

	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 61508-2
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 2
ICS 25.040.40 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems (IEC 61508-2:2000); German version EN 61508-2:2001 Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Prescriptions pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité (CEI 61508-2:2000); Version allemande EN 61508-2:2001 Die Europäische Norm EN 61508-2:2001 hat den Status einer Deutschen Norm. Beginn der Gültigkeit Die EN 61508-2 wurde am 2001-07-03 angenommen. Nationales Vorwort Anwendungsrichtlinie: DIN EN 61508-6 (VDE 0803 Teil 6) 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/254/CDV:1998-08. Die enthaltene IEC-Publikation wurde vom SC 65A „System aspects“ erarbeitet. Sie ist eine Sicherheits-Grundnorm, siehe hierzu auch 1.2. Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zum Jahr 2006 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 bis 4 und 74 Seiten EN DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

DIN EN 61508-2 (VDE 0803 Teil 2):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 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
–	IEC 60050(371):1984	IEV-Kapitel 371	–
–	IEC 60300-3-2:1993	DIN IEC 60300-3-2:2002	–
–	IEC 61000-1-1:1992	–	–
–	IEC 61000-2-5:1995	–	–
EN 61508-1:2001	IEC 61508-1:1998	DIN EN 61508-1 (VDE 0803 Teil 1):2002-11	VDE 0803 Teil 1
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

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
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
–	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 61508-3 (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 61508-6 (VDE 0803 Teil 6), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für die IEC 61508-2 und IEC 61508-3 (IEC 61508-6:2000); Deutsche Fassung EN 61508-6:2001.*

DIN EN 61508-7 (VDE 0803 Teil 7), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 7: Anwendungshinweise über Verfahren und Maßnahmen (IEC 61508-7:2000); Deutsche Fassung EN 61508-7:2001.*

E DIN IEC 60300-3-2:2002, *Zuverlässigkeitsmanagement – Teil 3-2: Anwendungsleitfaden; Erfassung von Zuverlässigkeitsdaten im Betrieb (IEC 56/785/CD:2002, Text Englisch).*

**Funktionale Sicherheit sicherheitsbezogener
elektrischer/elektronischer/programmierbarer elektronischer Systeme –
Teil 2: Anforderungen an sicherheitsbezogene
elektrische/elektronische/programmierbare elektronische Systeme
(IEC 61508-2:2000)**

Functional safety of
electrical/electronic/programmable electronic
safety-related systems –
Part 2: Requirements for
electrical/electronic/programmable electronic
safety-related systems
(IEC 61508-2:2000)

Sécurité fonctionnelle des systèmes
électriques/électroniques/électroniques
programmables relatifs à la sécurité –
Partie 2: Prescriptions pour les systèmes
électriques/électroniques/électroniques
programmables relatifs à la sécurité
(CEI 61508-2:2000)

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 61508-2:2000, 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 61508-2 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 Norm-Inhalt.

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

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 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 61508-2:2000 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

Inhalt

	Seite
Vorwort	2
Einleitung.....	5
1 Anwendungsbereich	7
2 Normative Verweisungen.....	10
3 Begriffe und Abkürzungen	10
4 Übereinstimmung mit dieser Norm	10
5 Dokumentation	11
6 Management der funktionalen Sicherheit	11
7 Anforderungen zum E/E/PES-Sicherheitslebenszyklus	11
7.1 Allgemeines.....	11
7.2 Spezifikation der E/E/PES-Sicherheitsanforderungen.....	15
7.3 Planung der Validierung der sicherheitsbezogenen E/E/PE-Systeme bezüglich der Sicherheit	18
7.4 E/E/PES-Entwurf und Entwicklung	18
7.5 E/E/PES-Integration.....	36
7.6 E/E/PES-Betriebs- und Instandhaltungsverfahren	37
7.7 Validierung der E/E/PES bezüglich der Sicherheit	38
7.8 E/E/PES-Modifikation.....	40
7.9 E/E/PES-Verifikation	40
8 Beurteilung der funktionalen Sicherheit	42
Anhang A (normativ) Verfahren und Maßnahmen für sicherheitsbezogene E/E/PE-Systeme: Beherrschung von Ausfällen während des Betriebs	43
A.1 Allgemeines.....	43
A.2 Sicherheitsintegrität der Hardware	44
A.3 Systematische Sicherheitsintegrität.....	54
Anhang B (normativ) Verfahren und Maßnahmen für sicherheitsbezogene E/E/PE-Systeme: Vermeidung von systematischen Ausfällen während der verschiedenen Phasen des Lebenszyklus	59
Anhang C (normativ) Diagnosedeckungsgrad und Anteil ungefährlicher Ausfälle	69
C.1 Berechnung von Diagnosedeckungsgrad und dem Anteil ungefährlicher Ausfälle eines Teilsystems	69
C.2 Bestimmung von Diagnosedeckungsfaktoren	70
Literaturhinweise	72
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen.....	73
Bilder	
Bild 1 – Gesamtrahmen dieser Norm.....	9
Bild 2 – E/E/PES-Sicherheitslebenszyklus (in der Realisierungsphase)	12
Bild 3 – Beziehung zwischen der IEC 61508-2 und IEC 61508-3 und ihrer Anwendungsbereiche	13
Bild 4 – Beziehung zwischen den Hardware- und Software-Architekturen von programmierbarer Elektronik	20
Bild 5 – Beispiel der Begrenzung der Sicherheitsintegrität der Hardware für eine einkanalige	

