

	DIN EN 61508-2 (VDE 0803-2)	
	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.	
ICS 35.240.50	Entwurf	Einsprüche bis 2009-08-31 Vorgesehen als Ersatz für DIN EN 61508-2 (VDE 0803-2):2002-12 Ersatz für E DIN IEC 61508-2 (VDE 0803-2):2006-07
Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (IEC 65A/523/CDV:2008); Deutsche Fassung FprEN 61508-2:2008		
Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems (IEC 65A/523/CDV:2008); German version FprEN 61508-2:2008		
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 65A/523/CDV:2008); Version allemande FprEN 61508-2:2008		
Anwendungswarnvermerk		
Dieser Norm-Entwurf mit Erscheinungsdatum 2009-06-08 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.		
Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.		
Stellungnahmen werden erbeten		
– vorzugsweise als Datei per E-Mail an dke@vde.com in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.dke.de/stellungnahme abgerufen werden – oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.		
Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevante Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.		
Gesamtumfang 183 Seiten		
DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

Beginn der Gültigkeit

Diese Norm gilt ab ...

Nationales Vorwort

Die Deutsche Fassung des europäischen Dokuments FprEN 61508-2:2008 „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme“ (Entwurf in der Umfrage) ist unverändert in diesen Norm-Entwurf übernommen worden.

Die Internationale Elektrotechnische Kommission (IEC) und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dem entsprechend ist das internationale Dokument IEC 65A/523/CDV:2008 „Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems“ unverändert in den Entwurf FprEN 61508-2:2008 übernommen worden.

Da die Deutsche Fassung noch nicht endgültig mit der Englischen und Französischen Fassung abgeglichen ist, ist die englische Originalfassung des IEC-CDV entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom SC 65A „System aspects“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet.

Bei der Abstimmung zu dem Europäischen Schluss-Entwurf bei CENELEC und dem Internationalen Schluss-Entwurf bei IEC [Final Draft International Standard (FDIS)] sind jeweils nur „JA/NEIN“-Entscheidungen möglich, wobei „NEIN“-Entscheidungen fundiert begründet werden müssen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Für diesen Norm-Entwurf ist das nationale Arbeitsgremium GK 914 „Funktionale Sicherheit elektrischer, elektronischer und programmierbarer elektronischer Systeme (E, E, PES) zum Schutz von Personen und Umwelt“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (www.dke.de) zuständig.

Änderungen

Gegenüber DIN EN 61508-2 (VDE 0803-2):2002-12 wurden folgende Änderungen vorgenommen:

- a) Um die Anwendbarkeit auf einzelne Geräte und Komponenten zu ermöglichen bzw. zu erleichtern, wurde:
 - die ehemalige „Spezifikation der E/E/PES-Sicherheitsanforderungen“ in den Teil 1, Unterabschnitt 7.10 verschoben und wird dort als „Spezifikation der Sicherheitsanforderungen des E/E/PE-Systems“ bezeichnet. In der ersten Phase der Realisierung des Sicherheitslebenszyklus des E/E/PE-Systems entsteht daher nun gemäß 7.2 eine „Spezifikation der Entwurfsanforderungen des E/E/PE-Systems“;
 - der Begriff „Element“ zur hierarchischen Gliederung eines E/E/PE-Systems unterhalb der Ebene von Teilsystemen eingeführt. Diese Einführung ist jedoch nicht widerspruchsfrei und konsistent innerhalb des Teils 2 erfolgt. Der neue Anhang D beschreibt in einem „Sicherheitshandbuch des Elements“ die für die Integration eines Elements in ein sicherheitsbezogenes System erforderlichen Informationen;
- b) Bestimmung der systematischen Eignung bei Synthese von Elementen nach Abschnitt 7.4.3;
- c) Einführung von Konformitätspfaden in 7.4.2.2, um die Übereinstimmung mit den Anforderungen zur systematischen Sicherheitsintegrität nachzuweisen;

- d) Einführung von Konformitätspfaden in 7.4.4, um die Übereinstimmung mit den Anforderungen der Sicherheitsintegrität der Hardware nachzuweisen;
- e) Behandlung der Entwicklung von ASICs (d. h. auch FPGA, PLD, CPLD) für den Einsatz in einem sicherheitsbezogenen System in Analogie zur Entwicklung sicherheitsbezogener Software mit Einführung eines V-Modells für den ASIC-Entwicklungslebenszyklus (siehe Bild 3). Zur Vermeidung von Ausfällen im Rahmen von Entwurf und Entwicklung digitaler ASICs erforderliche Maßnahmen sind im informativen Anhang F aufgeführt. Die Tabellen F.1 und F.2 bilden eine nach Sicherheits-Integritätslevel abgestufte Auflistung von erforderlichen Verfahren und Maßnahmen;
- f) Einführung von Regeln, die die Integration von zwei oder mehr Kanälen sowie Überwachungseinrichtungen auf dem Substrat eines digitalen ASICs erlauben, siehe Anhang E.

Nationaler Anhang NA (informativ)

Zusammenhang mit Europäischen und Internationalen Normen

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

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

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

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
—	IEC 60050(371):1984	a)	—
EN 60300-3-2:2005	IEC 60300-3-2:2004	DIN EN 60300-3-2:2005-09	—
—	IEC/TS 61000-1-2:2008	—	—
FprEN61508-1:2008	65A/522/CDV:2008	E DIN EN 61805-1 (VDE 0803-1) in Vorbereitung	(VDE 0803-1)
FprEN61508-3:2008	65A/524/CDV:2008	E DIN EN 61805-3 (VDE 0803-3) in Vorbereitung	(VDE 0803-3)
FprEN61508-4:2008	65A/525/CDV:2008	E DIN EN 61805-4 (VDE 0803-4) in Vorbereitung	(VDE 0803-4)
—	IEC 62280-1:2002	—	—
—	IEC 62280-2:2002	—	—
—	ISO/IEC Guide 51: 1999	—	—
—	IEC Guide 104:1997	—	—
a) "Internationales Elektrotechnisches Wörterbuch - Deutsche Ausgabe", im Rahmen der Datenbankanwendung DIN-TERM zu beziehen über Beuth Verlag.			

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN 60300-3-2, *Zuverlässigkeitsmanagement – Teil 3-2: Anwendungsleitfaden – Erfassung von Zuverlässigkeitsdaten im Betrieb*

E DIN EN 61805-1 (VDE 0803-1), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen*

E DIN EN 61805-3 (VDE 0803-3), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software*

E DIN EN 61805-4 (VDE 0803-4), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen*

Deutsche Fassung

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme –
Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme

Inhalt

	Seite
Einleitung	4
1 Anwendungsbereich	6
2 Normative Verweisungen	9
3 Begriffe und Abkürzungen	9
4 Übereinstimmung mit dieser Norm	9
5 Dokumentation	9
6 Management der funktionalen Sicherheit	10
7 Anforderungen des Sicherheitslebenszyklus des E/E/PE-Systems	10
7.1 Allgemeines	10
7.2 Entwurfsanforderungen des E/E/PE-Systems	14
7.3 Planung der Validierung der Sicherheit des E/E/PE-Systems	17
7.4 Entwurf und Entwicklung des E/E/PE-Systems	17
7.5 Integration des E/E/PE-Systems	39
7.6 Betriebs- und Instandhaltungsverfahren des E/E/PE-Systems	40
7.7 Validierung der Sicherheit des E/E/PE-Systems	42
7.8 Modifikation des E/E/PE-Systems	43
7.9 Verifikation des E/E/PE-Systems	44
8 Beurteilung der funktionalen Sicherheit	45
Anhang A (normativ) Verfahren und Maßnahmen für sicherheitsbezogene E/E/PE-Systeme: Beherrschung von Ausfällen während des Betriebs	46
A.1 Allgemeines	46
A.2 Sicherheitsintegrität der Hardware	47
A.3 Systematische Sicherheitsintegrität	58
Anhang B (normativ) Verfahren und Maßnahmen für sicherheitsbezogene E/E/PE-Systeme: Vermeidung von systematischen Ausfällen während der verschiedenen Phasen des Lebenszyklus	63
Anhang C (normativ) Diagnosedeckungsgrad und Anteil sicherer Ausfälle	73
C.1 Berechnung von Diagnosedeckungsgrad und dem Anteil sicherer Ausfälle eines Hardwareelements	73
C.2 Bestimmung von Diagnosedeckungsfaktoren	74
Anhang D (normativ) Sicherheitshandbuch für konforme Objekte	76

	Seite
D.1 Allgemeines	76
D.2 Inhalte	76
Anhang E (normativ) Besondere Architekturanforderungen für integrierte Schaltkreise (ICs) mit On-Chip-Redundanz	78
E.1 Allgemeines	78
E.2 Zusätzliche Anforderungen für On-Chip-Redundanz in SIL3	80
E.3 β -Faktor	80
Anhang F (informativ) Verfahren und Maßnahmen für ASICs: Vermeidung von systematischen Ausfällen	83
Literaturhinweise	92
Bilder	
Bild 1 – Gesamtrahmen dieser Norm	8
Bild 2 – Sicherheitslebenszyklus des E/E/PE-Systems (in der Realisierungsphase)	11
Bild 3 – ASIC-Entwicklungslebenszyklus (V-Modell)	12
Bild 4 – Beziehung zwischen IEC 61508-2 und IEC 61508-3 und ihre Anwendungsbereiche	12
Bild 5 (siehe 7.4.4.2.3): Beispiel: Bestimmung des maximalen SIL für eine festgelegte Architektur	25
Bild 6 – Beispiel (siehe 7.4.4.2.4): Bestimmung des maximalen SIL für eine festgelegte Architektur	29
Bild 7 – Architekturen für Datenkommunikation	39
Tabellen	
Tabelle 1 – Überblick – Realisierungsphase des Sicherheitslebenszyklus des E/E/PE-Systems	13
Tabelle 2 – Maximal zulässiger Sicherheits-Integritätslevel für eine Sicherheitsfunktion, die von einem sicherheitsbezogenen Typ A-Element ausgeführt wird	24
Tabelle 3 – Maximal zulässiger Sicherheits-Integritätslevel für eine Sicherheitsfunktion, die von einem sicherheitsbezogenen Typ B-Element ausgeführt wird	24
Tabelle A.1 – Fehler oder Ausfälle, die während des Betriebs erkannt oder zur Bestimmung des Anteils sicherer Ausfälle analysiert werden müssen	47
Tabelle A.2 – Elektrische Elemente	50
Tabelle A.3 – Elektronische Elemente	51
Tabelle A.4 – Verarbeitungseinheiten	52
Tabelle A.5 – Unveränderliche Speicherbereiche	52
Tabelle A.6 – Veränderliche Speicherbereiche	53
Tabelle A.7 – E/A-Einheiten und Schnittstellen (externe Kommunikation)	54
Tabelle A.8 – Datenwege (interne Kommunikation)	54
Tabelle A.9 – Energieversorgung	55
Tabelle A.10 – Programmablauf (Watchdog)	55
Tabelle A.11 – Takt	56
Tabelle A.12 – Kommunikation und Massenspeicher	56
Tabelle A.13 – Sensoren	57
Tabelle A.14 – Stellglieder (Aktoren)	57

	Seite
Tabelle A.15 – Verfahren und Maßnahmen zur Beherrschung von durch den Hardwareentwurf verursachten systematischen Ausfällen	59
Tabelle A.16 – Verfahren und Maßnahmen zur Beherrschung von durch umgebungsbedingte Beanspruchung oder Einflüsse verursachten systematischen Ausfällen.....	59
Tabelle A.17 – Verfahren und Maßnahmen zur Beherrschung von systematischen Ausfällen während des Betriebs.....	61
Tabelle A.18 – Wirksamkeit von Verfahren und Maßnahmen zur Beherrschung von systematischen Ausfällen	61
Tabelle B.1 – Verfahren und Maßnahmen zur Vermeidung von Irrtümern während der Spezifikation von E/E/PE-Entwurfsanforderungen (siehe 7.2)	65
Tabelle B.2 – Verfahren und Maßnahmen zur Vermeidung von Fehlern während Entwurf und Entwicklung des E/E/PE-Systems (siehe 7.4)	66
Tabelle B.3 – Verfahren und Maßnahmen zur Vermeidung von Fehlern während der Integration des E/E/PE-Systems (siehe 7.5)	67
Tabelle B.4 – Verfahren und Maßnahmen von Fehlern und Ausfällen während der Betriebs- und Instandhaltungsverfahren des E/E/PE-Systems (siehe 7.6)	68
Tabelle B.5 – Verfahren und Maßnahmen zur Vermeidung von Fehlern während der Validierung der Sicherheit des E/E/PE-Systems (siehe 7.7).....	68
Tabelle B.6 – Wirksamkeit von Verfahren und Maßnahmen zur Vermeidung von systematischen Ausfällen	70

Einleitung

Systeme, die aus elektrischen und/oder elektronischen Elementen bestehen, werden seit vielen Jahren verwendet, um Sicherheitsfunktionen in vielen Anwendungsbereichen auszuführen. Auf Rechnern basierende Systeme (allgemein ausgedrückt programmierbare elektronische Systeme) werden in allen Anwendungsbereichen benutzt, um Nicht-Sicherheitsfunktionen und zunehmend auch um Sicherheitsfunktionen auszuführen. Falls Rechnersystemtechnologie wirksam und sicherheitsgerichtet eingesetzt wird, ist es wichtig, dass die für die Entscheidungsfindung Verantwortlichen ausreichende Hilfestellung bezüglich der Sicherheitsaspekte erhalten, nach denen diese Entscheidungen getroffen werden.

Diese Internationale Norm beschreibt einen allgemeinen Lösungsweg für alle Tätigkeiten während des Sicherheitslebenszyklus für Systeme, die aus elektrischen und/oder elektronischen und/oder programmierbaren elektronischen (E/E/PE) Elementen bestehen und die eingesetzt werden, um Sicherheitsfunktionen auszuführen. Dieser allgemeine Lösungsweg wurde gewählt, um ein sinnvolles und konsistentes technisches Verfahren für alle elektrischen Sicherheitssysteme zu entwickeln. Ein Hauptziel ist es, die Entwicklung von anwendungsspezifischen Normen zu erleichtern.

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

Es ist berücksichtigt worden, dass eine große Vielfalt von Anwendungen in vielfältigen Anwendungsbereichen vorliegt, die sicherheitsbezogene E/E/PE-Systeme verwenden und diese einen weiten Bereich in Bezug auf Komplexität, Gefährdungs- und Risikopotentiale 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 und in Revisionen der bereits bestehenden Normen ermöglicht.

Diese Internationale Norm:

- betrachtet alle relevanten Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus (zum Beispiel vom anfänglichen Konzept über Entwurf, Implementierung, Betrieb und Instandhaltung bis zur Außerbetriebnahme), wenn E/E/PE-Systeme benutzt werden, um Sicherheitsfunktionen auszuführen;
- wurde unter Berücksichtigung einer sich schnell entwickelnden Technologie entworfen. Der Betrachtungsrahmen ist ausreichend robust und ausführlich genug, um auch für zukünftige Entwicklungen verwendbar zu sein;
- ermöglicht die Erstellung anwendungsspezifischer internationaler Normen, die sich mit sicherheitsbezogenen E/E/PE-Systemen befassen. Die Entwicklung anwendungsspezifischer internationaler Normen sollte innerhalb des Rahmens dieser Norm zu einem hohen Grad an Übereinstimmung (zum Beispiel von zugrunde liegenden Prinzipien, Terminologie usw.) führen, sowohl innerhalb der Anwendungsbereiche, als auch über die Anwendungsbereiche hinweg. Dies hat sowohl sicherheitstechnische als auch wirtschaftliche Vorteile;

ANMERKUNG 1 Hinweise [1] und [2] in den Literaturhinweisen sind anwendungsspezifische internationale Normen.

- liefert eine Methode für die Entwicklung der Spezifikation der Sicherheitsanforderungen, die notwendig ist, um die erforderliche funktionale Sicherheit für sicherheitsbezogene E/E/PE-Systeme zu erreichen;
- verwendet einen auf dem Risiko basierenden Lösungsansatz, durch den die Anforderungen zur Sicherheitsintegrität bestimmt werden können;

- führt Sicherheits-Integritätslevel für die Festlegung der Zielvorgabe der Sicherheitsintegrität der Sicherheitsfunktionen ein, die von den sicherheitsbezogenen E/E/PE-Systemen zu implementieren sind;

ANMERKUNG 2 Diese Norm legt weder die Anforderungen zur Sicherheitsintegrität für irgendeine Sicherheitsfunktion fest, noch bestimmt sie, wie der Sicherheits-Integritätslevel festgelegt wird. Stattdessen stellt sie einen risikobasierenden konzeptionellen Rahmen und Beispielverfahren bereit.

