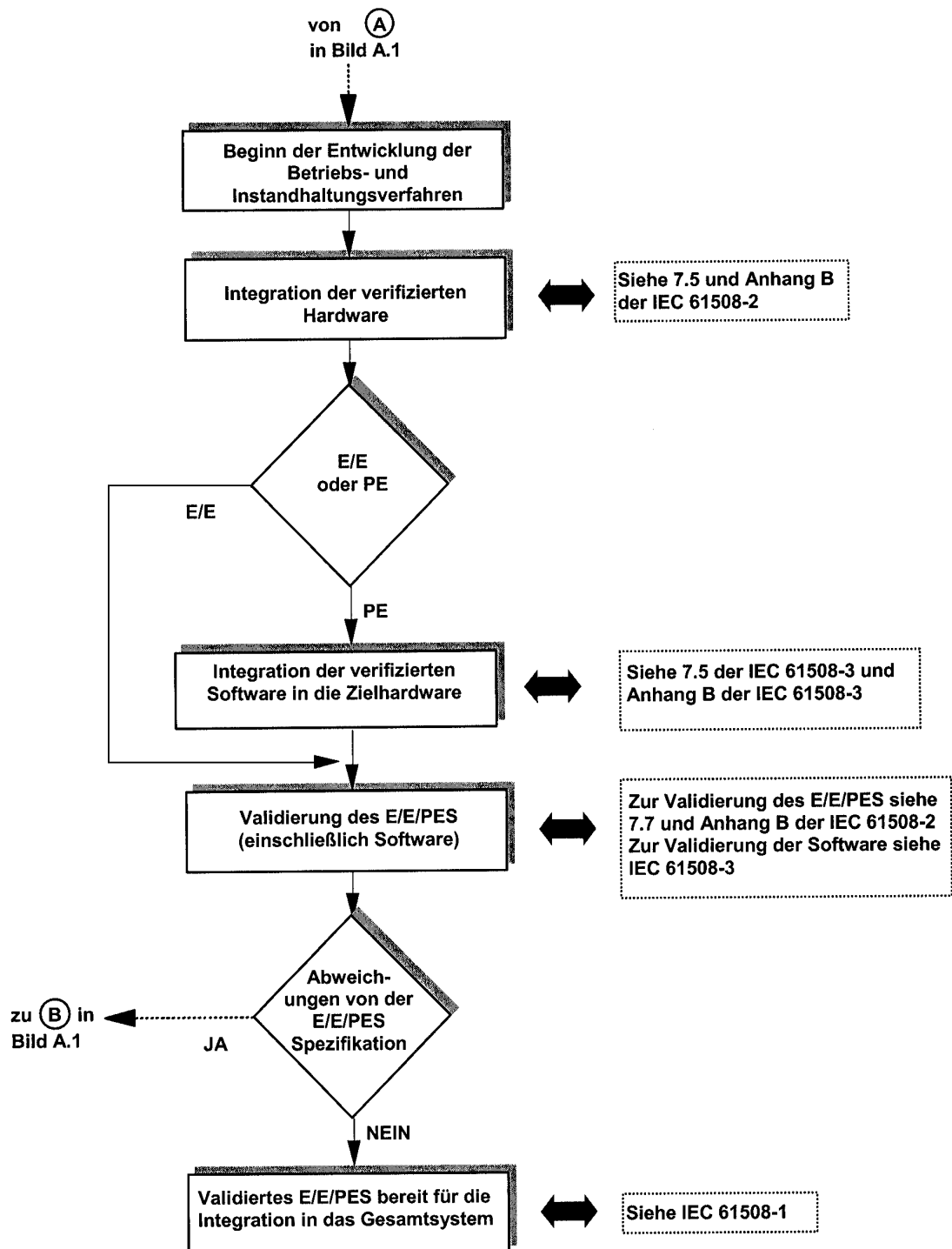
Anhang B stellt ein mögliches Verfahren zur Berechnung der Wahrscheinlichkeiten von Hardwareausfällen für sicherheitsbezogene E/E/PE-Systeme vor.

ANMERKUNG 4 Andere als in der Norm festgelegte Maßnahmen sind bei der Anwendung dieser Schritte ebenfalls annehmbar, wenn sie während der Sicherheitsplanung schriftlich begründet werden (siehe Abschnitt 6 der IEC 61508-1).