	Seite
Sicherheitsfunktion	25
Bild 6 – Beispiel der Begrenzung der Sicherheitsintegrität der Hardware für eine mehrkanalige Sicherheitsfunktion	27
Tabellen	
Tabelle 1 – Überblick – Realisierungsphase des E/E/PES-Sicherheitslebenszyklus	14
Tabelle 2 – Sicherheitsintegrität der Hardware: Einschränkungen aufgrund der Architektur für sicherheitsbezogene Typ A-Teilsysteme	24
Tabelle 3 – Sicherheitsintegrität der Hardware: Einschränkungen aufgrund der Architektur für sicherheitsbezogene Typ B-Teilsysteme	24
Tabelle A.1 – Fehler oder Ausfälle, die während des Betriebs erkannt oder zur Bestimmung des Anteils ungefährlicher Ausfälle analysiert werden müssen	45
Tabelle A.2 – Elektrische Teilsysteme	47
Tabelle A.3 – Elektronische Teilsysteme	47
Tabelle A.4 – Verarbeitungseinheiten	48
Tabelle A.5 – Unveränderliche Speicherbereiche	48
Tabelle A.6 – Veränderliche Speicherbereiche	49
Tabelle A.7 – E/A-Einheiten und Schnittstellen (externe Kommunikation)	49
Tabelle A.8 – Datenwege (interne Kommunikation)	50
Tabelle A.9 – Energieversorgung	50
Tabelle A.10 – Programmablauf (Watchdog)	51
Tabelle A.11 – Lüftung und Beheizungssystem (falls notwendig)	51
Tabelle A.12 – Takt	52
Tabelle A.13 – Kommunikation und Massenspeicher	52
Tabelle A.14 – Sensoren	53
Tabelle A.15 – Stellglieder (Aktoren)	53
Tabelle A.16 – Verfahren und Maßnahmen zur Beherrschung von durch den Hardwareentwurf und den Softwareentwurf verursachten systematischen Ausfällen	55
Tabelle A.17 – Verfahren und Maßnahmen zur Beherrschung von durch umgebungsbedingte Beanspruchung oder Einflüsse verursachten systematischen Ausfällen	56
Tabelle A.18 – Verfahren und Maßnahmen zur Beherrschung von systematischen Ausfällen während des Betriebs	57
Tabelle A.19 – Wirksamkeit von Verfahren und Maßnahmen zur Beherrschung von systematischen Ausfällen	58
Tabelle B.1 – Empfehlungen zur Vermeidung von Irrtümern während der Spezifikation der E/E/PES-Anforderungen (siehe 7.2)	61
Tabelle B.2 – Empfehlungen zur Vermeidung von Fehlern während des E/E/PES-Entwurfs und der Entwicklung (siehe 7.4)	62
Tabelle B.3 – Empfehlungen zur Vermeidung von Fehlern während der E/E/PES-Integration (siehe 7.5)	63
Tabelle B.4 – Empfehlungen zur Vermeidung von Fehlern und Ausfällen während der E/E/PES-Betriebs- und Instandhaltungsverfahren (siehe 7.6)	64
Tabelle B.5 – Empfehlungen zur Vermeidung von Fehlern während der Validierung der E/E/PES bezüglich der Sicherheit (siehe 7.7)	65
Tabelle B.6 – Wirksamkeit von Verfahren und Maßnahmen zur Vermeidung von systematischen Ausfällen	66

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/programmierbare 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/programmierbaren 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, die 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, Verfahren 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 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/ programmierbar elektronische Systeme

1 Anwendungsbereich

1.1 Dieser Teil der IEC 61508:

- a) ist dazu vorgesehen, nur nach einem gründlichen Verständnis der IEC 61508-1 angewendet zu werden, die den gesamten Rahmen für die Erreichung der funktionalen Sicherheit bereitstellt;
- b) ist für jedes sicherheitsbezogene System, wie durch die IEC 61508-1 definiert, anwendbar, das mindestens ein elektrisches, elektronisches oder programmierbares elektronisches Bauteil enthält;
- c) ist auf Teilsysteme und ihre Bauteile innerhalb eines sicherheitsbezogenen E/E/PE-Systems anwendbar (einschließlich Sensoren, Aktoren und der Bedienerschnittstelle);
- d) legt fest, wie die in Übereinstimmung mit der IEC 61508-1 entwickelten Informationen in Bezug auf die gesamten Sicherheitsanforderungen und ihre Zuordnung zu den sicherheitsbezogenen E/E/PE-Systemen verfeinert werden und legt fest, wie die gesamten Sicherheitsanforderungen in funktionale E/E/PE-Sicherheitsanforderungen und sicherheitsbezogene E/E/PE-Integritätsanforderungen verfeinert werden;
- e) legt Anforderungen für Tätigkeiten fest, die während des Entwurfs und der Herstellung der sicherheitsbezogenen E/E/PE-Systeme anzuwenden sind (z. B. legt er das Modell des E/E/PE-Sicherheitslebenszyklus fest), außer für Software, die in der IEC 61508-3 behandelt wird (siehe die Bilder 2 und 3). Diese Anforderungen schließen die Anwendung von Verfahren und Maßnahmen zur Vermeidung und Beherrschung von Fehlern und Ausfällen ein, die dem Sicherheits-Integritätslevel entsprechend abgestuft sind;
- f) legt die notwendigen Informationen zur Ausführung der Installation, Inbetriebnahme und der abschließenden Validierung der sicherheitsbezogenen E/E/PE-Systeme bezüglich der Sicherheit fest;
- g) richtet sich nicht an die Betriebs- und Instandhaltungsphase der sicherheitsbezogenen E/E/PE-Systeme – diese werden in der IEC 61508-1 behandelt – jedoch stellt die IEC 61508-2 Anforderungen für die Vorbereitung von Informationen und Verfahren bereit, die vom Anwender für den Betrieb und die Instandhaltung der sicherheitsbezogenen E/E/PE-Systeme benötigt werden;
- h) legt die Anforderungen fest, die durch die Organisation zu erfüllen sind, die irgendeine Modifikation der sicherheitsbezogenen E/E/PE-Systeme ausführt.

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

ANMERKUNG 2 Bild 3 zeigt die Beziehung zwischen der IEC 61508-2 und der IEC 61508-3.

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.

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 dieser Technischen Komitees speziell darauf verwiesen wird oder diese eingebunden werden.

ANMERKUNG 1 Die funktionale Sicherheit eines sicherheitsbezogenen E/E/PE-Systems kann nur erreicht werden, wenn alle zutreffenden Anforderungen erfüllt werden. Daher ist es wichtig, dass alle zutreffenden Anforderungen sorgfältig betrachtet und angemessen in Bezug genommen werden.

EN 61508-2:2001

ANMERKUNG 2 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.

1.3 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.