- legt Ausfallgrenzwerte für die von den sicherheitsbezogenen E/E/PE-Systemen auszuführenden Sicherheitsfunktionen fest, die mit den Sicherheits-Integritätsleveln verbunden sind;
- legt eine untere Grenze für die Ausfallgrenzwerte für eine Sicherheitsfunktion fest, die von einem einzelnen sicherheitsbezogenen E/E/PE-System ausgeführt wird. Für sicherheitsbezogene E/E/PE-Systeme, die:
 - in der Betriebsart mit einer niedrigen Anforderungsrate betrieben werden, ist die untere Grenze bei einer mittleren Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung von 10^{-5} festgelegt;
 - in der Betriebsart mit einer hohen Anforderungsrate oder bei kontinuierlicher Anforderung betrieben werden, ist die untere Grenze bei einer mittleren Häufigkeit gefahrbringender Ausfälle von $10^{-9} [h^{-1}]$ festgelegt;

ANMERKUNG 3 Ein einzelnes sicherheitsbezogenes E/E/PE-System bedeutet nicht notwendigerweise eine einkanalige Architektur.

ANMERKUNG 4 Es kann für einfache Systeme möglich sein, Entwürfe von sicherheitsbezogenen Systemen mit niedrigeren Zielwerten für die Sicherheitsintegrität zu erreichen, aber diese Grenzen werden als das betrachtet, was für relativ komplexe Systeme (zum Beispiel sicherheitsbezogene programmierbare elektronische Systeme) gegenwärtig erreicht werden kann.

- legt Anforderungen für die Vermeidung und Beherrschung von systematischen Fehlern fest, die auf Erfahrung und Urteilsvermögen beruhen, das durch praktische Erfahrung in der Industrie gewonnen wurde. Wenn auch die Wahrscheinlichkeit des Auftretens systematischer Ausfälle im Allgemeinen nicht quantifiziert werden kann, erlaubt die Norm jedoch für eine festgelegte Sicherheitsfunktion den Anspruch zu erheben, dass der mit der Sicherheitsfunktion verbundene Ausfallgrenzwert als erreicht betrachtet werden kann, wenn alle Anforderungen dieser Norm erfüllt worden sind;
- 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 eindeutig 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.

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 Gesamtrahmen für das Erreichen 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 Element enthält;
- c) ist auf Elemente 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 entwickelte Spezifikation der Sicherheitsanforderungen des E/E/PE-Systems in die Spezifikation der Entwurfsanforderungen des E/E/PE-Systems verfeinert wird, welche die Beschreibung der Sicherheitsfunktion des E/E/PE-Systems und die Beschreibung der Sicherheitsintegrität des E/E/PE-Systems umfasst;
- e) legt Anforderungen für Tätigkeiten fest, die während des Entwurfs und der Herstellung der sicherheitsbezogenen E/E/PE-Systeme anzuwenden sind (d. h. legt das Modell des Sicherheitslebenszyklus des E/E/PE-Systems fest), einschließlich für anwendungsspezifische integrierte Schaltkreise (ASICs) (siehe IEC 61508-4, 3.2.15), jedoch nicht für Software, die in der IEC 61508-3 behandelt wird (siehe Bilder 2 bis 4). 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 Sicherheit der sicherheitsbezogenen E/E/PE-Systeme fest;
- g) richtet sich nicht an die Betriebs- und Instandhaltungsphase der sicherheitsbezogenen E/E/PE-Systeme – diese wird in 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 4 zeigt die Beziehung zwischen der IEC 61508-2 und der IEC 61508-3.

- i) trifft nicht auf medizinische Einrichtungen gemäß der Normenreihe IEC 60601 zu.

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 zur Verwendung durch technische Komitees bei der Erstellung von Normen gemäß den in *IEC Guide 104* und *ISO/IEC Guide 51* enthaltenen Grundsätzen vorgesehen. Die IEC 61508 ist ebenfalls zur Verwendung als eigenständige Norm vorgesehen. Die horizontale Sicherheitsfunktion dieser internationalen Norm trifft nicht auf medizinische Einrichtungen gemäß der Normenreihe IEC 60601 zu.

1.3 Es steht in der Verantwortung 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 nicht anzuwenden sind, außer in den Festlegungen der Technischen Komitees wird darauf verwiesen oder sie werden eingebunden.

ANMERKUNG 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.

1.4 Bild 1 zeigt den Gesamtrahmen für die Teile 1 bis 7 der IEC 61508 und zeigt die Rolle, welche 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.

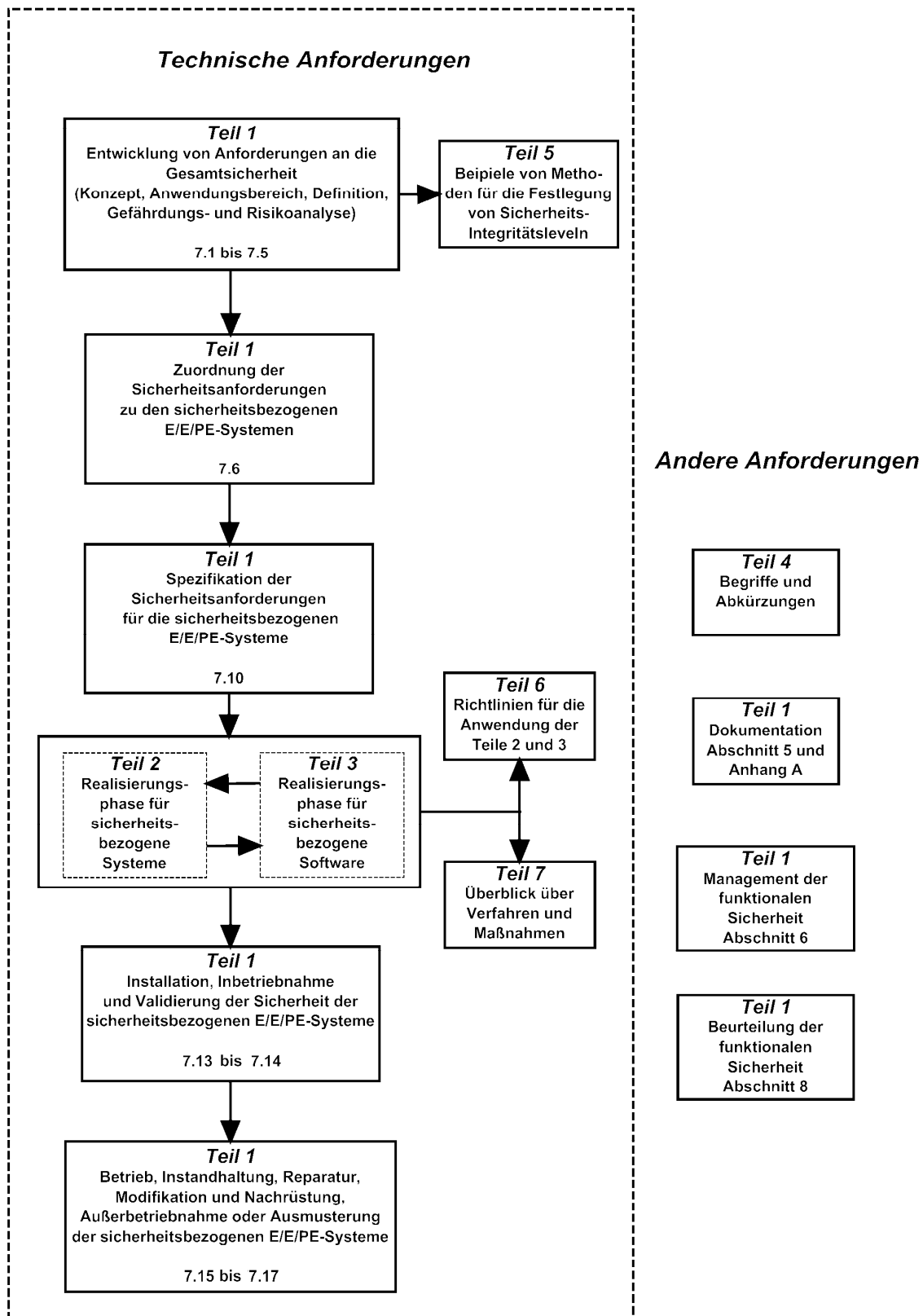


Bild 1 – Gesamttrahmen dieser Norm

2 Normative Verweisungen

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

IEC 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 61000-1-2, *Electromagnetic compatibility (EMC) — Part 1-2: General — Methodology for the achievement of the functional safety of electrical and electronic equipment with regard to electromagnetic phenomena*

IEC 61508-1:—, *Functional safety of electrical/electronic/programmable electronic safetyrelated systems – Part 1: General requirements*

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

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

ANMERKUNG Für eine Einführung in Normen der Reihe IEC 61508 siehe Literaturhinweis [3]. Für Anleitungen zur Anwendung der normativen Teile 1 bis 4 der IEC 61508 siehe Literaturhinweise [4], [5] und [6].

IEC 62280-1, *Railway applications – Communication, signalling and processing systems – Part 1: Safety-related communication in closed transmission systems*

IEC 62280-2, *Railway applications – Communication, signalling and processing systems – Part 2: Safety-related communication in open transmission systems*

ISO/IEC Guide 51:1999, *Guidelines for the inclusion of safety aspects in standards*

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

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.

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 des Sicherheitslebenszyklus des E/E/PE-Systems

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 Sicherheitslebenszyklus des E/E/PE-Systems.

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

7.1.1.2 Für alle Phasen des Sicherheitslebenszyklus des E/E/PE-Systems 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 Ergebnisse(Ausgaben), um mit dem Unterabschnitt überein zu stimmen.

7.1.2 Ziele

7.1.2.1 Das erste Ziel der Anforderungen dieses Unterabschnittes ist es, die Phasen in dem Sicherheitslebenszyklus des E/E/PE-Systems, 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 Sicherheitslebenszyklus des E/E/PE-Systems zu dokumentieren.

7.1.3 Anforderungen

7.1.3.1 Der Sicherheitslebenszyklus des E/E/PE-Systems, der für die Übereinstimmung mit dieser Norm verwendet werden muss, ist der in Bild 2 festgelegte. Bild 3 zeigt ein detailliertes V-Modell des ASIC-Entwicklungslebenszyklus für den Entwurf von ASICs (siehe IEC 61508-4, 3.2.15). Falls ein anderer Sicherheitslebenszyklus des E/E/PE-Systems oder ASIC-Entwicklungslebenszyklus 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 1 Bild 4 zeigt den Anwendungsbereich und die Beziehung zwischen der IEC 61508-2 und der IEC 61508-3.

ANMERKUNG 2 Es gibt bedeutende Ähnlichkeiten zwischen dem ASIC-Entwurfsprozess und dem Software-Entwicklungsprozess. IEC 61508-3 empfiehlt das V-Modell für den Entwurf von sicherheitsbezogener Software. Das V-Modell erfordert zur Vermeidung und Beherrschung systematischer Fehler einen klar strukturierten Entwurfsprozess und eine modulare Softwarestruktur. Der ASIC-Entwicklungslebenszyklus für den Entwurf von ASICs in Bild 3 folgt diesem Modell. Zunächst werden die Anforderungen für die ASIC-Spezifikation von den Systemanforderungen abgeleitet; ASIC-Architektur, ASIC-Entwurf und Modulentwurf folgen. Die Ergebnisse jeder Stufe auf der linken Seite des V werden Eingabe zur nächsten Stufe und werden weiterhin, wo erforderlich, auf die vorherige Stufe zur Iteration zurückgekoppelt, bis der endgültige Code erzeugt wird. Dieser Code wird gegen den entsprechenden Entwurf durch Post-Layout-

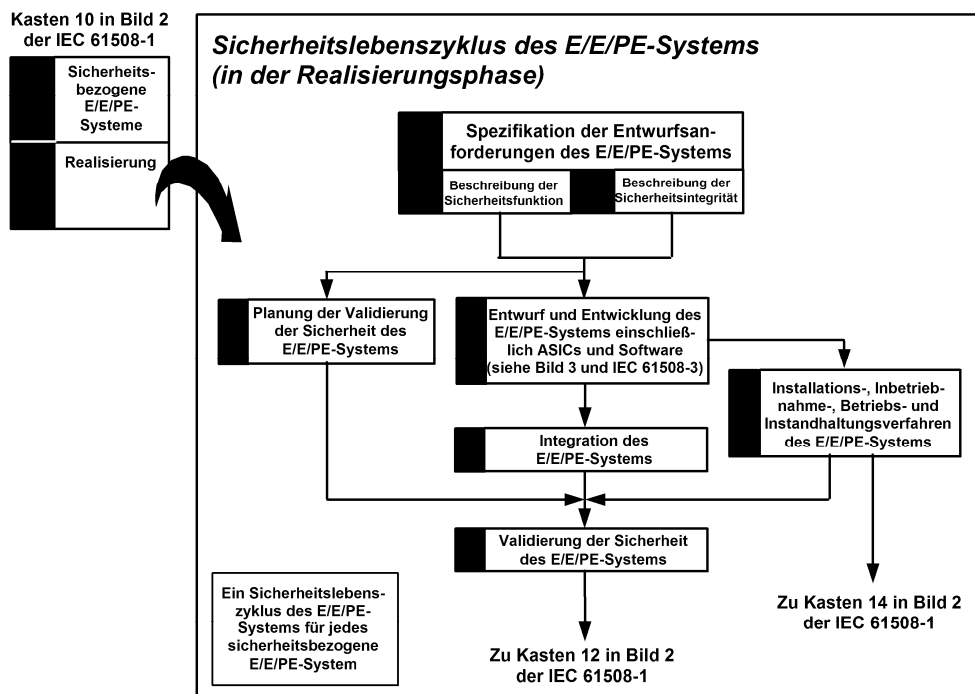
Simulation, Modultest, Modulintegrationstest und Verifikation des gesamten ASIC verifiziert. Die Ergebnisse von irgendeiner Stufe können eine Überarbeitung irgendeiner der vorherigen Stufen erfordern. Zum Schluss ist der ASIC nach seiner Integration in das sicherheitsbezogene E/E/PE-System validiert.

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 Sicherheitslebenszyklus des E/E/PE-Systems laufen.

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

7.1.3.4 Außer wenn während der Planung der funktionalen Sicherheit begründet, müssen die Ergebnisse jeder Phase des Sicherheitslebenszyklus des E/E/PE-Systems dokumentiert werden (siehe Abschnitt 5 der IEC 61508-1).

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



ANMERKUNG 1 Siehe auch IEC 61508-6, A.2(b).

ANMERKUNG 2 Dieses Bild zeigt nur jene Phasen des Sicherheitslebenszyklus des E/E/PE-Systems, die innerhalb der Realisierungsphase des Gesamt-Sicherheitslebenszyklus liegen. Der vollständige Sicherheitslebenszyklus des E/E/PE-Systems wird auch Aspekte der nachfolgenden Phasen des Gesamt-Sicherheitslebenszyklus (Kästen 12 bis 16 in Bild 2 von IEC 61508-1) enthalten, die spezifisch für das sicherheitsbezogene E/E/PE-System sind.