ANMERKUNG Bei programmierbaren elektronischen Systemen werden gleichzeitig die Software-Tätigkeiten ausgeführt.

Bild A.1 – Anwendung der IEC 61508-2



ANMERKUNG Bei programmierbaren elektronischen Systemen werden gleichzeitig die Software-Tätigkeiten ausgeführt.

Bild A.2 – Anwendung der IEC 61508-2 (Fortsetzung)

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

Die funktionalen Schritte der IEC 61508-3 (siehe Bild A.3) sind wie folgt.

- a) Erhalt der Anforderungen an die sicherheitsbezogenen E/E/PE-Systeme und der zutreffenden Teile der Sicherheitsplanung (siehe 7.3 der IEC 61508-2). Angemessene Aktualisierung der Sicherheitsplanung während der Softwareentwicklung.

ANMERKUNG 1 Frühere Lebenszyklusphasen haben bereits

- die erforderlichen Sicherheitsfunktionen und ihre Sicherheits-Integritätslevel festgelegt (siehe 7.4 und 7.5 der IEC 61508-1);
 - die Sicherheitsfunktionen sicherheitsbezogenen E/E/PE-Systemen zugewiesen (siehe 7.6 der IEC 61508-1); und
 - der Software innerhalb jedes sicherheitsbezogenen E/E/PE-Systems Funktionen zugewiesen (siehe 7.2 der IEC 61508-2).
- b) Bestimmung der Softwarearchitektur für alle Sicherheitsfunktionen, die der Software zugewiesen worden sind (siehe 7.4 der IEC 61508-3 und Anhang A der IEC 61508-3).
- c) Überprüfung der Software und Hardwarearchitektur und der sicherheitstechnischen Auswirkungen der Abwägungen zwischen Software und Hardware (siehe Bild 4 der IEC 61508-2) mit dem E/E/PES-Lieferanten/Entwickler. Falls notwendig, Wiederholung dieses Schrittes.
- d) Beginn der Planung für die Verifikation und Validierung der Software bezüglich der Sicherheit (siehe 7.3 und 7.9 der IEC 61508-3).
- e) Entwurf, Entwicklung und Verifizieren/Testen der Software nach:
- der Planung der Softwaresicherheit,
 - dem Software-Sicherheits-Integritätslevel und
 - dem Sicherheitslebenszyklus der Software.
- f) Vervollständigen der abschließenden Tätigkeiten der Softwareverifikation und Integration der verifizierten Software in die Zielhardware (siehe 7.5 der IEC 61508-3) und parallel dazu Entwicklung der Softwareaspekte der Verfahren, denen Anwender und Instandhaltungspersonal beim Betrieb des Systems zu folgen haben (siehe 7.6 der IEC 61508-3 und A.2 k)).
- g) Validierung der Software des integrierten sicherheitsbezogenen E/E/PE-Systems (siehe 7.7 der IEC 61508-3) zusammen mit dem Hardwareentwickler (siehe 7.7 der IEC 61508-2).
- h) Übergabe der Ergebnisse der Validierung der Software bezüglich der Sicherheit an die Systemingenieure für die weitere Integration in das Gesamtsystem.
- i) Falls eine Modifikation der E/E/PES-Software während der Betriebszeit notwendig wird, erneute Anwendung der IEC 61508-3 (siehe 7.8 der IEC 61508-3), sofern angebracht.

Einige Tätigkeiten finden im gesamten Sicherheitslebenszyklus des E/E/PES statt. Darunter sind die Verifikation (siehe 7.9 der IEC 61508-3) und die Beurteilung der funktionalen Sicherheit (siehe Abschnitt 8 der IEC 61508-3).

Durch Anwendung der obigen Schritte werden E/E/PES-Sicherheits-Verfahren und Maßnahmen im Hinblick auf das erforderliche Sicherheits-Integritätslevel ausgewählt. Zur Hilfestellung bei dieser Auswahl sind Tabellen mit der Einordnung der verschiedenen Verfahren/Maßnahmen unter die vier Sicherheits-Integritätslevel (siehe Anhang A der IEC 61508-3) formuliert worden. Aus den Tabellen wird für jedes Verfahren und jede Maßnahme auf eine Kurzbeschreibung mit Literaturhinweisen verwiesen (siehe Anhang C der IEC 61508-7).