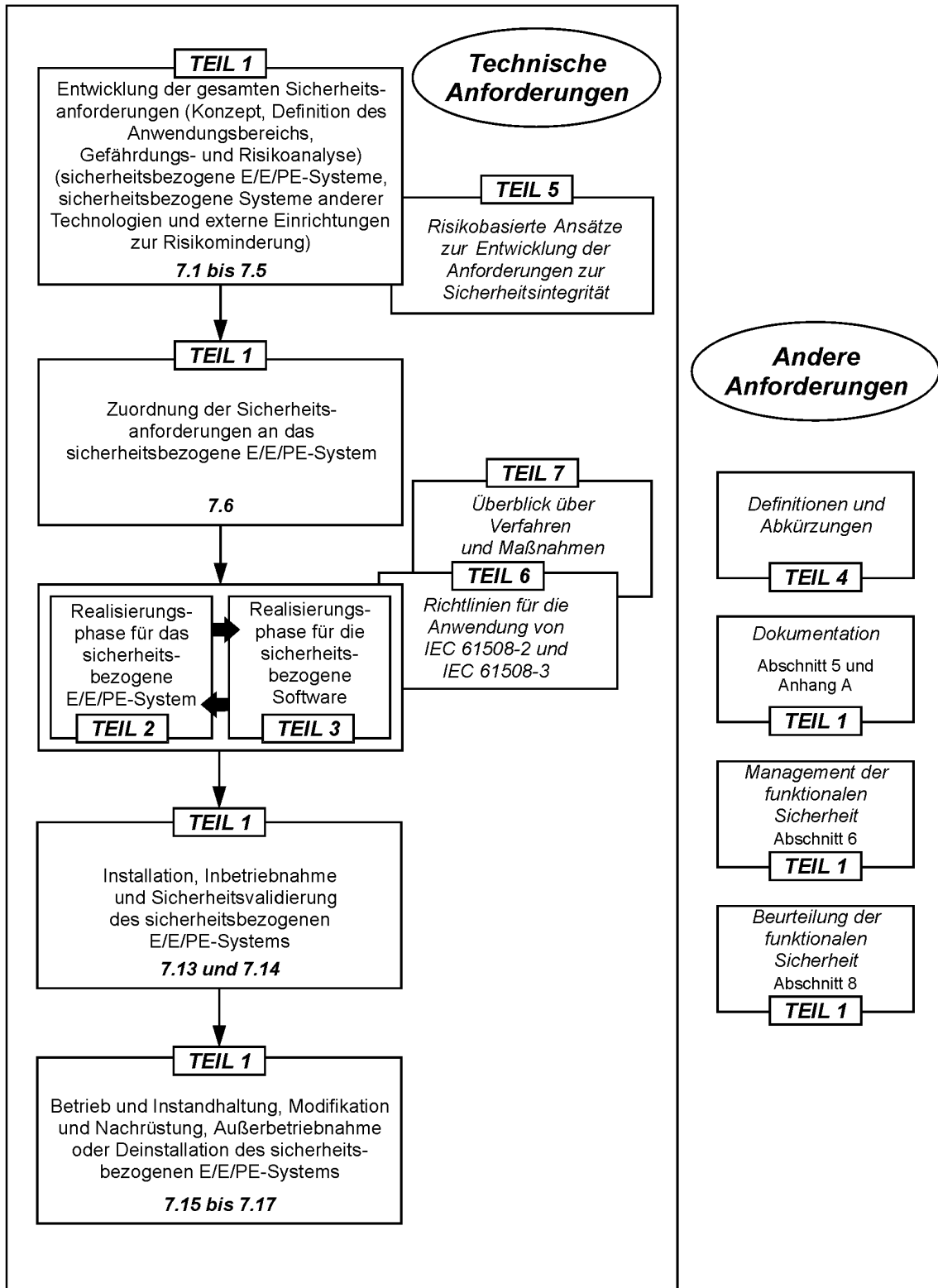


Bild 1 – Gesamtrahmen dieser Norm

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 60050(371):1984, *International Electrotechnical Vocabulary – Chapter 371: Telecontrol*.

IEC 60300-3-2:1993, *Dependability management – Part 3: Application guide – Section 2: Collection of dependability data from the field*.

IEC 61000-1-1:1992, *Electromagnetic compatibility (EMC) – Part 1: General – Section 1: Application and interpretation of fundamental definitions and terms*.

IEC 61000-2-5:1995, *Electromagnetic compatibility (EMC) – Part 2: Environment – Section 5: Classification of electromagnetic environments – Basic EMC publication*.

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

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 61508-6:200, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of parts 2 and 3¹⁾*.

IEC 61508-7:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*.

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

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

IEEE 352:1987, *IEEE guide for general principles of reliability analysis of nuclear power generating station safety systems*.

3 Begriffe und Abkürzungen

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

4 Übereinstimmung mit dieser Norm

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

¹⁾ zu veröffentlichen

5 Dokumentation

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

6 Management der funktionalen Sicherheit

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

7 Anforderungen zum E/E/PES-Sicherheitslebenszyklus

7.1 Allgemeines

7.1.1 Ziele und Anforderungen: Allgemeines

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

ANMERKUNG Die Ziele und Anforderungen für den gesamten Sicherheitslebenszyklus werden zusammen mit einer allgemeinen Einführung zur Struktur der Norm in der IEC 61508-1 gegeben.

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

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

7.1.2 Ziele

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

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

7.1.3 Anforderungen

7.1.3.1 Der E/E/PES-Sicherheitslebenszyklus, der für die Übereinstimmung mit dieser Norm verwendet werden muss, ist der in [Bild 2](#) festgelegte. Falls ein anderer E/E/PES-Sicherheitslebenszyklus verwendet wird, muss dieser während der Planung der funktionalen Sicherheit (siehe [Abschnitt 6 der IEC 61508-1](#)) festgelegt werden und alle Ziele und Anforderungen jedes Unterabschnitts der IEC 61508-2 müssen erfüllt werden.