Bild 2 – Sicherheitslebenszyklus des E/E/PE-Systems (in der Realisierungsphase)

— Entwurf —

E DIN EN 61508-2 (VDE 0803-2):2009-06
FprEN 61508-2:2008

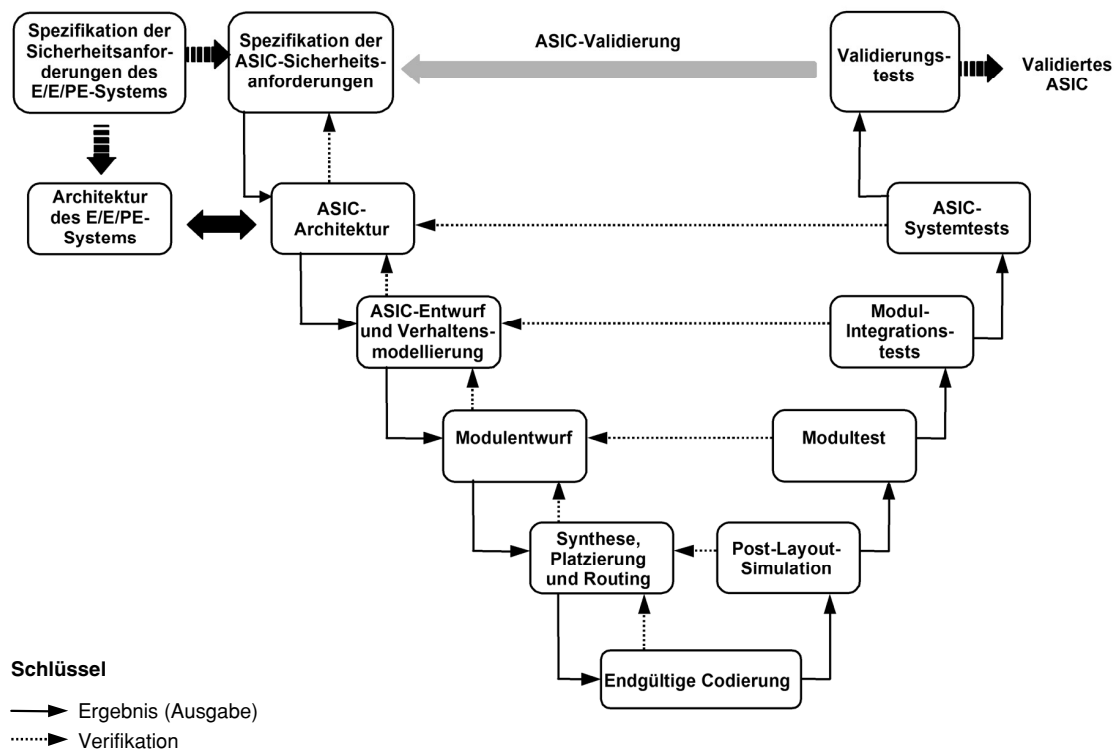


Bild 3 – ASIC-Entwicklungslebenszyklus (V-Modell)

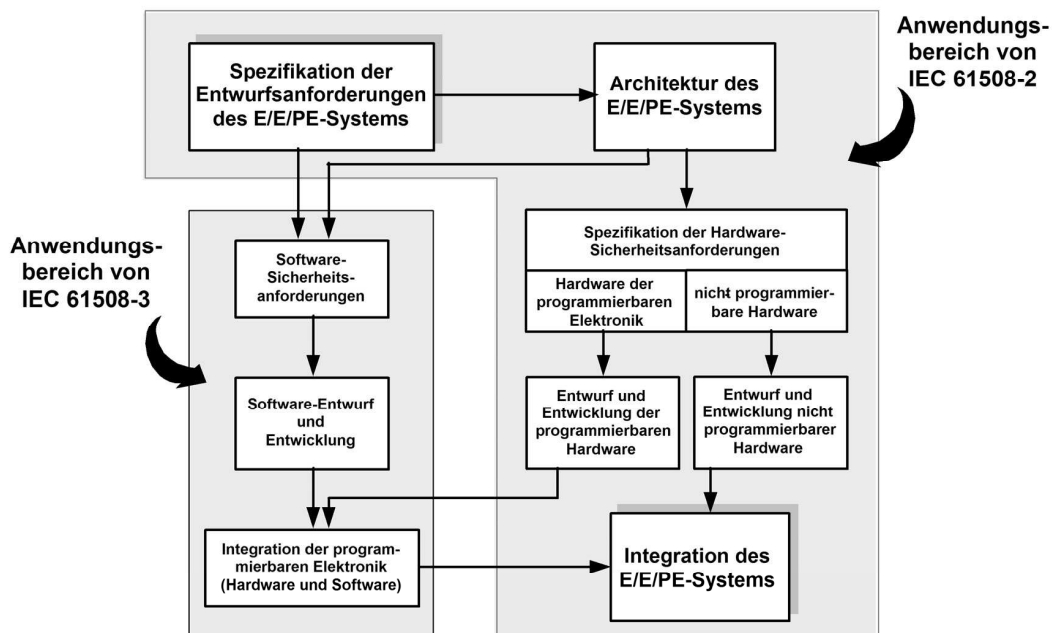


Bild 4 – Beziehung zwischen IEC 61508-2 und IEC 61508-3 und ihre Anwendungsbereiche

Tabelle 1 – Überblick – Realisierungsphase des Sicherheitslebenszyklus des E/E/PE-Systems

Phase des Sicherheitslebenszyklus		Ziele	Anwendungsbereich	Unterabschnitt für Anforderungen	Eingaben	Ergebnisse (Ausgaben)
Kastennummer in Bild 2	Titel					
10.1	Spezifikation der Entwurfsanforderungen des E/E/PE-Systems	Für jedes sicherheitsbezogene E/E/PE-System die Entwurfsanforderungen in Form von Teilsystemen und Elementen festzulegen (siehe IEC 61508-1, 7.10.2).	Sicherheitsbezogenes E/E/PE-System	7.2.2	Spezifikation der Sicherheitsanforderungen des E/E/PE-Systems (siehe IEC 61508-1, 7.10)	Spezifikation der Entwurfsanforderungen des E/E/PE-Systems, welche die Einrichtung und Architekturen für das E/E/PE-System beschreibt
10.2	Planung der Validierung der Sicherheit des E/E/PE-Systems	Die Validierung der Sicherheit des sicherheitsbezogenen E/E/PE-Systems zu planen.	Sicherheitsbezogenes E/E/PE-System	7.3.2	Spezifikation der Sicherheitsanforderungen des E/E/PE-Systems und Spezifikation der Entwurfsanforderungen des E/E/PE-Systems	Plan für die Validierung der Sicherheit der sicherheitsbezogenen E/E/PE-Systeme
10.3	Entwurf und Entwicklung des E/E/PE-Systems	Das sicherheitsbezogene E/E/PE-System (einschließlich ASICs, wenn zutreffend) zu entwerfen und zu entwickeln, um die Spezifikation der Entwurfsanforderungen des E/E/PE-Systems zu erfüllen (im Hinblick auf die Anforderungen zu den Sicherheitsfunktionen und die Anforderungen zur Sicherheitsintegrität (siehe 7.2)).	Sicherheitsbezogenes E/E/PE-System	7.4.2 bis 7.4.11	Spezifikation der Entwurfsanforderungen des E/E/PE-Systems	Entwurf der sicherheitsbezogenen E/E/PE-Systeme in Übereinstimmung mit der Spezifikation der Entwurfsanforderungen des E/E/PE-Systems Plan für den Integrationstest des E/E/PE-Systems Informationen zur PES-Architektur als Eingabe für die Spezifikation der Softwareanforderungen
10.4	Integration des E/E/PE-Systems	Das sicherheitsbezogene E/E/PE-System zu integrieren und zu testen.	Sicherheitsbezogenes E/E/PE-System	7.5.2	Entwurf des E/E/PE-Systems Plan der Integrationstests des E/E/PE-Systems Hardware und Software der programmierbaren Elektronik	Vollständig funktionierende sicherheitsbezogene E/E/PE-Systeme in Übereinstimmung mit dem Entwurf des E/E/PE-Systems Ergebnisse der Integrationstests des E/E/PE-Systems
10.5	Installations-, Inbetriebnahme-, Betriebs- und Instandhaltungsverfahren des E/E/PE-Systems	Verfahren zu entwickeln um sicherzustellen, dass die erforderliche funktionale Sicherheit des sicherheitsbezogenen E/E/PE-Systems während des Betriebs und der Instandhaltung aufrechterhalten wird.	Sicherheitsbezogenes E/E/PE-System EUC	7.6.2	Spezifikation der Entwurfsanforderungen des E/E/PE-Systems Entwurf des E/E/PE-Systems	Installations-, Inbetriebnahme-, Betriebs- und Instandhaltungsverfahren des E/E/PE-Systems für jedes einzelne E/E/PE-System

Tabelle 1 (fortgesetzt)

Phase des Sicherheitslebenszyklus		Ziele	Anwendungsbereich	Unterabschnitt für Anforderungen	Eingaben	Ergebnisse (Ausgaben)
Kastennummer in Bild 2	Titel					
10.6	Validierung der Sicherheit des E/E/PE-Systems	Zu validieren, dass das sicherheitsbezogene E/E/PE-System in jeder Hinsicht den Anforderungen zur Sicherheit im Sinne der erforderlichen Sicherheitsfunktionen und der Sicherheitsintegrität entspricht.	Sicherheitsbezogenes E/E/PE-System	7.7.2	Spezifikation der Sicherheitsanforderungen des E/E/PE-Systems und Spezifikation der Entwurfsanforderungen des E/E/PE-Systems Plan für die Validierung der Sicherheit der sicherheitsbezogenen E/E/PE-Systeme	Vollständig in Bezug auf Sicherheit validierte sicherheitsbezogene E/E/PE-Systeme Ergebnisse der Validierung der Sicherheit des E/E/PE-Systems
–	Modifikation des E/E/PE-Systems	Korrekturen, Verbesserungen oder Anpassungen an dem sicherheitsbezogenen E/E/PE-System zu machen und sicherzustellen, dass die erforderliche Sicherheitsintegrität erreicht wird und erhalten bleibt.	Sicherheitsbezogenes E/E/PE-System	7.8.2	Spezifikation der Entwurfsanforderungen des E/E/PE-Systems	Ergebnisse der Modifikation des E/E/PE-Systems
–	Verifikation des E/E/PE-Systems	Die Ergebnisse einer gegebenen Phase zu testen und zu bewerten, um Korrektheit und Konsistenz hinsichtlich der Produkte und Normen sicherzustellen, welche die Eingabe zu dieser Phase bilden.	Sicherheitsbezogenes E/E/PE-System	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/PE-Systems	Zu untersuchen und eine Beurteilung zu erreichen zu der durch das sicherheitsbezogene E/E/PE-System erreichten funktionalen Sicherheit.	Sicherheitsbezogenes E/E/PE-System	8	Plan für die Beurteilung der funktionalen Sicherheit des E/E/PE-Systems	Ergebnisse der Beurteilung der funktionalen Sicherheit des E/E/PE-Systems

7.2 Entwurfsanforderungen des E/E/PE-Systems

ANMERKUNG Diese Phase entspricht Kasten 10.1 von Bild 2.

7.2.1 Ziel

Das Ziel der Anforderungen dieses Unterabschnittes ist es, die Entwurfsanforderungen für jedes sicherheitsbezogene E/E/PE-System in Form von Teilsystemen und Elementen festzulegen.

ANMERKUNG 1 Die Spezifikation der Entwurfsanforderungen des E/E/PE-Systems wird normalerweise von der Spezifikation der Sicherheitsanforderungen des E/E/PE-Systems durch Zerlegung der Sicherheitsfunktionen und Zuordnung von Teilen der Sicherheitsfunktion zu Teilsystemen (zum Beispiel Gruppen von Sensoren, Logiksystemen oder Aktoren) abgeleitet. Die Anforderungen für die Teilsysteme können in der Spezifikation der Entwurfsanforderungen des E/E/PE-Systems enthalten sein oder können separat vorliegen und von der Spezifikation der Entwurfsanforderungen des E/E/PE-Systems referenziert sein. Teilsysteme können weiter in Elemente und Architekturen zerlegt werden, um die Anforderungen zu Entwurf und Entwicklung von 7.4 zu erfüllen. Die Anforderungen für diese Elemente können in den Anforderungen für die Teilsysteme enthalten sein oder können separat vorliegen und von den Anforderungen zum Teilsystem aus referenziert sein.

7.2.2 Allgemeines

7.2.2.1 Die Spezifikation der Entwurfsanforderungen des E/E/PE-Systems muss von den in 7.10 der IEC 61508-1 spezifizierten Sicherheitsanforderungen des E/E/PE-Systems abgeleitet 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 Sicherheitslebenszyklus des E/E/PE-Systems auszuführen (zum Beispiel Entwurf, Validierung, Beurteilung der funktionalen Sicherheit und Instandhaltung). Siehe auch 7.4.2.3.

7.2.2.2 Die Spezifikation der Entwurfsanforderungen des E/E/PE-Systems muss in einer Art und Weise ausgedrückt und strukturiert werden, so dass sie wie folgt ist:

- a) klar, genau, unzweideutig, nachprüfbar, testbar, pflegbar und ausführbar;
- b) geschrieben, um Denjenigen Unterstützung zu leisten, die wahrscheinlich die Informationen in irgendeiner Phase des Sicherheitslebenszyklus des E/E/PE-Systems verwenden; und
- c) zurückführbar auf die Spezifikation der Sicherheitsanforderungen des E/E/PE-Systems.

7.2.3 Spezifikation der Entwurfsanforderungen des E/E/PE-Systems

7.2.3.1 Die Spezifikation der Entwurfsanforderungen des E/E/PE-Systems muss Entwurfsanforderungen in Bezug auf Sicherheitsfunktionen (siehe 7.2.3.2) und Entwurfsanforderungen in Bezug auf Sicherheitsintegrität (siehe 7.2.3.3) enthalten.

7.2.3.2 Die Spezifikation der Entwurfsanforderungen des E/E/PE-Systems muss, wie durch die Spezifikation der Anforderungen zu den Sicherheitsfunktionen des E/E/PE-Systems (siehe 7.10.2.6 der IEC 61508-1) festgelegt, Einzelheiten der gesamten für die Implementierung der erforderlichen Sicherheitsfunktionen notwendigen Hardware und Software enthalten. Die Spezifikation muss für jede Sicherheitsfunktion beinhalten:

- a) Anforderungen für die Teilsysteme und Anforderungen für ihre Hardware- und Softwareelemente wie zutreffend;
- b) Anforderungen für die Integration der Teilsysteme und ihrer Hardware- und Softwareelemente, um die Spezifikation der Anforderungen zu den Sicherheitsfunktionen des E/E/PE-Systems zu erfüllen;
- c) Durchsatzleistungsfähigkeit, die es ermöglicht Anforderungen in Bezug auf Reaktionszeit zu erfüllen;
- d) Anforderungen zu Genauigkeit und Widerstandsfähigkeit für Messungen und Steuerungen;
- e) Schnittstellen des sicherheitsbezogenen E/E/PE-Systems und Bedienerschnittstellen;
- f) Schnittstellen zwischen den sicherheitsbezogenen E/E/PE-Systemen und allen anderen Systemen (entweder innerhalb oder außerhalb der EUC);
- g) alle Verhaltensweisen der sicherheitsbezogenen E/E/PE-Systeme, insbesondere Ausfallverhalten und die erforderliche Reaktion (zum Beispiel Alarm, automatisches Herunterfahren) der sicherheitsbezogenen E/E/PE-Systeme;
- h) die Bedeutung aller Hardware-/Softwarewechselwirkungen und wo zutreffend, alle erforderlichen Einschränkungen zwischen Hardware und Software;

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

- i) alle Grenzbedingungen und Einschränkungen für die sicherheitsbezogenen E/E/PE-Systeme und ihre zugehörigen Elemente, zum Beispiel zeitliche Einschränkungen, oder Einschränkungen wegen möglicher Ausfälle infolge gemeinsamer Ursache;
- j) alle speziellen Anforderungen in Bezug auf die Verfahren für Einschalten und Wiederstart der sicherheitsbezogenen E/E/PE-Systeme.

7.2.3.3 Die Spezifikation der Entwurfsanforderungen des E/E/PE-Systems muss für den Entwurf relevante Einzelheiten enthalten, um den Sicherheits-Integritätslevel und den erforderlichen Ausfallgrenzwert für die Sicherheitsfunktion, wie durch die Spezifikation der Anforderungen zur Sicherheitsintegrität des E/E/PE-Systems festgelegt (siehe 7.10.2.7 der IEC 61508-1), zu erreichen, einschließlich:

- a) der Architektur jedes Teilsystems, die erforderlich ist, um die Einschränkungen auf Grund der Architektur zur Sicherheitsintegrität der Hardware (siehe 7.4.4) zu erfüllen;
- b) aller relevanten Zuverlässigkeitsmodellierungsparameter, wie zum Beispiel der erforderlichen Häufigkeit von Wiederholungsprüfungen aller Hardwareelemente, die zum Erreichen des Ausfallgrenzwerts notwendig sind;

ANMERKUNG 1 Während der Spezifikation der Entwurfsanforderungen des E/E/PE-Systems sollte die Anwendung, in der die sicherheitsbezogenen E/E/PE-Systeme verwendet werden sollen, berücksichtigt werden. Dies ist insbesondere für die Instandhaltung wichtig, wo 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 Zeit für Produkte in einer besser überwachten Anwendung.