Ausgearbeitete Beispiele für die Anwendung der Tabellen zur Sicherheitsintegrität werden in Anhang E gegeben, und die IEC 61508-7 beinhaltet einen probabilistischen Ansatz für die Bestimmung der Sicherheitsintegrität von vorentwickelter Software (siehe Anhang D der IEC 61508-7).

ANMERKUNG 2 Andere als in dieser Norm festgelegte Maßnahmen sind bei der Anwendung dieser Schritte ebenfalls annehmbar, wenn sie während der Sicherheitsplanung schriftlich begründet werden (siehe Abschnitt 6 der IEC 61508-1).

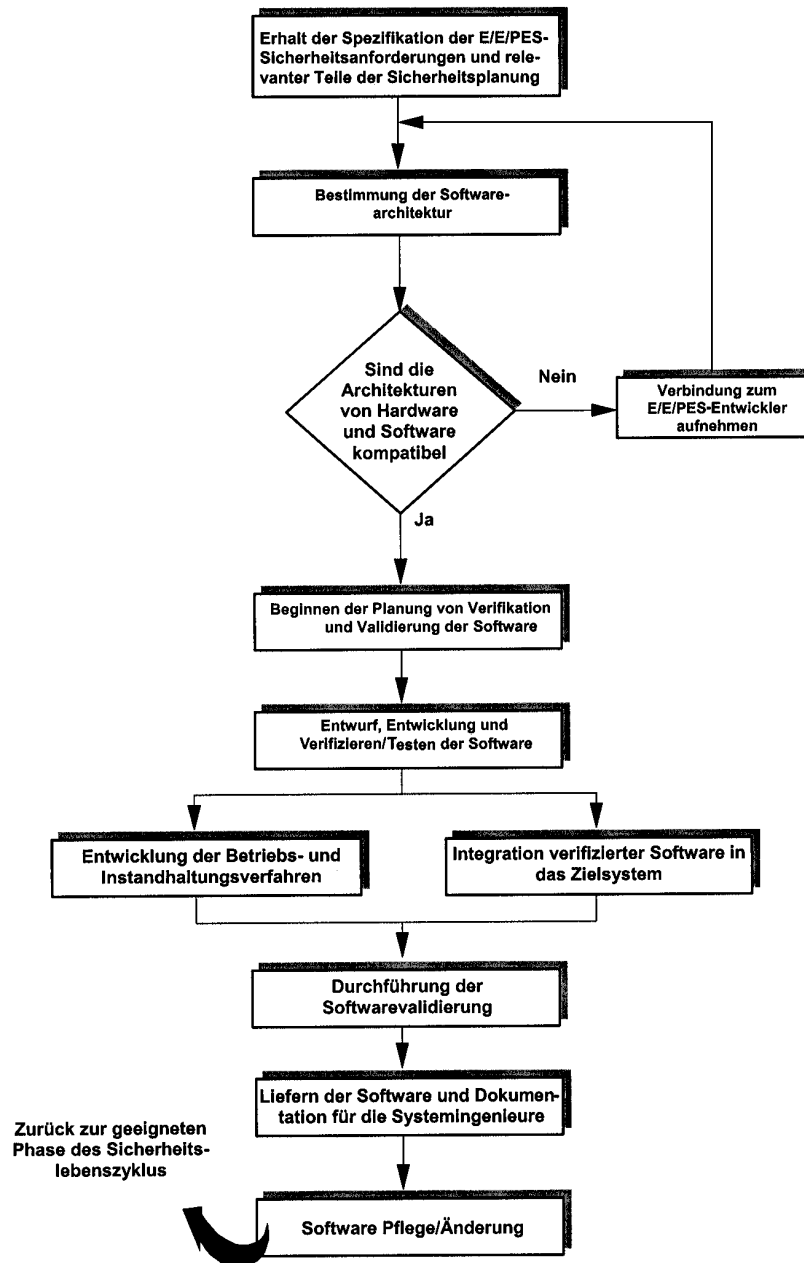


Bild A.3 – Anwendung der IEC 61508-3