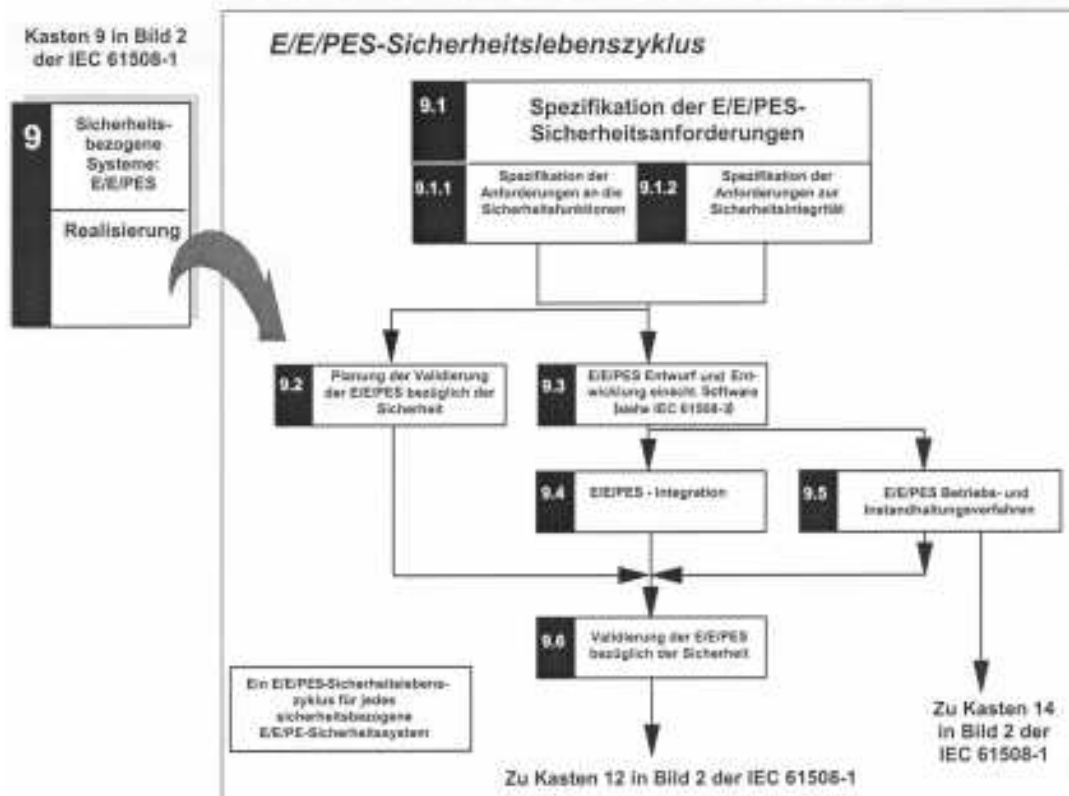
ANMERKUNG [Bild 3](#) zeigt den Anwendungsbereich und die Beziehung zwischen der IEC 61508-2 und der [IEC 61508-3](#).

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

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

7.1.3.4 Außer wenn es nicht während der Planung der funktionalen Sicherheit begründet wird, müssen die Ergebnisse jeder Phase des E/E/PES-Sicherheitslebenszyklus dokumentiert werden (siehe [Abschnitt 5 der IEC 61508-1](#)).

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



ANMERKUNG Siehe auch [IEC 61508-6, A.2\(b\)](#).

Bild 2 – E/E/PES-Sicherheitslebenszyklus (in der Realisierungsphase)

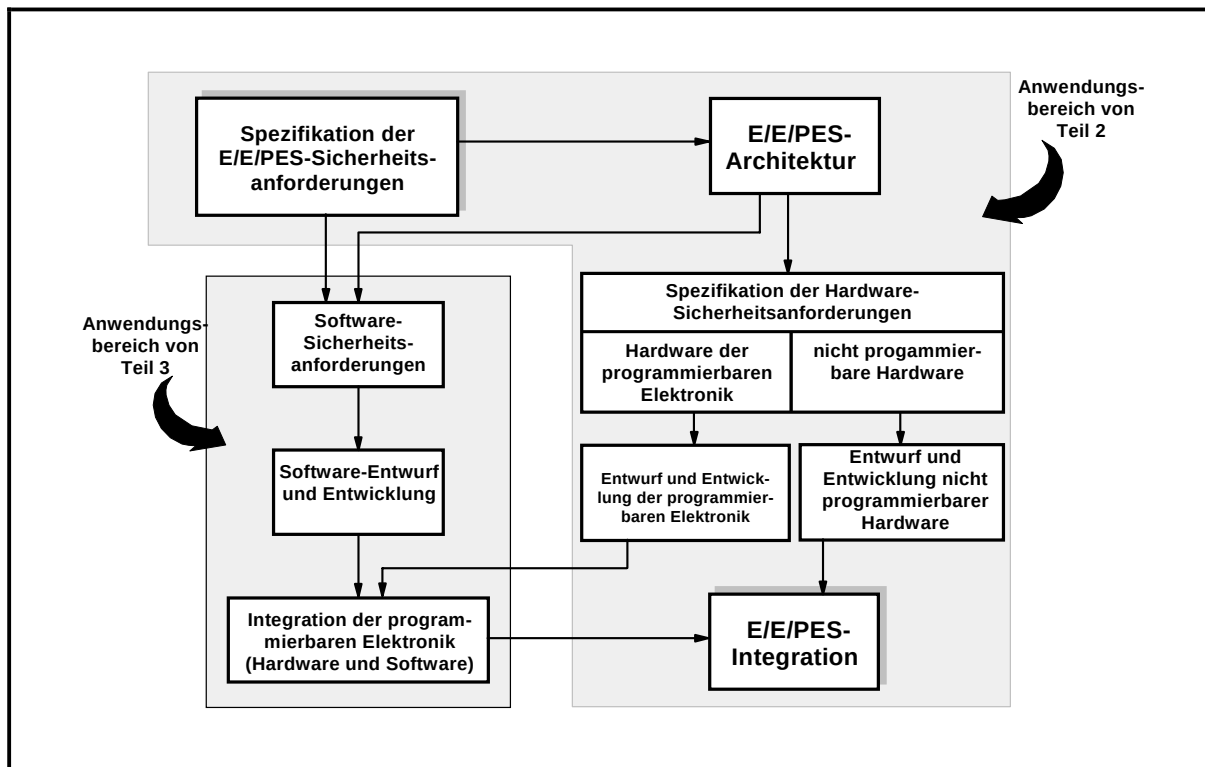


Bild 3 – Beziehung zwischen der IEC 61508-2 und IEC 61508-3 und ihrer Anwendungsbereiche