- c) den zu erfolgenden Handlungen im Falle eines durch Diagnosemaßnahmen erkannten gefahrbringenden Ausfalls;
- d) den Anforderungen, Einschränkungen, Funktionen und Einrichtungen, um die Durchführung der Wiederholungsprüfung der E/E/PE-Hardware zu ermöglichen;
- e) dem Leistungsvermögen verwendeter Einrichtungen den Extremwerten aller Umgebungsbedingungen (z. B. Temperatur, Feuchte, mechanisch, elektrisch) zu entsprechen, die als während des Sicherheitslebenszyklus des E/E/PE-Systems erforderlich festgelegt sind, einschließlich Herstellung, Lagerung, Transport, Prüfung, Installation, Inbetriebnahme, Betrieb und Instandhaltung;
- f) der erforderlichen elektromagnetischen Störfestigkeit (siehe IEC 61000-1-2, zweite Edition in Vorbereitung);
- g) der für das Sicherheitsmanagement (siehe Teil 1, Abschnitt 6.2.5) notwendigen Maßnahmen zu Qualitätssicherung/Qualitätskontrollmaßnahmen.

ANMERKUNG 2 Die Störfestigkeit kann sich für unterschiedliche Elemente des sicherheitsbezogenen Systems unterscheiden, abhängig vom physikalischen Ort und den Anordnungen der Energieversorgungen.

ANMERKUNG 3 Hilfestellung kann in EMV-Produktnormen gefunden werden. Es ist jedoch wichtig zu berücksichtigen, dass für besondere Einsatzorte oder wenn die Betriebsmittel für die Verwendung in rauer elektromagnetischer Umgebung vorgesehen sind, höhere Störfestigkeitspegel oder zusätzliche Störfestigkeitsanforderungen, als die in solchen Normen festgelegten, notwendig sein können.

7.2.3.4 Die Spezifikation der Entwurfsanforderungen des E/E/PE-Systems muss mit dem Fortschritt im Entwurf im Detail vervollständigt und nach Modifikation wie notwendig aktualisiert werden.

7.2.3.5 Zur Vermeidung von Irrtümern während der Entwicklung der Spezifikation der Entwurfsanforderungen des E/E/PE-Systems muss eine angemessene Gruppe von Verfahren und Maßnahmen nach Tabelle B.1 verwendet werden.

7.2.3.6 Die durch die Entwurfsanforderungen des E/E/PE-Systems auferlegten Auswirkungen auf die Architektur (wie zum Beispiel eine Anforderung für weit reichende Konfigurationsmöglichkeiten) müssen berücksichtigt werden.

ANMERKUNG Dies sollte die Überlegung der Einfachheit der Implementierung, um den erforderlichen Sicherheits-Integritätslevel zu erreichen, einschließen (einschließlich Überlegungen zur Architektur und zur Zuteilung von Funktionalität zu Konfigurationsdaten oder zum Embedded-System).

7.3 Planung der Validierung der Sicherheit des E/E/PE-Systems

ANMERKUNG Diese Phase entspricht Kasten 10.2 in Bild 2. Sie wird üblicherweise parallel zum Entwurf und zur Entwicklung des E/E/PE-Systems (siehe 7.4) ausgeführt.

7.3.1 Ziel

Das Ziel der Anforderungen dieses Unterabschnittes ist es, die Validierung der Sicherheit des sicherheitsbezogenen E/E/PE-Systems 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 das sicherheitsbezogene E/E/PE-System die Spezifikation der Sicherheitsanforderungen des E/E/PE-Systems (siehe IEC 61508-1, 7.10) und die Spezifikation der Entwurfsanforderungen des E/E/PE-Systems (siehe 7.2) erfüllt.

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

- a) alle in der Spezifikation der Sicherheitsanforderungen des E/E/PE-Systems und der Spezifikation der Entwurfsanforderungen des E/E/PE-Systems 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 Bewertungskriterien, die anzuwenden sind, um die festgelegten elektromagnetischen Störfestigkeitseinstufungsgrenzwerte zu validieren;

ANMERKUNG Anleitung zur Spezifikation der Tests der elektromagnetischen Störfestigkeit für Elemente von sicherheitsbezogenen Systemen ist in IEC 61000-1-2 enthalten.

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

7.4 Entwurf und Entwicklung des E/E/PE-Systems

ANMERKUNG Diese Phase entspricht Kasten 10.3 in Bild 2. Sie wird üblicherweise parallel zur Planung der Validierung der Sicherheit des E/E/PE-Systems (siehe 7.3) ausgeführt.

7.4.1 Ziel

Das Ziel der Anforderungen dieses Unterabschnittes ist es, das sicherheitsbezogene E/E/PE-System (einschließlich ASICs wenn zutreffend, siehe IEC 61508-4, 3.2.15) zu entwerfen und zu entwickeln, um die Spezifikation der Entwurfsanforderungen des E/E/PE-Systems (im Hinblick auf die Anforderungen zu den Sicherheitsfunktionen und die Anforderungen zur Sicherheitsintegrität (siehe 7.2)) zu erfüllen.

7.4.2 Allgemeine Anforderungen

7.4.2.1 Der Entwurf des sicherheitsbezogenen E/E/PE-Systems muss in Übereinstimmung mit der Spezifikation der E/E/PE-Entwurfsanforderungen (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 Gesamt-Hardwarearchitektur und Gesamt-Softwarearchitektur, Sensoren, Aktoren, programmierbarer Elektronik, ASICs, Embedded-Software, Anwendungssoftware, Daten usw.) muss alle Anforderungen von a) bis e) wie folgt erfüllen:

- a) die Anforderungen zur Sicherheitsintegrität der Hardware, bestehend aus
 - den Einschränkungen der Sicherheitsintegrität der Hardware auf Grund der Architektur (siehe 7.4.4) und
 - den Anforderungen für die Quantifizierung der Auswirkung zufälliger Ausfälle (siehe 7.4.5);
- b) die besonderen Architektur Anforderungen für ICs mit On-Chip-Redundanz (siehe Anhang E), wo zutreffend, außer es kann begründet werden, dass der gleiche Grad von Unabhängigkeit zwischen verschiedenen Kanälen durch Anwendung eines anderen Maßnahmenkatalogs erreicht wird;
- c) die Anforderungen zur systematischen Sicherheitsintegrität (systematische Eignung), die durch Ausführung einer der nachfolgenden Konformitätspfade erfüllt werden können:
 - Pfad 1_S: Übereinstimmung mit den Anforderungen zur Vermeidung von systematischen Fehlern (siehe 7.4.6 und IEC 61508-3) und den Anforderungen zur Beherrschung von systematischen Fehlern (siehe 7.4.7 und IEC 61508-3); oder
 - Pfad 2_S: Übereinstimmung mit den Anforderungen für den Nachweis, dass die Betriebsmittel betriebsbewährt sind (siehe 7.4.10); oder
 - Pfad 3_S (nur Software): Übereinstimmung mit den Anforderungen von IEC 61508-3, 7.4.2.1 und Anhang G;

ANMERKUNG Das tief gestellte „S“ in den oben aufgeführten Pfaden bezeichnet die systematische Sicherheitsintegrität zur Unterscheidung von den Pfaden 1_H und Pfad 2_H für die Sicherheitsintegrität der Hardware.

- d) die Anforderungen an das Systemverhalten bei Erkennung eines Fehlers (siehe 7.4.8);
- e) die Anforderungen für Datenkommunikationsprozesse (siehe 7.4.11).

7.4.2.3 Wenn ein sicherheitsbezogenes E/E/PE-System sowohl Sicherheitsfunktionen, als auch Nicht-Sicherheitsfunktionen enthält, 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).

ANMERKUNG 1 Eine ausreichende Unabhängigkeit der Implementierung liegt vor, wenn gezeigt wird, dass die Wahrscheinlichkeit eines abhängigen Ausfalls zwischen den nicht sicherheitsbezogenen 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 Sicherheitslebenszyklus des E/E/PE-Systems auszuführen (zum Beispiel Entwurf, Validierung, Beurteilung der funktionalen Sicherheit und Instandhaltung).

7.4.2.4 Die Anforderungen an 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-Integritätslevel 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

Sicherheits-Integritätslevel enthalten, im Vergleich zum höchsten Sicherheits-Integritätslevel, der mit den betroffenen Sicherheitsfunktionen verbunden ist, ausreichend gering ist.

ANMERKUNG 2 Wenn mehrere Sicherheitsfunktionen in einem sicherheitsbezogenen E/E/PE-System implementiert werden, ist es notwendig, die Möglichkeit zu betrachten, dass ein einzelner Fehler einen Ausfall mehrerer Sicherheitsfunktionen bedingt. In einer solchen Situation kann es angemessen sein, die Anforderungen für Hardware und Software auf der Basis eines höheren Sicherheits-Integritätslevels, als dem mit irgendeiner der Sicherheitsfunktionen in Verbindung stehenden, in Abhängigkeit von dem mit einem solchen Ausfall verbundenen Risiko, festzulegen.

7.4.2.5 Ist Unabhängigkeit zwischen den Sicherheitsfunktionen gefordert (siehe 7.4.2.3 und 7.4.2.4), muss Folgendes während des Entwurfs dokumentiert werden:

- a) die Methode zum Erreichen der Unabhängigkeit;
- b) die Begründung der Methode.

7.4.2.6 Die Anforderungen an sicherheitsbezogene Software (siehe IEC 61508-3) müssen dem Entwickler des sicherheitsbezogenen E/E/PE-Systems zur Verfügung gestellt werden.

7.4.2.7 Der Entwickler des sicherheitsbezogenen E/E/PE-Systems muss die Anforderungen für die sicherheitsbezogene Software und Hardware überprüfen, um sicherzustellen, dass die Anforderungen angemessen festgelegt sind. Insbesondere muss der Entwickler des E/E/PE-Systems Folgendes betrachten:

- a) Sicherheitsfunktionen;
- b) Anforderungen zur Sicherheitsintegrität des sicherheitsbezogenen E/E/PE-Systems;
- c) Betriebsmittel- und Bedienerschnittstellen.

7.4.2.8 Die Dokumentation des Entwurfs des sicherheitsbezogenen E/E/PE-Systems muss diejenigen Verfahren und Maßnahmen festlegen, die während der Phasen des Sicherheitslebenszyklus des E/E/PE-Systems notwendig sind, um den Sicherheits-Integritätslevel zu erreichen.

7.4.2.9 Die Dokumentation des Entwurfs des sicherheitsbezogenen E/E/PE-Systems muss die Begründung für die Verfahren und Maßnahmen enthalten, die gewählt worden sind, um eine Zusammenstellung zu bilden, die für den erforderlichen Sicherheits-Integritätslevel ausreichend ist.

ANMERKUNG Die Wahl eines gesamtheitlichen Lösungsansatzes mit Ausführung unabhängiger Typ-Prüfungen der sicherheitsbezogenen E/E/PE-Systeme (einschließlich Sensoren, Aktoren usw.) für Hardware und Software, Diagnose-tests und Programmierwerkzeuge und, wo immer möglich, Verwendung angemessener Programmiersprachen für die Software bietet die Möglichkeit, die Komplexität des Anwendungsengineering des E/E/PE-Systems zu reduzieren.

7.4.2.10 Während der Entwurfs- und Entwicklungstätigkeiten muss die Bedeutung (wo relevant) aller Hardware- und Software-Wechselwirkungen identifiziert, bewertet und dokumentiert werden.

7.4.2.11 Der Entwurf muss auf einer Aufteilung in Teilsysteme basieren, wobei jedes Teilsystem einen festgelegten Entwurf und eine Zusammenstellung von Integrationstests besitzt (siehe 7.4.9).

ANMERKUNG 1 Ein Teilsystem kann als aus einem einzigen Element oder einer Gruppe von Elementen bestehend betrachtet werden. Siehe IEC 61508-4 für Definitionen. Ein vollständiges sicherheitsbezogenes E/E/PE-System setzt sich aus einer Anzahl von identifizierbaren und separaten Teilsystemen zusammen, die, wenn sie zusammengefügt sind, die betrachtete Sicherheitsfunktion implementieren. Ein Teilsystem kann mehr als einen Kanal besitzen. Siehe 7.4.9.3 und 7.4.9.4.

ANMERKUNG 2 Wann immer möglich, sollten vorhandene verifizierte Teilsysteme in der Implementierung verwendet werden. Diese Aussage ist nur gültig, wenn beinahe 100 % Übereinstimmung in Teilsystem- oder Elementfunktionalität, Kapazität und Leistungsfähigkeit mit den neuen Anforderungen besteht oder das verifizierte Teilsystem oder Element in einer solchen Art und Weise strukturiert ist, dass es dem Anwender möglich ist, nur die für die spezielle Anwendung erforderliche Funktion, Kapazität oder Leistungsfähigkeit auszuwählen. Eine übermäßige Funktionalität, Kapazität oder Leistungsfähigkeit kann schädlich für die Systemsicherheit sein, wenn das vorhandene Teilsystem oder Element übermäßig kompliziert ist oder nicht verwendete Bestandteile enthält, und wenn ein Schutz gegen unbeabsichtigte Funktionen nicht erreicht werden kann.

7.4.2.12 Wenn der einleitende Entwurf des sicherheitsbezogenen E/E/PE-Systems abgeschlossen worden ist, muss eine Analyse durchgeführt werden, um zu ermitteln, ob irgendein vernünftigerweise vorhersehbarer Ausfall des sicherheitsbezogenen E/E/PE-Systems eine Gefährdungssituation verursachen oder eine Anforderung an irgendeine andere Maßnahme zur Risikobeherrschung stellen könnte. Wenn irgendein vernünftigerweise vorhersehbarer Ausfall eine dieser Auswirkung haben könnte, muss die erste Priorität die Veränderung des Entwurfs des sicherheitsbezogenen E/E/PE-Systems sein, um solche Ausfallarten zu vermeiden. Wenn dies nicht erfolgen kann, müssen Maßnahmen gewählt werden, um die Wahrscheinlichkeit solcher Ausfallarten auf ein Maß zu reduzieren, das angemessen zum Ausfallgrenzwert ist. Diese Maßnahmen müssen den Anforderungen dieser Norm unterliegen.

7.4.2.13 Unterlastung (en: de-rating, siehe IEC 61508-7) sollte für alle Hardwareelemente berücksichtigt werden. Die Begründung für den Betrieb irgendwelcher Hardwareelemente an ihren Grenzen muss dokumentiert werden (siehe IEC 61508-1, Abschnitt 5).

ANMERKUNG Wo Unterlastung angebracht ist, ist ein Unterlastungsgrad von mindestens zweidrittel typisch.

7.4.2.14 Wenn der Entwurf eines sicherheitsbezogenen E/E/PE-Systems ein oder mehrere ASICs zur Implementierung einer Sicherheitsfunktion einschließt, muss ein ASIC-Entwicklungslebenszyklus (siehe 7.1.3.1) angewendet werden.

7.4.3 Synthese von Elementen zum Erreichen der erforderlichen systematischen Eignung

7.4.3.1 Um die Anforderungen zur systematischen Sicherheitsintegrität zu erfüllen, kann das vorgesehene sicherheitsbezogene E/E/PE-System unter den in diesem Abschnitt beschriebenen Umständen in Elemente unterschiedlicher systematischer Eignung aufgeteilt werden.

ANMERKUNG 1 Die systematische Eignung eines Elements bestimmt das Potenzial für systematische Fehler dieses Elements, dass sie zu einem Ausfall der Sicherheitsfunktion führen. Das Konzept der systematischen Eignung eines Elements ist gleichermaßen auf Hardware- und Softwareelemente anwendbar.

ANMERKUNG 2 IEC 61508-1, Abschnitt 7.6.2.7 beachtet den Nutzen von Unabhängigkeit und Diversität auf der Ebene einer Sicherheitsfunktion und der sicherheitsbezogenen E/E/PE-Systeme, zu denen sie zugeordnet werden könnte. Diese Ideen können auch auf der Ebene des detaillierten Entwurfs angewendet werden, wo eine Anordnung von Elementen, die eine Sicherheitsfunktion implementieren, potenziell eine bessere systematische Leistungsfähigkeit erreichen kann, als einzelne Elemente.