Tabelle 1 – Überblick – Realisierungsphase des E/E/PES-Sicherheitslebenszyklus

Phase des Sicherheitslebenszyklus		Ziele	Anwendungsbereich	Unterabschnitt für Anforderungen	Eingaben	Ergebnisse (Ausgaben)
Kastennummer in Bild 2	Titel					
9.1	Spezifikation der E/E/PES-Sicherheitsanforderungen	Die Anforderungen für jedes sicherheitsbezogene E/E/PE-System in Form von erforderlichen Sicherheitsfunktionen und der erforderlichen Sicherheitsintegrität festlegen, um die erforderliche funktionale Sicherheit zu erreichen.	Sicherheitsbezogene E/E/PE-Systeme	7.2.2	Beschreibung der Zuordnung der Sicherheitsanforderungen (siehe 7.6 der IEC 61508-1)	E/E/PES-Sicherheitsanforderungen Anforderungen zur Softwaresicherheit als Eingabe für die Spezifikation der Softwaresicherheitsanforderungen
9.2	Planung der Validierung der sicherheitsbezogenen E/E/PE-Systeme bezüglich der Sicherheit	Die Validierung der sicherheitsbezogenen E/E/PE-Systeme bezüglich der Sicherheit planen.	Sicherheitsbezogene E/E/PE-Systeme	7.3.2	E/E/PES-Sicherheitsanforderungen	Plan für die Validierung der sicherheitsbezogenen E/E/PE-Systeme bezüglich der Sicherheit
9.3	E/E/PES-Entwurf und Entwicklung	Entwerfen der sicherheitsbezogenen E/E/PE-Systeme, um die Anforderungen zu den Sicherheitsfunktionen und zur Sicherheitsintegrität zu erfüllen.	Sicherheitsbezogene E/E/PE-Systeme	7.4.2 bis 7.4.9	E/E/PES-Sicherheitsanforderungen	Entwurf der sicherheitsbezogenen E/E/PE-Systeme in Übereinstimmung mit den E/E/PES-Sicherheitsanforderungen Plan für den E/E/PES-Integrationstest Informationen zur PES-Architektur als Eingabe für die Spezifikation der Softwareanforderungen
9.4	E/E/PES-Integration	Integration und Test der sicherheitsbezogenen E/E/PE-Systeme.	Sicherheitsbezogene E/E/PE-Systeme	7.5.2	E/E/PES-Entwurf Plan des E/E/PES-Integrationstests Hardware und Software der programmierbaren Elektronik	Vollständig funktionierende sicherheitsbezogene E/E/PE-Systeme in Übereinstimmung mit dem E/E/PES-Entwurf Ergebnisse der E/E/PES-Integrationstests
9.5	E/E/PES-Installations-, Inbetriebnahme-, Betriebs- und Instandhaltungsverfahren	Verfahren entwickeln um sicherzustellen, dass die funktionale Sicherheit der sicherheitsbezogenen E/E/PE-Systeme während des Betriebs und der Instandhaltung aufrechterhalten wird.	Sicherheitsbezogene E/E/PE-Systeme EUC	7.6.2	E/E/PES-Sicherheitsanforderungen E/E/PES-Entwurf	E/E/PES-Installations-, Inbetriebnahme-, Betriebs- und Instandhaltungsverfahren für jedes einzelne E/E/PES

Tabelle 1 (fortgesetzt)

Phase des Sicherheitslebenszyklus		Ziele	Anwendungsbereich	Unterabschnitt für Anforderungen	Eingaben	Ergebnisse (Ausgaben)
Kastennummer in Bild 2	Titel					
9.6	Validierung der E/E/PES bezüglich der Sicherheit	Validieren, dass die sicherheitsbezogenen E/E/PE-Systeme in jeder Hinsicht den Anforderungen zur Sicherheit im Sinne der erforderlichen Sicherheitsfunktionen und der Sicherheitsintegrität entsprechen.	Sicherheitsbezogene E/E/PE-Systeme	7.7.2	E/E/PES-Sicherheitsanforderungen Plan für die Validierung der sicherheitsbezogenen E/E/PE-Systeme bezüglich der Sicherheit	Vollständig validierte sicherheitsbezogene E/E/PE-Systeme Ergebnisse der Validierung der E/E/PES bezüglich der Sicherheit
–	E/E/PES-Modifikation	Korrekturen, Verbesserungen oder Anpassungen an den sicherheitsbezogenen E/E/PE-Systemen machen und sicherstellen, dass der erforderliche Sicherheits-Integritätslevel erreicht wird und erhalten bleibt.	Sicherheitsbezogene E/E/PE-Systeme	7.8.2	E/E/PES-Sicherheitsanforderungen	Ergebnisse der E/E/PES-Modifikation
–	E/E/PES-Verifikation	Die Ergebnisse einer gegebenen Phase testen und bewerten, um Korrektheit und Konsistenz hinsichtlich der Produkte und Normen sicherzustellen, die die Eingabe zu dieser Phase bilden.	Sicherheitsbezogene E/E/PE-Systeme	7.9.2	Wie oben – hängt von der Phase ab Plan für die Verifikation der sicherheitsbezogenen E/E/PE-Systeme für jede Phase	Wie oben – hängt von der Phase ab Ergebnisse der Verifikation der sicherheitsbezogenen E/E/PE-Systeme für jede Phase
–	Beurteilung der funktionalen Sicherheit des E/E/PES	Untersuchen und beurteilen, ob die funktionale Sicherheit durch die sicherheitsbezogenen E/E/PE-Systeme erreicht worden ist.	Sicherheitsbezogene E/E/PE-Systeme	8	Plan für die Beurteilung der funktionalen Sicherheit des E/E/PES	Ergebnisse der Beurteilung der funktionalen Sicherheit des E/E/PES

7.2 Spezifikation der E/E/PES-Sicherheitsanforderungen

ANMERKUNG Diese Phase entspricht Kasten 9.1 von Bild 2.

7.2.1 Ziel

Das Ziel der Anforderungen dieses Unterabschnittes ist es, die Anforderungen für jedes sicherheitsbezogene E/E/PE-System in Form von erforderlichen Sicherheitsfunktionen und der erforderlichen Sicherheitsintegrität festzulegen, um die erforderliche funktionale Sicherheit zu erreichen.

ANMERKUNG Die Sicherheitsfunktionen können zum Beispiel erforderlich sein, um die EUC in einen sicheren Zustand zu versetzen oder einen sicheren Zustand aufrechtzuerhalten.

7.2.2 Allgemeine Anforderungen

7.2.2.1 Die Spezifikation der E/E/PES-Sicherheitsanforderungen muss von der Zuordnung der Sicherheitsanforderungen, die in 7.6 der IEC 61508-1 beschrieben ist, und von den Anforderungen, die während der Planung der funktionalen Sicherheit (siehe Abschnitt 6 der IEC 61508-1) festgelegt werden, abgeleitet werden. Diese Informationen müssen dem Entwickler des E/E/PES zur Verfügung gestellt werden.

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

7.2.2.2 Die E/E/PES-Sicherheitsanforderungen müssen in einer Art und Weise ausgedrückt und strukturiert werden, so dass sie

- a) klar, genau, unzweideutig, nachprüfbar, testbar, pflegbar und ausführbar sind und
- b) geschrieben sind, um denjenigen Unterstützung zu leisten, die wahrscheinlich die Informationen an irgendeiner Stufe des E/E/PES-Sicherheitslebenszyklus verwenden.

7.2.2.3 Die Spezifikation der E/E/PES-Sicherheitsanforderungen muss die Anforderungen an die E/E/PES-Sicherheitsfunktionen (siehe 7.2.3.1) und die Anforderungen an die E/E/PES-Sicherheitsintegrität (siehe 7.2.3.2) enthalten.

7.2.3 E/E/PES-Sicherheitsanforderungen

7.2.3.1 Die Spezifikation der Anforderungen an die E/E/PES-Sicherheitsfunktionen muss enthalten:

- a) eine Beschreibung aller Sicherheitsfunktionen, die notwendig sind, um die erforderliche funktionale Sicherheit zu erreichen. Diese Beschreibung muss für jede Sicherheitsfunktion:
 - ausführliche detaillierte Anforderungen liefern, die ausreichend für den Entwurf und die Entwicklung der sicherheitsbezogenen E/E/PE-Systeme sind,
 - die beabsichtigte Art und Weise enthalten, wie die sicherheitsbezogenen E/E/PE-Systeme einen sicheren Zustand der EUC erreichen oder aufrechterhalten,
 - festlegen, ob und für welche Dauer eine kontinuierliche Steuerung oder Regelung zum Erreichen oder Aufrechterhalten eines sicheren Zustands der EUC erforderlich ist und
 - festlegen, ob die Sicherheitsfunktion für sicherheitsbezogene E/E/PE-Systeme anwendbar ist, die in der Betriebsart mit niedriger Anforderungsrate oder der Betriebsart mit hoher Anforderungsrate bzw. kontinuierlicher Anforderung betrieben werden;
- b) die Leistungsfähigkeit in Bezug auf Durchsatz und Ansprechzeit;
- c) die Schnittstellen des sicherheitsbezogenen E/E/PE-Systems und die Bedienerchnittstellen, die notwendig sind, um die erforderliche funktionale Sicherheit zu erreichen;
- d) alle für die funktionale Sicherheit relevanten Informationen, die einen Einfluss auf den Entwurf des sicherheitsbezogenen E/E/PE-Systems haben können;
- e) alle Schnittstellen zwischen den sicherheitsbezogenen E/E/PE-Systemen und allen anderen Systemen (entweder direkt innerhalb oder außerhalb der EUC angeschlossen);
- f) alle relevanten Betriebsarten der EUC, einschließlich:
 - Vorbereitung zur Verwendung, einschließlich Einstellungen und Justage,
 - Einschaltphase, Lernphase, Automatikbetrieb, manueller Betrieb, halbautomatischer Betrieb, stabile Betriebsphase,
 - stabiler Zustand ohne Betrieb, Rücksetzen, Herunterfahren, Instandhaltung,
 - vernünftigerweise vorhersehbare unnormale Bedingungen;

ANMERKUNG 1 Vernünftigerweise vorhersehbare unnormale Bedingungen sind die Bedingungen, die entweder für die Entwickler oder die Anwender vernünftigerweise vorhersehbar sind.

ANMERKUNG 2 Für besondere Betriebsarten (zum Beispiel Einstellung, Justage oder Instandhaltung) können zusätzliche Sicherheitsfunktionen erforderlich sein, um diese Tätigkeiten sicher ausführen zu können.

- g) alle erforderlichen Arten des Verhaltens der sicherheitsbezogenen E/E/PE-Systeme – insbesondere das Ausfallverhalten und die erforderliche Reaktion (zum Beispiel Alarm, automatisches Herunterfahren usw.) der sicherheitsbezogenen E/E/PE-Systeme müssen genau beschrieben werden;
- h) die Bedeutung aller Hardware-/Softwarewechselwirkungen – wo zutreffend, müssen alle erforderlichen Einschränkungen zwischen Hardware und Software identifiziert und dokumentiert werden;

ANMERKUNG 3 Wo diese Wechselwirkungen vor Beendigung des Entwurfs nicht bekannt sind, können nur allgemeine Einschränkungen angegeben werden.

- i) Grenzbedingungen und Einschränkungen für die sicherheitsbezogenen E/E/PE-Systeme und ihre zugehörigen Teilsysteme, zum Beispiel zeitliche Einschränkungen;
- j) jede spezielle Anforderung mit Bezug zu den Verfahren für das Einschalten und den Wiederstart der sicherheitsbezogenen E/E/PE-Systeme.

7.2.3.2 Die Spezifikation der Anforderungen zur E/E/PES-Sicherheitsintegrität muss enthalten:

- a) den Sicherheits-Integritätslevel für jede Sicherheitsfunktion und, wenn erforderlich (siehe Anmerkung 2), den erforderlichen Ausfallgrenzwert für die Sicherheitsfunktion;

ANMERKUNG 1 Der Sicherheits-Integritätslevel einer Sicherheitsfunktion bestimmt den Ausfallgrenzwert für die Sicherheitsfunktion nach IEC 61508-1, Tabellen 2 und 3.

ANMERKUNG 2 Der Ausfallgrenzwert einer Sicherheitsfunktion muss festgelegt werden, wenn die erforderliche Risikominderung für eine Sicherheitsfunktion unter Verwendung einer quantitativen Methode bestimmt worden ist (siehe IEC 61508-1, 7.5.2.2).

- b) die Betriebsart für jede Sicherheitsfunktion (niedrige Anforderungsrate oder hohe Anforderungsrate bzw. kontinuierliche Anforderung);
- c) Anforderungen, Einschränkungen, Funktionen und Einrichtungen, um die Durchführung der Wiederholungsprüfung der sicherheitsbezogenen E/E/PES-Hardware zu ermöglichen;
- d) die Extremwerte aller Umgebungsbedingungen, die während des E/E/PES-Sicherheitslebenszyklus einschließlich Herstellung, Lagerung, Transport, Prüfung, Installation, Inbetriebnahme, Betrieb und Instandhaltung wahrscheinlich auftreten werden;
- e) die elektromagnetischen Störfestigkeitsgrenzwerte (siehe IEC 61000-1-1), die erforderlich sind, um elektromagnetische Verträglichkeit zu erreichen – die elektromagnetischen Störfestigkeitsgrenzwerte sollten sowohl unter Berücksichtigung der elektromagnetischen Umgebung (siehe IEC 61000-2-5) als auch des erforderlichen Sicherheits-Integritätslevels abgeleitet werden.