7.4.3.2 Für ein Element mit der systematischen Eignung SIL N ($N = 1, 2, 3$), bei dem ein systematischer Fehler dieses Elements nicht zu einem Ausfall der festgelegten Sicherheitsfunktion führt, dies jedoch nur in Kombination mit einem zweiten systematischen Fehler eines anderen Elements mit der systematischen Eignung SIL N erfolgt, kann die systematische Eignung der Kombination der beiden Elemente als eine systematische Eignung von SIL ($N + 1$) betrachtet werden, vorausgesetzt dass zwischen den beiden Elementen eine ausreichende Unabhängigkeit besteht (siehe Abschnitt 7.4.3.4).

ANMERKUNG Die Unabhängigkeit der Elemente kann nur beurteilt werden, wenn die konkrete Anwendung der Elemente in Bezug auf die definierten Sicherheitsfunktionen bekannt ist.

7.4.3.3 Die systematische Eignung, die für eine Kombination von Elementen in Anspruch genommen werden kann, wenn jedes einzelne Element die systematische Eignung SIL N besitzt, kann höchstens SIL ($N + 1$) betragen. Ein Element von SIL N kann nur einmal auf diese Weise verwendet werden. Es ist nicht gestattet SIL ($N + 2$) und besser durch aufeinander folgendes Zusammenfügen von Anordnungen aus SIL N-Elementen zu erreichen.

7.4.3.4 Ausreichende Unabhängigkeit im Entwurf zwischen Elementen und in der Anwendung von Elementen muss durch eine Analyse gemeinsamer Ursachen begründet werden, um zu zeigen, dass die Wahrscheinlichkeit einer Beeinträchtigung zwischen Elementen und zwischen den Elementen und der Umgebung ausreichend gering im Vergleich zum Sicherheits-Integritätslevel der betrachteten Sicherheitsfunktion ist.

ANMERKUNG 1 Für die systematische Eignung schließen mögliche Methoden zum Erreichen ausreichender Unabhängigkeit hinsichtlich Hardwareentwurf, Realisierung, Betrieb und Instandhaltung Folgendes ein:

- Funktionale Diversität: Verwendung unterschiedlicher Methoden, um die gleichen Ergebnisse zu erreichen;
- Diversitäre Technologien: Verwendung unterschiedlicher Arten von Betriebsmitteln, um die gleichen Ergebnisse zu erreichen;
- Gemeinsame Teile/Dienste: Sicherstellen, dass es keine gemeinsamen Teile oder Dienste oder Hilfssysteme (zum Beispiel Stromversorgungen) gibt, deren Ausfall zu einem gefahrbringenden Ausfall aller Systeme führen kann;
- Gemeinsame Verfahren: Sicherstellen, dass es keine gemeinsamen Betriebs-, Instandhaltungs-, oder Prüfverfahren gibt.

ANMERKUNG 2 Unabhängigkeit von der Anwendung bedeutet, dass Elemente das Ausführungsverhalten untereinander nicht derart ungünstig beeinträchtigen, dass ein gefahrbringender Ausfall auftreten wird.

ANMERKUNG 3 Zur Unabhängigkeit von Softwareelementen siehe IEC 61508-3, Abschnitte 7.4.2.8 und 7.4.2.9.

7.4.4 Einschränkungen der Sicherheitsintegrität der Hardware auf Grund der Architektur

ANMERKUNG 1 Die Anforderungen in Bezug auf Einschränkungen der Sicherheitsintegrität der Hardware sind in Anhang C festgelegt.

ANMERKUNG 2 IEC 61508-6, A.2, gibt einen Überblick über die notwendigen Schritte zum Erreichen der erforderlichen Sicherheitsintegrität der Hardware und zeigt wie dieser Unterabschnitt zu anderen Anforderungen dieser Norm in Bezug steht.

Im Kontext der Sicherheitsintegrität der Hardware ist der höchste Sicherheits-Integritätslevel, der für eine Sicherheitsfunktion beansprucht werden kann, durch die Einschränkungen der Sicherheitsintegrität der Hardware begrenzt, die durch die Implementierung einer der beiden möglichen Pfade (auf System- oder Teilsystemebene zu implementieren) erreicht werden müssen.

- Pfad 1_H basierend auf Ideen der Hardware-Fehlertoleranz und des Anteils sicherer Ausfälle; oder
- Pfad 2_H basierend auf Bauteilzuverlässigkeitsdaten, die aus der Rückmeldung von Endanwendern stammen, erhöhten Konfidenzniveaus und einer Hardware-Fehlertoleranz für festgelegte Sicherheits-Integritätslevel.

Anwendungsspezifische Normen, die auf IEC 61508 basieren, können auf einen bevorzugten Pfad hinweisen (d. h. Pfad 1_H oder Pfad 2_H).

ANMERKUNG 3 Das tief gestellte „H“ in den oben aufgeführten Pfaden bezeichnet die Sicherheitsintegrität der Hardware zur Unterscheidung von den Pfaden 1_S und Pfad 2_S und Pfad 3_S für die systematische Sicherheitsintegrität.

7.4.4.1 Allgemeine Anforderungen

7.4.4.1.1 Im Hinblick auf die Anforderungen zur Hardware-Fehlertoleranz:

- a) bedeutet eine Hardware-Fehlertoleranz von N, dass N + 1 die minimale Anzahl von Fehlern ist, die zu einem Verlust der Sicherheitsfunktion führen können. Bei der Bestimmung der Hardware-Fehlertoleranz darf keine Berücksichtigung von anderen Maßnahmen erfolgen, welche die Auswirkungen von Fehlern beherrschen können, wie zum Beispiel Diagnoseeinrichtungen; und
- b) werden, wo ein Fehler direkt zu einem oder mehreren nachfolgenden Fehlern führt, diese Fehler als ein Einzelfehler betrachtet;
- c) können bei der Bestimmung der erreichten Hardware-Fehlertoleranz bestimmte Fehler unter der Voraussetzung ausgeschlossen werden, dass die Wahrscheinlichkeit ihres Auftretens sehr gering ist im Verhältnis zu den Anforderungen zur Sicherheitsintegrität des Teilsystems. Jeder einzelne Fehlerausschluss muss begründet und dokumentiert werden (siehe Anmerkung 2);
- d) ist der Anteil sicherer Ausfälle eines Elements definiert als das Verhältnis der mittleren Ausfallraten ungefährlicher Ausfälle plus gefahrbringender erkannter Ausfälle des Elements zu der mittleren Gesamtausfallrate des Elements (siehe Anhang C).

ANMERKUNG 1 Die Einschränkungen der Sicherheitsintegrität der Hardware wurden aufgenommen, um eine ausreichend robuste Architektur unter Berücksichtigung des Komplexitätsniveaus der Teilsysteme zu erreichen. Der höchste zulässige Sicherheits-Integritätslevel für die durch das sicherheitsbezogene E/E/PE-System implementierte Sicherheitsfunktion, der unter Anwendung dieser Anforderungen abgeleitet wird, ist der höchstens für die Sicherheitsfunktion in Anspruch nehmbare, auch wenn in einigen Fällen Zuverlässigkeitsberechnungen zeigen, dass ein höherer Sicherheits-Integritätslevel erreicht werden könnte. Es ist weiterhin anzumerken, dass auch wenn die Hardware-Fehlertoleranz für alle Teilsysteme erreicht wird, trotzdem eine Zuverlässigkeitsberechnung notwendig ist, um zu zeigen, dass der festgelegte Ausfallgrenzwert erreicht worden ist; dies kann erfordern, dass die Hardware-Fehlertoleranz erhöht werden muss, um die Entwurfsanforderungen zu erfüllen.

ANMERKUNG 2 Die Anforderungen zur Hardware-Fehlertoleranz beziehen sich auf die unter den normalen Betriebsbedingungen verwendete Teilsystem-Architektur. Die Anforderungen zur Hardware-Fehlertoleranz können verringert werden, während das sicherheitsbezogene E/E/PE-System im Betrieb repariert wird. Jedoch müssen die Schlüsselp Parameter in Bezug auf jede Verringerung vorher bewertet worden sein (zum Beispiel Zeit bis zur Wiederherstellung im Vergleich zur Wahrscheinlichkeit einer Anforderung). Bestimmte Fehler können ausgeschlossen werden, weil, wenn ein Element eindeutig eine sehr geringe Ausfallwahrscheinlichkeit auf Grund von Eigenschaften besitzt, die durch seinen Entwurf und seine Konstruktion inhärent bedingt sind (zum Beispiel ein mechanisches Aktor-Verbindungssystem), es üblicherweise nicht als notwendig erachtet wird, die Sicherheitsintegrität irgendeiner Sicherheitsfunktion, die dieses Element verwendet, (auf Grund der Hardware-Fehlertoleranz) einzuschränken.

ANMERKUNG 3 Die Wahl des Pfades ist anwendungs- und sektorabhängig und das Folgende sollte berücksichtigt werden, wenn der Pfad ausgewählt wird:

- für einige Sicherheitsfunktionen gibt es nach einem Ausfall keinen sicheren Zustand;
- ein sicherer Zustand einer Funktion könnte eine neue Gefährdung hervorrufen oder eine zusätzliche Ursache für eine bestehende Gefährdung sein;
- Redundanz könnte nicht für alle Funktionen umsetzbar sein;
- Reparatur ist nicht immer möglich oder rasch (z. B. nicht durchführbar innerhalb einer Zeit, die im Vergleich zum Intervall für die Wiederholungsprüfung unbedeutend ist).

ANMERKUNG 4 Besondere Architektur Anforderungen für ICs mit On-Chip-Redundanz sind in Anhang E enthalten.

7.4.4.1.2 Ein Element kann als vom Typ A betrachtet werden, wenn für die Bauteile, die für das Erreichen der Sicherheitsfunktion erforderlich sind:

- a) das Ausfallverhalten aller eingesetzten Bauteile eindeutig definiert ist; und
- b) das Verhalten des Elements unter Fehlerbedingungen vollständig bestimmt werden kann; und
- c) ausreichend verlässliche Ausfalldaten existieren, um zu zeigen, dass die angenommenen Ausfallraten für erkannte und unerkannte gefahrbringende Ausfälle erreicht werden (siehe 7.4.9.3 bis 7.4.9.5).

7.4.4.1.3 Ein Element muss als vom Typ B betrachtet werden, wenn für die Bauteile, die für das Erreichen der Sicherheitsfunktion erforderlich sind:

- a) das Ausfallverhalten von mindestens einem eingesetzten Bauteil nicht eindeutig definiert ist; oder
- b) das Verhalten des Elements unter Fehlerbedingungen nicht vollständig bestimmt werden kann; oder
- c) keine ausreichend zuverlässigen Ausfalldaten vorliegen, um die beanspruchten Ausfallraten für erkannte und unerkannte gefahrbringende Ausfälle zu unterstützen (siehe 7.4.9.3 bis 7.4.9.5).

ANMERKUNG Dies bedeutet, dass falls mindestens ein Bauteil eines Elements selbst die Bedingungen für ein Typ B-Element erfüllt, dieses Element eher als Typ B, wie als Typ A betrachtet werden muss.

7.4.4.2 Pfad 1_H

7.4.4.2.1 Um den maximalen Sicherheits-Integritätslevel zu bestimmen, der für eine Sicherheitsfunktion in Anspruch genommen werden kann, muss das folgende Verfahren befolgt werden:

- 1) Definition der Teilsysteme aus denen das sicherheitsbezogene E/E/PE-System besteht;

- 2) für jedes Teilsystem Bestimmung des Anteils sicherer Ausfälle für alle Elemente im Teilsystem, mit einer Hardware-Fehlertoleranz von null;
- 3) für jedes Element Berücksichtigung des erreichten Anteils sicherer Ausfälle und der Hardware-Fehlertoleranz von null zur Bestimmung des maximalen Sicherheits-Integritätslevels, der aus Spalte 2, Tabelle 2 für Typ A-Elemente und aus Spalte 2, Tabelle 3 für Typ B-Elemente in Anspruch genommen werden kann;
- 4) Anwendung der Methode in 7.4.4.2.3 und 7.4.4.2.4 zur Bestimmung des maximalen Sicherheits-Integritätslevels, der für das Teilsystem in Anspruch genommen werden kann;
- 5) der maximale Sicherheits-Integritätslevel, der für ein sicherheitsbezogenes E/E/PE-System in Anspruch genommen werden kann, muss durch das Teilsystem bestimmt werden, das den niedrigsten Sicherheits-Integritätslevel erreicht hat.

7.4.4.2.2 Zur Anwendung auf Teilsysteme, die Elemente enthalten, die die speziellen, unten detaillierten Anforderungen erfüllen, ist als Alternative zur Anwendung der Anforderungen aus 7.4.4.2.1 (2) bis 7.4.4.2.1 (4) Folgendes anwendbar:

- 1) das Teilsystem enthält mehr als ein Element; und
- 2) die Elemente sind gleichen Typs; und
- 3) alle Elemente haben Anteile sicherer Ausfälle erreicht, die in den gleichen Bereichen liegen (siehe Anmerkung), die in den Tabellen 2 und 3 angegeben sind; dann kann das folgende Verfahren befolgt werden:
 - a) Bestimmung des Anteils sicherer Ausfälle eines Elements;
 - b) Bestimmung der Hardware-Fehlertoleranz des Teilsystems;
 - c) Bestimmung des maximalen Sicherheits-Integritätslevels, der für das Teilsystem in Anspruch genommen werden kann, aus Tabelle 2, wenn die Elemente dem Typ A entsprechen;
 - d) Bestimmung des maximalen Sicherheits-Integritätslevels, der für das Teilsystem in Anspruch genommen werden kann, aus Tabelle 3, wenn die Elemente dem Typ B entsprechen.

ANMERKUNG Der Bereich auf den in (3) oben hingewiesen ist, bezieht sich auf die Tabellen 2 und 3, wo der Anteil sicherer Ausfälle in einen von vier Bereichen klassifiziert ist (d. h. $< 60\%$, $60\% - < 90\%$, $90\% - < 99\%$ und $\geq 99\%$). Alle SFF haben im gleichen Bereich zu liegen (z. B. alle im Bereich $< 90\%$, 90%).

BEISPIEL 1 Um den maximal zulässigen Sicherheits-Integritätslevel zu bestimmen, der durch ein Teilsystem mit einer Hardware-Fehlertoleranz von eins für die festgelegte Sicherheitsfunktion erreicht worden ist, bei dem eine Element-Sicherheitsfunktion durch parallele Elemente ausgeführt wird, kann die folgende Methode angewendet werden, vorausgesetzt das Teilsystem erfüllt die Anforderungen von 7.4.4.2.2. In diesem Beispiel sind alle Elemente vom Typ B und die Anteile sicherer Ausfälle der Elemente liegen im Bereich von $90\% - < 99\%$.

Aus Tabelle 3 ist durch Inaugenscheinnahme ersichtlich, dass für eine Hardware-Fehlertoleranz gleich eins, mit Anteilen sicherer Ausfälle für beide Elemente im Bereich von $90\% - < 99\%$, der maximal zulässige Sicherheits-Integritätslevel für die festgelegte Sicherheitsfunktion SIL3 beträgt.

BEISPIEL 2 Um die erforderliche Hardware-Fehlertoleranz für ein Teilsystem für die festgelegte Sicherheitsfunktion zu bestimmen, bei dem eine Element-Sicherheitsfunktion durch parallele Elemente ausgeführt wird, kann die folgende Methode angewendet werden, vorausgesetzt das Teilsystem erfüllt die Anforderungen von 7.4.4.2.2. In diesem Beispiel sind alle Elemente vom Typ A und die Anteile sicherer Ausfälle der Elemente liegen im Bereich von $60\% - < 90\%$. Der Sicherheits-Integritätslevel der Sicherheitsfunktion ist SIL3.

Aus Tabelle 2 ist durch Inaugenscheinnahme ersichtlich, dass zum Erreichen der Anforderung von SIL3 die erforderliche Hardware-Fehlertoleranz gleich eins sein muss. Dies bedeutet, dass zwei parallele Elemente notwendig sind.