ANMERKUNG 3 Es ist wichtig zu berücksichtigen, dass der Sicherheits-Integritätslevel ein Faktor in der Bestimmung der elektromagnetischen Störfestigkeitsgrenzwerte ist, dies gilt besonders, weil der elektromagnetische Störpegel in einer Umgebung einer statistischen Verteilung unterworfen ist. In den meisten Praxissituationen ist es nicht möglich, einen absoluten Störpegel zu bestimmen, es kann nur ein Pegel festgelegt werden, von dem erwartet wird, dass er in der Praxis nicht überschritten wird (dies ist der elektromagnetische Verträglichkeitspegel). Unglücklicherweise machen es praktische Schwierigkeiten sehr schwierig, die Wahrscheinlichkeit, die mit dieser Erwartung verbunden ist, zu definieren. Daher garantiert der Störfestigkeitsgrenzwert nicht, dass das sicherheitsbezogene E/E/PE-System nicht auf Grund elektromagnetischer Störungen ausfällt, er liefert nur einen Grad an Vertrauen, dass ein solcher Ausfall nicht auftritt. Der tatsächlich erreichte Grad an Vertrauen ist eine Funktion des Störfestigkeitsgrenzwertes in Bezug zur statistischen Verteilung der Störpegel in der Betriebsumgebung. Für höhere Sicherheits-Integritätslevels kann es notwendig sein, einen höheren Grad an Vertrauen zu haben, was bedeutet, dass die Spanne, um die der Störfestigkeitsgrenzwert den Verträglichkeitspegel überschreitet, für höhere Sicherheits-Integritätslevels größer sein sollte.

ANMERKUNG 4 Weitere Hilfestellung kann in EMV-Produktnormen gefunden werden, es ist jedoch wichtig zu berücksichtigen, dass höhere als in solchen Normen festgelegte Störfestigkeitspegel für besondere Einsatzorte, oder wenn die Betriebsmittel für die Verwendung in rauer elektromagnetischer Umgebung vorgesehen sind, notwendig sein können.

ANMERKUNG 5 Während der Entwicklung der Spezifikation der E/E/PES-Sicherheitsanforderungen sollte die Anwendung, in der die sicherheitsbezogenen E/E/PE-Systeme zu verwenden sind, berücksichtigt werden. Dies ist insbesondere für die Instandhaltung wichtig, wobei das festgelegte Intervall für die Wiederholungsprüfung nicht kleiner sein sollte, als vernünftigerweise für die jeweilige Anwendung erwartet werden kann. Zum Beispiel ist die Zeit zwischen Wartungen, die realistischerweise für allgemein verwendete Massenprodukte erreicht werden kann, wahrscheinlich größer als die für Produkte in einer besser überwachten Anwendung.

7.2.3.3 Zur Vermeidung von Irrtümern während der Spezifikation der E/E/PES-Sicherheitsanforderungen muss eine angemessene Gruppe von Verfahren und Maßnahmen nach Tabelle B.1 verwendet werden.

7.3 Planung der Validierung der sicherheitsbezogenen E/E/PE-Systeme bezüglich der Sicherheit

ANMERKUNG Diese Phase entspricht Kasten 9.2 in [Bild 2](#). Sie wird üblicherweise parallel zu E/E/PES-Entwurf und Entwicklung (siehe 7.4) ausgeführt.

7.3.1 Ziel

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

7.3.2 Anforderungen

7.3.2.1 Es muss eine Planung durchgeführt werden, um die Schritte (sowohl verfahrensmäßige als auch technische) festzulegen, die für den Nachweis ausgeführt werden müssen, dass die sicherheitsbezogenen E/E/PE-Systeme die Spezifikation der E/E/PES-Sicherheitsanforderungen (siehe [7.2](#)) erfüllen.

ANMERKUNG Siehe [IEC 61508-3](#) zum Validierungsplan für die Software.

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

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

ANMERKUNG Hilfestellung bei der Festlegung der Störfestigkeitstestgrenze ist in IEC 61000-2-5 und IEC 61000-4 enthalten.

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

7.4 E/E/PES-Entwurf und Entwicklung

ANMERKUNG Diese Phase entspricht Kasten 9.3 in [Bild 2](#). Sie wird üblicherweise parallel zur Planung der Validierung des sicherheitsbezogenen E/E/PE-Systems bezüglich der Sicherheit (siehe 7.3) ausgeführt.

7.4.1 Ziel

Das Ziel der Anforderungen dieses Unterabschnittes ist es, sicherzustellen, dass der Entwurf und die Implementierung der sicherheitsbezogenen E/E/PE-Systeme die festgelegten Anforderungen an die Sicherheitsfunktionen und die Sicherheitsintegrität (siehe [7.2](#)) erfüllt.

7.4.2 Allgemeine Anforderungen

7.4.2.1 Der Entwurf der E/E/PES-Systeme muss in Übereinstimmung mit der Spezifikation der E/E/PES-Sicherheitsanforderungen (siehe [7.2](#)) unter Berücksichtigung aller Anforderungen aus 7.4 erstellt werden.

7.4.2.2 Der Entwurf des sicherheitsbezogenen E/E/PE-Systems (einschließlich der gesamten Hardware- und Softwarearchitektur, Sensoren, Aktoren, programmierbarer Elektronik, Embedded Software,