Tabelle 2 – Maximal zulässiger Sicherheits-Integritätslevel für eine Sicherheitsfunktion, die von einem sicherheitsbezogenen Typ A-Element ausgeführt wird

Anteil sicherer Ausfälle eines Elements	Hardware-Fehlertoleranz		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % – < 90 %	SIL2	SIL3	SIL4
90 % – < 99 %	SIL3	SIL4	SIL4
≥ 99 %	SIL3	SIL4	SIL4
ANMERKUNG 1 Diese Tabelle kann auf zwei unterschiedliche Arten angewendet werden: i. Für allgemeine Anwendung auf alle Teilsysteme siehe 7.4.4.2.1. ii. Für Anwendung auf Teilsysteme, die Elemente enthalten, die die speziellen Anforderungen von 7.4.4.2.2 erfüllen. Um zu beanspruchen, dass ein Teilsystem einen speziellen SIL direkt nach dieser Tabelle erfüllt, ist es notwendig alle Anforderungen in 7.4.4.2.2 zu erfüllen. ANMERKUNG 2 Die Anforderungen in 7.4.4.2.3 und 7.4.4.2.4 beruhen auf den in dieser Tabelle und Tabelle 3 festgelegten Daten. ANMERKUNG 3 Siehe Anhang C zu Einzelheiten bezüglich der Berechnung des Anteils sicherer Ausfälle.			

Tabelle 3 – Maximal zulässiger Sicherheits-Integritätslevel für eine Sicherheitsfunktion, die von einem sicherheitsbezogenen Typ B-Element ausgeführt wird

Anteil sicherer Ausfälle eines Elements	Hardware-Fehlertoleranz		
	0	1	2
< 60 %	nicht erlaubt	SIL1	SIL2
60 % - < 90 %	SIL1	SIL2	SIL3
90 % - < 99 %	SIL2	SIL3	SIL4
≥ 99 %	SIL3	SIL4	SIL4
ANMERKUNG 1 Diese Tabelle kann auf zwei unterschiedliche Arten angewendet werden: i. Für allgemeine Anwendung auf alle Teilsysteme siehe 7.4.4.2.1. ii. Für Anwendung auf Teilsysteme, die Elemente enthalten, die die speziellen Anforderungen von 7.4.4.2.2 erfüllen. Um zu beanspruchen, dass ein Teilsystem einen speziellen SIL direkt nach dieser Tabelle erfüllt, ist es notwendig alle Anforderungen in 7.4.4.2.2 zu erfüllen. ANMERKUNG 2 Die Anforderungen in 7.4.4.2.3 und 7.4.4.2.4 beruhen auf den in dieser Tabelle und Tabelle 2 festgelegten Daten. ANMERKUNG 3 Siehe Anhang C zu Einzelheiten bezüglich der Berechnung des Anteils sicherer Ausfälle.			

7.4.4.2.3 In einem sicherheitsbezogenen E/E/PE-Teilsystem, in dem eine Anzahl von Element-Sicherheitsfunktionen durch eine serielle Kombination von Elementen ausgeführt wird (wie zum Beispiel in Bild 5), muss der maximale Sicherheits-Integritätslevel, der für die betrachtete Sicherheitsfunktion beansprucht werden kann, durch das Element bestimmt werden, das den niedrigsten Sicherheits-Integritätslevel erreicht hat für den erreichten Anteil sicherer Ausfälle für eine Hardware-Fehlertoleranz von null.

BEISPIEL (siehe Bild 6) Angenommen wird eine Architektur, in der eine Anzahl von Element-Sicherheitsfunktionen von einem Teilsystem ausgeführt wird, das aus einem einzelnen Kanal mit den Elementen 1, 2 und 3 besteht und die Elemente die Anforderungen der Tabellen 2 und 3 wie folgt erfüllen:

- Element 1 erreicht mit einer Hardware-Fehlertoleranz von null und mit einem bestimmten Anteil sicherer Ausfälle die Anforderungen von SIL1;
- Element 2 erreicht mit einer Hardware-Fehlertoleranz von null und mit einem bestimmten Anteil sicherer Ausfälle die Anforderungen von SIL2;
- Element 3 erreicht mit einer Hardware-Fehlertoleranz von null und mit einem bestimmten Anteil sicherer Ausfälle die Anforderungen von SIL1;
- sowohl Element 1, als auch Element 3, beschränken den maximal in Anspruch nehmenden SIL für die erreichte Hardware-Fehlertoleranz und den Anteil sicherer Ausfälle auf nur SIL1.

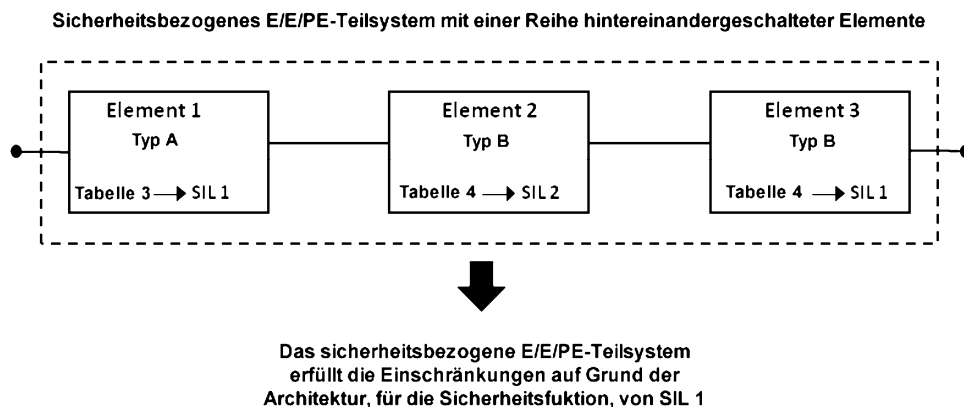


**Bild 5 (siehe 7.4.4.2.3): Beispiel:
Bestimmung des maximalen SIL für eine festgelegte Architektur**

7.4.4.2.4 In einem sicherheitsbezogenen E/E/PE-Teilsystem, in dem eine Element-Sicherheitsfunktion durch eine Anzahl von Kanälen (Kombination von parallelen Elementen) mit einer Hardware-Fehlertoleranz von N ausgeführt wird, muss der maximale Sicherheits-Integritätslevel, der für die betrachtete Sicherheitsfunktion beansprucht werden kann, durch Folgendes bestimmt werden:

- Gruppierung der seriellen Kombination von Elementen für jeden Kanal und nachfolgend Bestimmung des maximalen Sicherheits-Integritätslevels, der für die betrachtete Sicherheitsfunktion für jeden Kanal in Anspruch genommen werden kann (siehe 7.4.4.2.3); und
- Auswahl des Kanals mit dem höchsten Sicherheits-Integritätslevel, der für die betrachtete Sicherheitsfunktion erreicht worden ist und nachfolgend Addition von N Sicherheits-Integritätsleveln zur Bestimmung des maximalen Sicherheits-Integritätslevels für die Gesamtkombination des Teilsystems.

ANMERKUNG 1 N ist die Hardware-Fehlertoleranz der Kombination paralleler Elemente (siehe 7.4.4.1.1).

ANMERKUNG 2 Zur Anwendung dieses Abschnitts siehe nachfolgendes Beispiel.

BEISPIEL Die Zusammenstellung und Analyse dieser Kombinationen kann auf verschiedenen Wegen ausgeführt werden. Um eine der möglichen Vorgehensweisen darzustellen, wird eine Architektur angenommen, in der eine spezielle Sicherheitsfunktion durch zwei Teilssysteme X und Y ausgeführt wird, wobei wie in Bild 6 Teilssystem X aus den Elementen 1, 2, 3 und 4 besteht und Teilssystem Y aus einem einzelnen Element 5 besteht. Die Verwendung paralleler Kanäle in Teilssystem X stellt sicher, dass die Elemente 1 und 2 den von Teilssystem X geforderten Teil der Sicherheitsfunktion unabhängig von den Elementen 3 und 4 ausführen und umgekehrt. Die Sicherheitsfunktion wird ausgeführt:

- im Falle eines Fehlers in entweder Element 1 oder Element 2 (da die Kombination der Elemente 3 und 4 in der Lage ist, den erforderlichen Teil der Sicherheitsfunktion auszuführen); oder

- im Falle eines Fehlers in entweder Element 3 oder Element 4 (da die Kombination der Elemente 1 und 2 in der Lage ist, den erforderlichen Teil der Sicherheitsfunktion auszuführen).

Die Bestimmung des maximalen Sicherheits-Integritätslevels, der für die betrachtete Sicherheitsfunktion beansprucht werden kann, wird in den folgenden Schritten genauer beschrieben.

Für Teilsystem X erfüllt jedes Element im Hinblick auf die festgelegte betrachtete Sicherheitsfunktion die Anforderungen der Tabellen 2 und 3 wie folgt:

- Element 1 erreicht mit einer Hardware-Fehlertoleranz von null und mit einem bestimmten Anteil sicherer Ausfälle die Anforderungen von SIL3;
- Element 2 erreicht mit einer Hardware-Fehlertoleranz von null und mit einem bestimmten Anteil sicherer Ausfälle die Anforderungen von SIL2;
- Element 3 erreicht mit einer Hardware-Fehlertoleranz von null und mit einem bestimmten Anteil sicherer Ausfälle die Anforderungen von SIL2;
- Element 4 erreicht mit einer Hardware-Fehlertoleranz von null und mit einem bestimmten Anteil sicherer Ausfälle die Anforderungen von SIL1.

Für Teilsystem X werden die Elemente wie folgt kombiniert, um für die betrachtete Sicherheitsfunktion einen maximalen Sicherheits-Integritätslevel der Hardware zu ergeben:

- a) Kombination der Elemente 1 und 2: Die Hardware-Fehlertoleranz und der Anteil sicherer Ausfälle, der durch die Kombination der Elemente 1 und 2 (jedes entspricht jeweils einzeln den Anforderungen von SIL3 beziehungsweise SIL2) erreicht wird, entspricht den Anforderungen des SIL2 (bestimmt durch Element 2, siehe 7.4.4.2.3);
- b) Kombination der Elemente 3 und 4: Die Hardware-Fehlertoleranz und der Anteil sicherer Ausfälle, der durch die Kombination der Elemente 3 und 4 (jedes entspricht jeweils einzeln den Anforderungen von SIL2 beziehungsweise SIL1) erreicht wird, entspricht den Anforderungen des SIL1 (bestimmt durch Element 4, siehe 7.4.4.2.3);
- c) Weitere Kombination der Kombination der Elemente 1 und 2 mit der Kombination der Elemente 3 und 4: Der maximale Sicherheits-Integritätslevel, der für die betrachtete Sicherheitsfunktion in Anspruch genommen werden kann, wird durch Auswahl des Kanals mit dem höchsten erreichten Sicherheits-Integritätslevel bestimmt und nachfolgend Addition von N Sicherheits-Integritätsleveln zur Bestimmung des maximalen Sicherheits-Integritätslevels für die Gesamtkombination der Elemente. In diesem Beispiel besteht das Teilsystem aus zwei parallelen Kanälen mit einer Hardware-Fehlertoleranz von eins. Der Kanal mit dem höchsten Sicherheits-Integritätslevel für die betrachtete Sicherheitsfunktion ist derjenige, der die Elemente 1 und 2 enthält, die die Anforderungen für SIL2 erfüllen. Daher beträgt für das Teilsystem der maximale Sicherheits-Integritätslevel $(\text{SIL } 2 + 1) = \text{SIL3}$ für eine Hardware-Fehlertoleranz von eins (siehe 7.4.4.2.4).

Für Teilsystem Y erreicht Element 5 mit einer Hardware-Fehlertoleranz von null und mit einem bestimmten Anteil sicherer Ausfälle die Anforderungen von SIL2.

Für das vollständige sicherheitsbezogene E/E/PE-System (bestehend aus den Teilsystemen X und Y, die für die betrachtete Sicherheitsfunktion die Anforderungen von SIL2 beziehungsweise SIL3 erreicht haben) wird der maximale Sicherheits-Integritätslevel, der für ein sicherheitsbezogenes E/E/PE-System in Anspruch genommen werden kann, durch das Teilsystem bestimmt, das den niedrigsten Sicherheits-Integritätslevel erreicht hat (7.4.4.2.1 (5)). Daher beträgt für dieses Beispiel der maximale Sicherheits-Integritätslevel, der für das sicherheitsbezogene E/E/PE-System für die betrachtete Sicherheitsfunktion in Anspruch genommen werden kann, SIL2.

7.4.4.2.5 Bei der Abschätzung des Anteils sicherer Ausfälle eines Elements, das zur Verwendung in einem Teilsystem mit einer Hardware-Fehlertoleranz von null vorgesehen ist und das eine Sicherheitsfunktion oder einen Teil einer Sicherheitsfunktion ausführt, die in der Betriebsart mit hoher Anforderungsrate oder bei kontinuierlicher Anforderung betrieben wird, darf die Diagnose nur angerechnet werden, wenn:

- die Summe von Diagnose-Testintervall und die Zeit, um die festgelegte Reaktion durchzuführen, um einen sicheren Zustand zu erreichen oder aufrechtzuerhalten, kleiner ist, als die Prozess-Sicherheitszeit; oder
- bei Betrieb in der Betriebsart mit hoher Anforderungsrate, das Verhältnis der Diagnose-Testrate zur Anforderungsrate 100 gleicht oder übertrifft.

7.4.4.2.6 Bei der Abschätzung des Anteils sicherer Ausfälle eines Elements, das:

- eine Hardware-Fehlertoleranz größer null besitzt und das eine Sicherheitsfunktion oder einen Teil einer Sicherheitsfunktion ausführt, die in der Betriebsart mit hoher Anforderungsrate oder bei kontinuierlicher Anforderung betrieben wird, oder
- eine Sicherheitsfunktion oder einen Teil einer Sicherheitsfunktion in der Betriebsart mit niedriger Anforderungsrate ausführt,

darf die Diagnose nur angerechnet werden, wenn die Summe von Diagnose-Testintervall und die Zeit zur Ausführung der Reparatur eines erkannten Ausfalls geringer ist, als die in der Berechnung zur Ermittlung der erreichten Sicherheitsintegrität für diese Sicherheitsfunktion verwendete MTTR.

ANMERKUNG 1 Die Elemente 1 und 2 führen den von Teilsystem X geforderten Teil der Sicherheitsfunktion unabhängig von den Elementen 3 und 4 aus und umgekehrt.

ANMERKUNG 2 Die Teilsysteme, welche die Sicherheitsfunktion ausführen, sind über das gesamte sicherheitsbezogene E/E/PE-System verteilt und reichen von den Sensoren bis zu den Aktoren.

**Bild 6 – Beispiel (siehe 7.4.4.2.4):
Bestimmung des maximalen SIL für eine festgelegte Architektur**

7.4.4.3 Pfad 2_H

7.4.4.3.1 Die minimale Hardware-Fehlertoleranz für jedes Teilsystem eines sicherheitsbezogenen E/E/PE-Systems, das eine Sicherheitsfunktion eines festgelegten Sicherheits-Integritätslevel ausführt, muss wie folgt sein:

- eine Hardware-Fehlertoleranz von 2 für eine festgelegte Sicherheitsfunktion von SIL4, außer die Bedingungen des Abschnitts 7.4.4.3.2 treffen zu;
- eine Hardware-Fehlertoleranz von 1 für eine festgelegte Sicherheitsfunktion von SIL3, außer die Bedingungen des Abschnitts 7.4.4.3.2 treffen zu;
- eine Hardware-Fehlertoleranz von 0 für eine festgelegte Sicherheitsfunktion von SIL1 oder SIL2.

7.4.4.3.2 Nur für Typ A-Elemente kann eine sichere alternative Architektur mit reduzierter HFT ausgeführt werden, wenn ermittelt wird, dass durch die Umsetzung der in 7.4.4.3.1 festgelegten Anforderungen zur HFT für eine Sicherheitsfunktion von SIL3 oder SIL4 die geforderte HFT zusätzliche Ausfälle einführen würde und die Umsetzung zu einer Abnahme der Gesamtsicherheit der EUC führen würde. In einem solchen Fall muss dies begründet und dokumentiert werden. Die Begründung muss Nachweise liefern, dass:

- a) Übereinstimmung mit den in 7.4.4.2.1 festgelegten Anforderungen zur HFT zusätzliche Ausfälle einführen würde und die Übereinstimmung zu einer Abnahme der Gesamtsicherheit der EUC führen würde; und
- b) wenn die HFT auf null verringert wird, die in dem Element, das die Sicherheitsfunktion ausführt, identifizierten Ausfallarten ausgeschlossen werden können, da die Rate(n) gefährbringender Ausfälle der zugehörigen identifizierten Fehlerart(n) sehr gering im Vergleich zum Ausfallgrenzwert der betrachteten Sicherheitsfunktion ist(sind) (siehe 7.4.1.1 (c)).