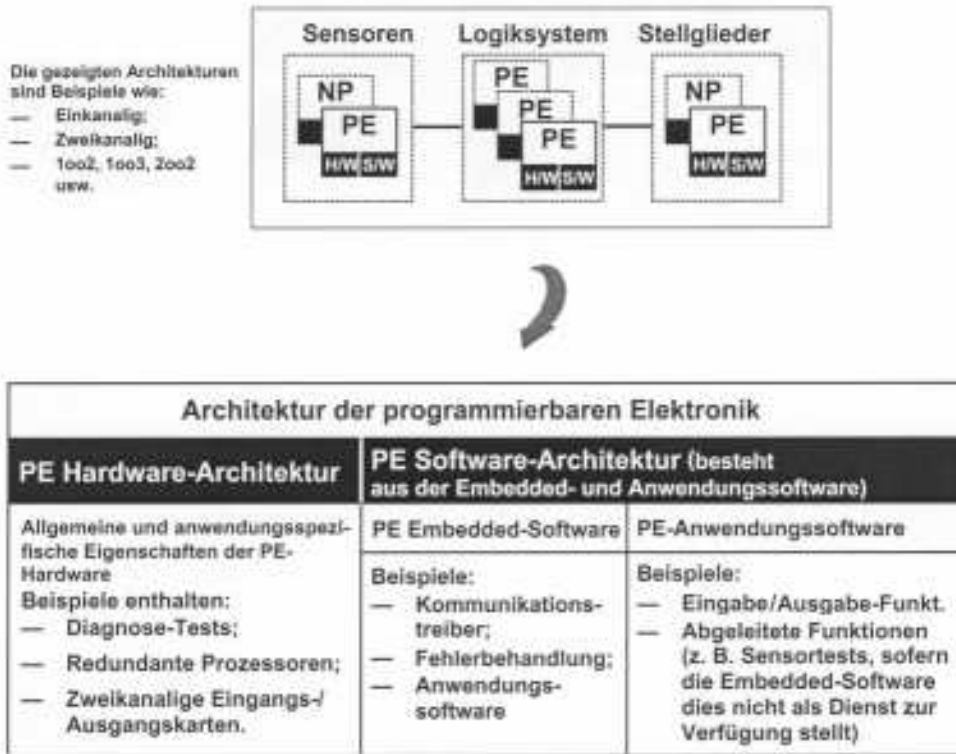
Anwendungssoftware usw.), siehe Bild 4, muss so ausgeführt werden, dass alle Anforderungen a) bis c) wie folgt erfüllt werden:

- a) die Anforderungen zur Sicherheitsintegrität der Hardware, bestehend aus
 - den Einschränkungen der Sicherheitsintegrität der Hardware aufgrund der Architektur (siehe 7.4.3.1) und
 - den Anforderungen an die Wahrscheinlichkeit gefahrbringender zufälliger Hardwareausfälle (siehe 7.4.3.2);
- b) die Anforderungen zur systematischen Sicherheitsintegrität, bestehend aus
 - den Anforderungen zur Vermeidung von Ausfällen (siehe 7.4.4) und den Anforderungen zur Beherrschung von systematischen Ausfällen (siehe 7.4.5), oder
 - dem Nachweis, dass die Betriebsmittel „betriebsbewährt“ sind (siehe 7.4.7.6 bis 7.4.7.12);
- c) die Anforderungen an das Systemverhalten bei Erkennung eines Fehlers (siehe 7.4.6).

ANMERKUNG 1 Gesamtrahmen der E/E/PES-Sicherheitsintegrität: Die umfassende Methode zur Auswahl eines Entwurfsansatzes, um das Erreichen eines Sicherheits-Integritätslevels (sowohl der Sicherheitsintegrität der Hardware als auch der systematischen Sicherheitsintegrität) in sicherheitsbezogenen E/E/PE-Systemen darzulegen, ist wie folgt:

- Bestimmung des erforderlichen Sicherheits-Integritätslevels (SIL) der Sicherheitsfunktionen (siehe IEC 61508-1 und IEC 61508-5);
- setze: Sicherheitsintegrität der Hardware = systematische Sicherheitsintegrität = SIL (siehe 7.4.3.2.1);
- zur Sicherheitsintegrität der Hardware: Bestimmung der Architektur, um die Einschränkungen aufgrund der Architektur zu erfüllen (siehe 7.4.3.1) und aufzeigen, dass die Wahrscheinlichkeiten des Ausfalls der Sicherheitsfunktionen infolge zufälliger Hardwareausfälle die erforderlichen Ausfallgrenzwerte erfüllen (siehe 7.4.3.2);
- zur systematischen Sicherheitsintegrität: Auswahl von Entwurfsmerkmalen, die systematische Fehler im tatsächlichen Betrieb beherrschen (tolerieren) (siehe 7.4.5), oder Bestätigung, dass die Anforderungen zur „Betriebsbewährung“ erfüllt worden sind (siehe 7.4.7.6 bis 7.4.7.12); und
- zur systematischen Sicherheitsintegrität: Auswahl von Verfahren und Maßnahmen, die systematische Fehler während des Entwurfs und der Entwicklung vermeiden (siehe 7.4.4), oder Bestätigung, dass die Anforderungen zur „Betriebsbewährung“ erfüllt worden sind (siehe 7.4.7.6 bis 7.4.7.12).

ANMERKUNG 2 IEC 61508-3 enthält die Anforderungen zur Softwarearchitektur (siehe 7.4.2.2), die Anforderungen zur Erstellung einer Spezifikation der Integrationstests für programmierbare Elektronik und Software (siehe 7.5) und die Anforderungen zur Integration der programmierbaren Elektronik und der Software gemäß dieser Spezifikation (siehe 7.5). In allen Fällen ist eine enge Zusammenarbeit zwischen dem Entwickler der sicherheitsbezogenen E/E/PE-Systeme und dem Softwareentwickler notwendig.



Legende

PE programmierbare Elektronik

NP nicht-programmierbare Geräte

H/W Hardware

S/W Software

MoON M aus N Kanälen [en: M out of N] (zum Beispiel ist 1oo2 eine Architektur mit 1 aus 2 Kanälen)

Bild 4 – Beziehung zwischen den Hardware- und Software-Architekturen von programmierbarer Elektronik

7.4.2.3 Wo ein sicherheitsbezogenes E/E/PE-System sowohl Sicherheitsfunktionen als auch Nicht-Sicherheitsfunktionen enthalten muss, muss die gesamte Hardware und Software als sicherheitsbezogen behandelt werden, es sei denn, es kann gezeigt werden, dass die Implementierung der Sicherheitsfunktionen und Nicht-Sicherheitsfunktionen ausreichend unabhängig voneinander ist (d. h., dass der Ausfall irgendeiner Nicht-Sicherheitsfunktion keinen gefährlichen Ausfall einer Sicherheitsfunktion verursachen kann). Wo immer möglich, sollten die Sicherheitsfunktionen von den Nicht-Sicherheitsfunktionen getrennt werden.

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

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

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

ANMERKUNG 1 Eine ausreichende Unabhängigkeit der Implementierung liegt vor, wenn gezeigt wird, dass die Wahrscheinlichkeit eines abhängigen Ausfalls zwischen den Teilen, die Sicherheitsfunktionen unterschiedlicher