ANMERKUNG Fehlertoleranz ist die bevorzugte Lösung um das erforderliche Vertrauen zu erreichen, dass eine robuste Architektur erreicht worden ist. Wenn Abschnitt 7.4.4.3.2 angewendet wird, ist der Zweck der Begründung aufzuzeigen, dass die vorgeschlagene alternative Architektur eine gleichwertige oder bessere Lösung ergibt. Dies kann vom technischen Umfeld und/oder der Anwendung abhängen: Back-up (z. B. analytische Redundanz, Ersatz eines ausgefallenen Sensorausgangs durch physikalische Berechnung von Ergebnissen von anderen Sensorausgängen), Verwendung von Artikeln der gleichen Technologie mit höherer Zuverlässigkeit (wenn vorhanden), Wechsel zu einer zuverlässigeren Technologie, Verminderung des Einflusses von Ausfällen infolge gemeinsamer Ursache durch Verwendung diversifizierter Technologie, Erhöhung der Konstruktionsgrenzen, Einschränkung der Umgebungsbedingungen (z. B. für elektronische Bauteile), Verminderung der Unsicherheit der Zuverlässigkeitsdaten durch Sammlung von mehr Rückmeldungen aus dem Feld oder Expertenmeinungen usw.

7.4.4.3.3 Wenn Pfad 2_H gewählt wird, müssen die bei der Quantifizierung der Auswirkung von zufälligen Hardwareausfällen (siehe 7.4.5) verwendeten Zuverlässigkeitsdaten:

- a) auf Rückmeldungen aus dem Feld basieren, die von in Verwendung befindlichen Einrichtungen stammen. Die verwendeten Daten müssen auf Daten basieren, die in Übereinstimmung mit veröffentlichten Normen (z. B. IEC 60300-3-2: "Zuverlässigkeitsmanagement - Teil 3-2: Anwendungsleitfaden - Erfassung von Zuverlässigkeitsdaten im Betrieb" oder ISO 14224: "Erdöl-, petrochemische und Erdgasindustrie - Sammlung und Austausch von Zuverlässigkeits- und Wartungsdaten für Ausrüstungen") gesammelt sind; und
- b) nach dem Umfang von Rückmeldungen aus dem Feld und/oder Expertenmeinungen und/oder spezielle Tests bewertet werden, um das Mittel und den Unsicherheitsfaktor (z. B. das 90 %-Konfidenzintervall oder die Wahrscheinlichkeitsverteilung) jedes in den Berechnungen verwendeten Zuverlässigkeitsparameters (z. B. Ausfallrate) abzuschätzen.

ANMERKUNG 1 Endanwender sind dazu aufgerufen relevante Bauteilzuverlässigkeitsdatensammlungen, wie in veröffentlichten Normen beschrieben, zu organisieren.

ANMERKUNG 2 Das 90 %-Konfidenzintervall einer Ausfallrate λ ist das Intervall $[\lambda_{5\%}, \lambda_{95\%}]$, in dem ihr tatsächlicher Wert eine Wahrscheinlichkeit der Zugehörigkeit von 90 % hat. λ hat eine Wahrscheinlichkeit von 5 % besser als $\lambda_{5\%}$ zu sein

und schlechter als $\lambda_{95\%}$. Auf einer rein statistischen Basis, kann das Mittel der Ausfallrate durch Verwendung der „Maximum-Likelihood-Schätzung“ abgeschätzt werden und die Konfidenzgrenzen ($\lambda_{95\%}$, $\lambda_{95\%}$) können durch Verwendung der χ^2 Funktion berechnet werden. Die Genauigkeit hängt von der kumulierten Beobachtungszeit und der Anzahl der beobachteten Ausfälle ab. Um statistische Beobachtungen, Expertenmeinungen und spezielle Tests zu berücksichtigen, kann der Bayes'sche Ansatz verwendet werden. Dieser kann verwendet werden, um relevante Wahrscheinlichkeitsverteilungsfunktionen für die weitere Verwendung in einer Monte-Carlo-Simulation anzupassen.

Wenn Pfad 2_H gewählt wird, müssen die Unsicherheiten der Zuverlässigkeitsdaten berücksichtigt werden, um den Ausfallgrenzwert (d. h. PFD_{avg} oder PFH) zu berechnen und das System muss verbessert werden, bis eine Konfidenz größer 90 % vorliegt, dass der Ausfallgrenzwert erreicht wird.

ANMERKUNG 3 Wenn Unsicherheiten der Zuverlässigkeitsdaten berücksichtigt werden, verhalten sich PFD_{avg} oder PFH als Zufallsvariablen. Daher wird aus den obigen Anforderungen wenn SIL_i als Ziel vorgesehen ist:

- Wahrscheinlichkeit $\{PFD_{avg} < 10^{-i}\} \geq 90\%$ in der Betriebsart mit niedriger Anforderungsrate;
- Wahrscheinlichkeit $\{PFH < 10^{-(i+4)}\} \geq 90\%$ in der Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung.

7.4.4.3.4 Alle im Pfad 2_H verwendeten Elemente des Typs B müssen mindestens einen Diagnosedeckungsgrad nicht kleiner 60 % besitzen.

7.4.5 Anforderungen zur Quantifizierung der Auswirkung von zufälligen Hardwareausfällen

ANMERKUNG IEC 61508-6, A.2, gibt einen Überblick über die notwendigen Schritte zum Erreichen der erforderlichen Sicherheitsintegrität der Hardware und zeigt wie dieser Unterabschnitt zu anderen Anforderungen dieser Norm in Bezug steht.

7.4.5.1 Für jede Sicherheitsfunktion muss die erreichte Sicherheitsintegrität des sicherheitsbezogenen E/E/PE-Systems infolge zufälliger Hardwareausfälle (einschließlich Soft-Errors) und zufälliger Ausfälle von Datenkommunikationsprozessen in Übereinstimmung mit 7.4.5.2 und 7.4.11 abgeschätzt werden und muss gleich oder kleiner dem in der Spezifikation der Sicherheitsanforderungen des E/E/PE-Systems (siehe IEC 61508-1, 7.10) festgelegten Ausfallgrenzwert sein.

ANMERKUNG Um zu zeigen, dass dieses erreicht worden ist, ist es notwendig, eine Zuverlässigkeitsvorhersage für die relevante Sicherheitsfunktion unter Verwendung eines angemessenen Verfahrens (siehe 7.4.5.2) zu treffen und die Ergebnisse mit dem Ausfallgrenzwert der relevanten Sicherheitsfunktion (siehe IEC 61508-1) zu vergleichen.

7.4.5.2 Die nach 7.4.5.1 erforderliche Abschätzung des erreichten Ausfallmaßes jeder Sicherheitsfunktion muss Folgendes berücksichtigen:

- a) die Architektur des sicherheitsbezogenen E/E/PE-Systems, in Form seiner Teilsysteme, wie sie in Bezug zu jeder betrachteten Sicherheitsfunktion steht;

ANMERKUNG 1 Dieses schließt die Entscheidung ein, welche Ausfallarten der Elemente der Teilsysteme in einer seriellen Konfiguration vorhanden sind (d. h. jeder Ausfall führt zu einem Ausfall der Ausführung der relevanten Sicherheitsfunktion) und welche in einer parallelen Konfiguration vorhanden sind (d. h. es sind gemeinsam auftretende Ausfälle notwendig, damit die relevante Sicherheitsfunktion ausfällt).

- b) die Architektur jedes Teilsystems des sicherheitsbezogenen E/E/PE-Systems, in Form seiner Elemente, wie sie in Bezug zu jeder betrachteten Sicherheitsfunktion steht;
- c) die geschätzte Ausfallrate jedes Teilsystems und seiner Elemente in allen Modi, die zu einem gefahrbringenden Ausfall des sicherheitsbezogenen E/E/PE-Systems führen, jedoch durch Diagnosetests erkannt werden (siehe 7.4.9.4 bis 7.4.9.5). Es sollte unter Berücksichtigung der Quellen der Daten und ihrer Genauigkeit oder Toleranz eine Rechtfertigung für die Ausfallraten angegeben werden. Dies kann Berücksichtigung und den Vergleich von Daten aus einer Anzahl von Quellen und die Auswahl von Ausfallraten von Systemen, die dem betrachteten am meisten ähneln, einschließen;
- d) die Anfälligkeit des sicherheitsbezogenen E/E/PE-Systems und seiner Teilsysteme für Ausfälle infolge gemeinsamer Ursache (siehe Anmerkungen 2 und 13). Es muss eine Begründung für die gemachten Annahmen vorliegen;

ANMERKUNG 2 Wenn Ausfälle infolge gemeinsamer Ursache zwischen den sicherheitsbezogenen E/E/PE-Systemen und den Ursachen für Anforderungen oder anderen Schutzschichten identifiziert werden, ist eine Bestätigung erforderlich, dass dies berücksichtigt worden ist, als der Sicherheits-Integritätslevel und die Anforderungen zum Ausfallgrenzwert festgelegt worden sind. Zu Methoden der Bestimmung der Faktoren gemeinsamer Ursachen siehe IEC 61508-6, Anhang D.

- e) den Diagnosedeckungsgrad der Diagnosetests (bestimmt gemäß Anhang C), das zugehörige Diagnose-Testintervall und die Rate gefährlicher unerkannter Ausfälle der Diagnose jedes Teilsystems infolge zufälliger Hardwareausfälle. Wo relevant dürfen nur diejenigen Diagnosetests berücksichtigt werden, welche die Anforderungen von 7.4.5.3 erfüllen. Das Diagnose-Testintervall und die nachfolgende Zeit zur Reparatur ergeben zusammen die mittlere Zeit bis zur Wiederherstellung, die im Zuverlässigkeitsmodell betrachtet werden muss. Für sicherheitsbezogene E/E/PE-Systeme, die in der Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung betrieben werden und wo jeder gefahrbringende Ausfall eines Kanals in einem gefahrbringenden Ausfall des sicherheitsbezogenen E/E/PE-Systems mündet, ist es notwendig, das Diagnose-Testintervall zusätzlich zur mittleren Zeit bis zur Wiederherstellung im Zuverlässigkeitsmodell zu berücksichtigen, falls es nicht mindestens eine Größenordnung kleiner als die Zeit zwischen den erwarteten Anforderungen ist (siehe 7.4.5.3);

ANMERKUNG 3 Bei der Festlegung des Diagnose-Testintervalls ist es notwendig, die Zeitabstände aller Tests, die zum Diagnosedeckungsgrad beitragen, zu berücksichtigen.

- f) die Intervalle, innerhalb deren Wiederholungsprüfungen ausführt werden müssen, um gefahrbringende Fehler zu erkennen;
- g) ob wahrscheinlich ist, dass die Wiederholungsprüfung 100 % wirksam ist;

ANMERKUNG 4 Eine mangelhafte Wiederholungsprüfung führt zu einer Sicherheitsfunktion, die nicht in einen „Wie-Neu“-Zustand zurückgesetzt wird und daher zu einem Anstieg der Ausfallwahrscheinlichkeit. Es sollte eine Rechtfertigung für die gemachten Annahmen gegeben werden, insbesondere sollten die verlängerungsfähigen Zeiträume der Elemente oder die Auswirkung auf die Risikominderung über die Lebensdauer der Sicherheitsfunktion einbezogen werden. Es wird notwendig sein, die Zeitdauer der Prüfung zu betrachten, wenn der Gegenstand außer Betrieb geprüft wird, während die Prüfung ausgeführt wird.

- h) die Reparaturzeiten für erkannte Ausfälle;

ANMERKUNG 5 Die Reparaturzeit bildet einen Teil der mittleren Zeit bis zur Wiederherstellung (siehe IEC 61508-6, Anhang B für ein Beispiel, wie die mittlere Zeit bis zur Wiederherstellung in der Berechnung der Ausfallwahrscheinlichkeit verwendet werden kann). Die Reparatur kann nur als unmittelbar betrachtet werden, wenn die EUC während der Reparatur abgeschaltet ist oder sich in einem sicheren Zustand befindet. In Fällen, in denen eine Reparatur nicht durchgeführt werden kann, während die EUC abgeschaltet ist und sich in einem sicheren Zustand befindet, ist es besonders wichtig, dass die Dauer, in der keine Reparatur durchgeführt werden kann, vollständig berücksichtigt wird. Besonders wichtig ist dies, wenn diese Zeitspanne relativ groß ist. Alle in Bezug auf Reparaturen relevanten Faktoren sollten in Betracht gezogen werden.

- i) die Auswirkungen zufälligen menschlichen Irrtums, wenn das Eingreifen einer Person für das Erreichen der Sicherheitsfunktion erforderlich ist;

ANMERKUNG 6 Der zufällige Charakter menschlichen Irrtums sollte in Betracht gezogen werden in Fällen, in denen eine Person vor einem unsicheren Zustand gewarnt wird und eingreifen muss, wo nicht gezeigt werden kann, dass Untätigkeit des Bedieners durch Mechanismen oder Verfahren daran gehindert ist, die Sicherheitsfunktion zu beeinflussen. In diesen Fällen sollte der zufällige Charakter menschlichen Irrtums in die Gesamtberechnung einbezogen werden.

ANMERKUNG 7 IEC 61508-6, Anhang B beschreibt einen vereinfachten Lösungsansatz, der zur Abschätzung der Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung einer Sicherheitsfunktion infolge zufälliger Hardwareausfälle verwendet werden kann, um zu bestimmen, dass eine Architektur den erforderlichen Ausfallgrenzwert erreicht.

ANMERKUNG 8 IEC 61508-6, A.2, gibt einen Überblick über die notwendigen Schritte zum Erreichen der erforderlichen Sicherheitsintegrität der Hardware und zeigt wie dieser Unterabschnitt zu anderen Anforderungen dieser Norm in Bezug steht.

ANMERKUNG 9 Es ist notwendig für jede Sicherheitsfunktion die Zuverlässigkeit der sicherheitsbezogenen E/E/PE-Systeme separat zu quantifizieren, weil unterschiedliche Ausfallarten der Elemente vorkommen werden und sich ebenso die Architektur der sicherheitsbezogenen E/E/PE-Systeme (im Sinne von Redundanz) ändern kann.

ANMERKUNG 10 Ausfälle infolge gemeinsamer Ursachen können von anderen Effekten als tatsächlichen Ausfällen von Hardwareelementen herrühren (z. B. elektromagnetischer Beeinflussung, Dekodierfehlern usw.). Solche Ausfälle werden im Sinne dieser Norm jedoch im Rahmen der Quantifizierung der Auswirkungen zufälliger Hardwareausfälle betrachtet. Die Staffelung der Testung von Elementen vermindert die Wahrscheinlichkeit eines Ausfalls infolge gemeinsamer Ursache.

- j) die Tatsache, dass zahlreiche Modellbildungs-Methoden zur Verfügung stehen und dass die Auswahl der am besten passenden Methode Sache desjenigen ist, der die Analyse durchführt und von den Umständen abhängen wird. Verfügbare Methoden schließen Ursache-Wirkungsanalyse (IEC 61508-7, B.6.6.2), Fehlerbaum-Analyse (IEC 61508-7, B.6.6.5), Markov-Modelle (IEC 61508-6, Anhang B und IEC 61508-7, B.6.6.6), Zuverlässigkeits-Blockdiagramme (IEC 61508-6, Anhang B und IEC 61508-7, B.6.6.6) und Petri-Netze (IEC 61508-6, Anhang B und IEC 61508-7, B.2.3.3) ein.

7.4.5.3 Bei der Quantifizierung der Auswirkung von zufälligen Hardwareausfällen eines Teilsystems mit einer Fehlertoleranz von null, dass eine Sicherheitsfunktion oder einen Teil einer Sicherheitsfunktion ausführt, die in der Betriebsart mit hoher Anforderungsrate oder bei kontinuierlicher Anforderung betrieben wird, darf die Diagnose nur angerechnet werden, wenn:

- die Summe von Diagnose-Testintervall und die Zeit zur Durchführung der festgelegten Reaktion, um einen sicheren Zustand zu erreichen oder aufrechtzuerhalten, kleiner ist, als die Prozess-Sicherheitszeit; oder
- in der Betriebsart mit hoher Anforderungsrate, das Verhältnis der Diagnose-Testrate zur Anforderungsrate 100 gleicht oder übertrifft.

7.4.5.4 Das Diagnose-Testintervall jedes Teilsystems, das:

- eine Fehlertoleranz größer null besitzt und das eine Sicherheitsfunktion oder einen Teil einer Sicherheitsfunktion ausführt, die in der Betriebsart mit hoher Anforderungsrate oder bei kontinuierlicher Anforderung betrieben wird; oder
- eine Sicherheitsfunktion oder einen Teil einer Sicherheitsfunktion in der Betriebsart mit niedriger Anforderungsrate ausführt;

muss so gewählt sein, dass die Summe von Diagnose-Testintervall und die Zeit zur Ausführung der Reparatur eines erkannten Ausfalls geringer ist, als die in der Berechnung zur Ermittlung der erreichten Sicherheitsintegrität für diese Sicherheitsfunktion verwendete MTTR.

7.4.5.5 Wenn für einen bestimmten Entwurf die Anforderung zur Sicherheitsintegrität für die betreffende Sicherheitsfunktion nicht erreicht wird, muss Folgendes durchgeführt werden:

- a) Bestimmung der kritischen Elemente, Teilsysteme und/oder Parameter;
- b) Bewertung der Wirkung möglicher Verbesserungsmaßnahmen für kritische Elemente, Teilsysteme oder Parameter (zum Beispiel, zuverlässigere Bauteile, zusätzlicher Schutz gegen Ausfälle infolge gemeinsamer Ursache, erhöhter Diagnosedeckungsgrad, erweiterte Redundanz, Reduzierung des Intervalls für die Wiederholungsprüfung, gestaffelte Tests usw.);
- c) Auswahl und Durchführung der anwendbaren Verbesserungen;
- d) Wiederholung der notwendigen Schritte, um die neue Wahrscheinlichkeit eines zufälligen Hardwareausfalls zu bestimmen.

7.4.6 Anforderungen zur Vermeidung von systematischen Fehlern

ANMERKUNG Siehe 7.4.2.2 c) zu Einzelheiten wann die Anforderungen dieses Unterabschnitts gelten.

7.4.6.1 Es muss eine angemessene Gruppe von Verfahren und Maßnahmen verwendet werden, die entwickelt sind, um die Entstehung von Fehlern während des Entwurfs und der Entwicklung der Hardware

und der Software des sicherheitsbezogenen E/E/PE-Systems zu verhindern (siehe Tabelle B.2 und IEC 61508-3).

ANMERKUNG Diese Norm enthält keine besonderen Anforderungen in Bezug auf die Vermeidung systematischer Fehler während des Entwurfs von serienmäßig hergestellten elektronischen integrierten Schaltkreisen, wie zum Beispiel Standard-Mikroprozessoren. Dies ist darin begründet, dass die Wahrscheinlichkeit von Fehlern in solchen Geräten durch strenge Entwicklungsverfahren, strenge Tests und umfassende Einsatzerfahrung mit aussagekräftigen Rückmeldungen durch Anwender auf ein Minimum herabgesetzt ist. Für elektronische integrierte Schaltkreise, für die eine solche Grundlage nicht zu rechtfertigen ist (zum Beispiel neue Bauteile oder ASICs), gelten bei Verwendung in einem sicherheitsbezogenen E/E/PE-System die Anforderungen für ASICs (siehe 7.4.6.7 und informativer Anhang F). In Zweifelsfällen (über umfassende Einsatzerfahrung mit aussagekräftigen Rückmeldungen durch Anwender) sollten die Anforderungen für „Felderfahrung“ aus Tabelle B.6 mit einer Wirksamkeit von „niedrig“ für SIL1 und SIL2, einer Wirksamkeit von „mittel“ für SIL3 und einer Wirksamkeit von „hoch“ für SIL4 berücksichtigt werden.

7.4.6.2 In Übereinstimmung mit dem erforderlichen Sicherheits-Integritätslevel muss die gewählte Entwurfsmethode Merkmale besitzen, die Folgendes unterstützen:

- a) Transparenz, Modularität und andere Merkmale, welche die Komplexität beeinflussen,
- b) klare und genaue Beschreibung von:
 - Funktionalität;
 - Schnittstellen der Teilsysteme und Elemente;
 - Reihenfolge und zeitlichem Bezug der Informationen;
 - Parallelbetrieb und Synchronisation;
- c) klare und genaue Dokumentation und Kommunikation von Informationen;
- d) Verifikation und Validierung.

7.4.6.3 Während des Entwurfsstadiums müssen Anforderungen zur Instandhaltung formalisiert werden, um sicherzustellen, dass die Anforderungen zur Sicherheitsintegrität der sicherheitsbezogenen E/E/PE-Systeme weiterhin erfüllt werden.

7.4.6.4 Wo anwendbar, müssen automatische Testwerkzeuge und integrierte Entwicklungswerkzeuge verwendet werden.

7.4.6.5 Während des Entwurfs müssen Integrationstests des E/E/PE-Systems geplant werden. Die Dokumentation der Planung der Tests muss beinhalten:

- a) die Arten der Tests, die durchzuführen sind und die zu befolgenden Verfahren;
- b) die Testumgebung, Werkzeuge, Konfiguration und Programme;
- c) die Kriterien für bestanden/nicht bestanden.

7.4.6.6 Während des Entwurfs müssen diejenigen Tätigkeiten, die auf Entwicklerseite durchgeführt werden können, von jenen unterschieden werden, die Zugang auf Anwenderseite erfordern.

7.4.6.7 Es muss eine angemessene Gruppe von Verfahren und Maßnahmen verwendet werden, die unentbehrlich zur Verhinderung der Entstehung von Fehlern während des Entwurfs und der Entwicklung von ASICs sind. Verfahren und Maßnahmen, die das Erreichen relevanter Eigenschaften unterstützen, sind in Anhang F angegeben. Der zugehörige ASIC-Entwicklungslebenszyklus ist in Bild 3 gezeigt.

7.4.7 Anforderungen zur Beherrschung systematischer Fehler

ANMERKUNG Siehe 7.4.2.2. c) für Einzelheiten unter welchen Bedingungen die Anforderungen dieses Abschnitts zutreffen.

7.4.7.1 Zur Beherrschung systematischer Fehler muss der Entwurf des E/E/PE-Systems Entwurfsmerkmale besitzen, um die sicherheitsbezogenen E/E/PE-Systeme gegen Folgendes tolerant zu machen:

- a) alle verbleibenden Entwurfsfehler in der Hardware, es sei denn, die Möglichkeit von Hardware-Entwurfsfehlern kann ausgeschlossen werden (siehe Tabelle A.15);
- b) umgebungsbedingte Beanspruchungen, einschließlich elektromagnetischer Störungen (siehe Tabelle A.16);
- c) Irrtümer, die vom Bediener der EUC gemacht werden (siehe Tabelle A.17);
- d) alle verbleibenden Entwurfsfehler in der Software (siehe 7.4.3 der IEC 61508-3 und zugehörige Tabelle);
- e) Fehler und andere Effekte, die von irgendeinem Datenkommunikationsprozess herrühren (siehe 7.4.11).

7.4.7.2 Während der Entwurfs- und der Entwicklungstätigkeiten müssen Instandhaltbarkeit und Testbarkeit berücksichtigt werden, um die Verwirklichung dieser Eigenschaften in den endgültigen sicherheitsbezogenen E/E/PE-Systemen zu erleichtern.

7.4.7.3 Der Entwurf der sicherheitsbezogenen E/E/PE-Systeme muss menschliche Fähigkeiten und Einschränkungen berücksichtigen und muss für die notwendigen Handlungen des Bedienungs- und Instandhaltungspersonals geeignet sein. Solche Entwurfsanforderungen müssen ergonomischen Erfahrungsgrundsätzen folgen und auf den wahrscheinlichen Ausbildungs- und Kenntnisstand der Bediener Rücksicht nehmen, zum Beispiel bei in großen Stückzahlen produzierten sicherheitsbezogenen E/E/PE-Systemen, wobei der Bediener ein Teil der breiten Öffentlichkeit ist.

ANMERKUNG 1 Es sollte Entwurfsziel sein, dass vorhersehbare kritische Fehlbedienungen des Bedieners oder des Instandhaltungspersonals soweit wie möglich durch den Entwurf verhindert oder beseitigt werden, oder dass die Aktion eine zweite Bestätigung vor der Ausführung erfordert.

ANMERKUNG 2 Einige Fehlbedienungen des Bedieners oder des Instandhaltungspersonals können nicht durch die sicherheitsbezogenen E/E/PE-Systeme ausgeglichen werden, zum Beispiel, wenn sie außer durch direkte Inspektion nicht erkennbar sind oder realistischerweise nicht aufgedeckt werden können, so wie es zum Beispiel bei einigen mechanischen Ausfällen in der EUC möglich ist.

7.4.8 Anforderungen zum Systemverhalten bei Erkennung eines Fehlers

ANMERKUNG Die Anforderungen dieses Unterabschnitts treffen für spezifizierte Sicherheitsfunktionen zu, die durch ein einzelnes sicherheitsbezogenes E/E/PE-System ausgeführt werden, wo die Gesamt-Sicherheitsfunktion nicht zu anderen risikomindernden Maßnahmen zugeordnet worden ist.

7.4.8.1 Die Erkennung eines gefahrbringenden Fehlers (durch Diagnosetests, Wiederholungsprüfungen oder durch irgendwelche anderen Mittel) in einem Teilsystem, das eine Hardware-Fehlertoleranz von mehr als null besitzt, muss entweder

- a) zu einer festgelegten Reaktion führen, um einen sicheren Zustand zu erreichen oder aufrechtzuerhalten (siehe Anmerkung); oder
- b) zur Isolation des fehlerhaften Bestandteils des Teilsystems führen, um einen weiterhin sicheren Betrieb der EUC zu ermöglichen, während der fehlerhafte Bestandteil repariert wird. Wenn die Reparatur nicht innerhalb der mittleren Zeit bis zur Wiederherstellung (MTTR), die in der Berechnung der Wahrscheinlichkeit eines zufälligen Hardwareausfalls (siehe 7.4.5.2) angenommen ist, abgeschlossen wird, muss eine festgelegte Reaktion ausgeführt werden, um einen sicheren Zustand zu erreichen oder aufrechtzuerhalten (siehe Anmerkung).

ANMERKUNG Die festgelegte Reaktion, die erforderlich ist, um einen sicheren Zustand zu erreichen oder aufrechtzuerhalten, wird in den Sicherheitsanforderungen des E/E/PE-Systems festgelegt (siehe IEC 61508-1, 7.10). Sie kann zum Beispiel aus der sicheren Abschaltung der EUC oder des Teils der EUC bestehen, der für die funktionale Sicherheit auf dem fehlerhaften Teilsystem beruht.

7.4.8.2 Die Erkennung eines gefahrbringenden Fehlers (durch Diagnosetests, Wiederholungsprüfungen oder durch irgendwelche anderen Mittel) in einem Teilsystem, das eine Hardware-Fehlertoleranz von null besitzt muss in dem Fall, in dem das Teilsystem nur Sicherheitsfunktionen in der Betriebsart mit niedriger Anforderungsrate ausführt, entweder

- a) zu einer festgelegten Reaktion führen, um einen sicheren Zustand zu erreichen oder aufrechtzuerhalten; oder
- b) zur Reparatur des fehlerhaften Teilsystems innerhalb der mittleren Zeitspanne bis zur Wiederherstellung (MTTR), die in der Berechnung der Wahrscheinlichkeit eines zufälligen Hardwareausfalls (siehe 7.4.5.2) angenommen ist, führen. Während dieser Zeit muss der Fortbestand der Sicherheit der EUC durch zusätzliche Maßnahmen und Einschränkungen sichergestellt werden. Die Sicherheitsintegrität, die sich aus diesen Maßnahmen und Einschränkungen ergibt, muss mindestens gleichwertig zu der Sicherheitsintegrität sein, die sich durch das sicherheitsbezogene E/E/PE-System in der Abwesenheit von Fehlern ergibt. Die zusätzlichen Maßnahmen und Einschränkungen müssen in den Betriebs- und Instandhaltungsverfahren des Systems (siehe 7.6) festgelegt werden.

ANMERKUNG Die festgelegte Reaktion, die erforderlich ist, um einen sicheren Zustand zu erreichen oder aufrechtzuerhalten, wird in den Sicherheitsanforderungen des E/E/PE-Systems festgelegt (siehe 7.2.3.1). Sie kann zum Beispiel aus der sicheren Abschaltung der EUC oder des Teils der EUC bestehen, der für die funktionale Sicherheit auf dem fehlerhaften Teilsystem beruht.

7.4.8.3 Die Erkennung eines gefahrbringenden Fehlers (durch Diagnosetests, Wiederholungsprüfungen oder durch irgendwelche anderen Mittel) in einem Teilsystem, das eine Hardware-Fehlertoleranz von null besitzt, muss in dem Fall eines Teilsystems, das irgendeine Sicherheitsfunktion(en) in der Betriebsart mit hoher Anforderungsrate oder mit kontinuierlicher Anforderung ausführt, zu einer festgelegten Reaktion führen, um einen sicheren Zustand zu erreichen oder aufrechtzuerhalten (siehe Anmerkung).

ANMERKUNG Die festgelegte Reaktion, die erforderlich ist, um einen sicheren Zustand zu erreichen oder aufrechtzuerhalten, wird in den Sicherheitsanforderungen des E/E/PE-Systems festgelegt (siehe IEC 61508-1, 7.10). Sie kann zum Beispiel aus der sicheren Abschaltung der EUC oder des Teils der EUC bestehen, der für die funktionale Sicherheit auf dem fehlerhaften Teilsystem beruht.

7.4.9 Anforderungen zur Implementierung des E/E/PE-Systems

7.4.9.1 Das sicherheitsbezogene E/E/PE-System muss in Übereinstimmung mit dem Entwurf des E/E/PE-Systems verwirklicht werden.

7.4.9.2 Alle Teilsysteme und ihre Elemente, die von einer oder mehreren Sicherheitsfunktionen verwendet werden, müssen identifiziert und als sicherheitsbezogene Teilsysteme und Elemente beschrieben werden.

7.4.9.3 Die folgenden Informationen müssen für jedes sicherheitsbezogene Teilsystem und Element im angemessenen Rahmen verfügbar sein (siehe auch 7.4.9.4):

ANMERKUNG Für einen Lieferanten eines Teilsystems oder Elements, für das Übereinstimmung mit IEC 61508 beansprucht wird, ist es notwendig, diese Informationen dem Konstrukteur eines sicherheitsbezogenen Systems (oder eines anderen Teilsystems oder Elements) im Sicherheitshandbuch für konforme Objekte zugänglich zu machen, siehe Anhang D.

- a) eine angemessene funktionale Spezifikation des Teilsystems und seiner Elemente;
- b) alle Anweisungen oder Einschränkungen in Bezug auf die Anwendung der Teilsystems und seiner Elemente, die beachtet werden sollten, um systematische Ausfälle des Teilsystems zu verhindern;
- c) die systematische Eignung jedes Elements (siehe 7.4.2.2 c));
- d) Identifikation der Hardware- und/oder Softwarekonfiguration des Elements, um ein Konfigurationsmanagement des sicherheitsbezogenen E/E/PE-Systems in Übereinstimmung mit IEC 61508-1, 6.2.1 zu ermöglichen;
- e) dokumentarischer Nachweis, dass das Teilsystem und seine Elemente verifiziert worden sind, dass es seine funktionalen Sicherheitsanforderungen erfüllt.

7.4.9.4 Die folgenden Informationen müssen für jedes sicherheitsbezogene Element, das für zufällige Hardwareausfälle verantwortlich ist, verfügbar sein (siehe auch 7.4.9.3 und 7.4.9.5):

ANMERKUNG 1 Für einen Lieferanten eines Elements, für das Übereinstimmung mit IEC 61508 beansprucht wird, ist es notwendig, diese Informationen dem Konstrukteur eines sicherheitsbezogenen Systems im Sicherheitshandbuch des Elements zugänglich zu machen, siehe Anhang D.

- a) die Ausfallarten des Elements (im Hinblick auf das Verhalten seiner Ausgänge) in Bezug auf zufällige Hardwareausfälle, die zu einem Ausfall der Sicherheitsfunktion führen und nicht durch interne Diagnosemaßnahmen des Elements erkannt werden oder nicht durch Diagnosemaßnahmen extern zum Element erkennbar sind (siehe 7.4.9.5);
- b) für jede Ausfallart nach a) eine geschätzte Ausfallrate;
- c) die Ausfallarten des Elements (im Hinblick auf das Verhalten seiner Ausgänge) in Bezug auf zufällige Hardwareausfälle, die zu einem Ausfall der Sicherheitsfunktion führen und durch interne Diagnosemaßnahmen des Elements erkannt werden oder durch Diagnosemaßnahmen extern zum Element erkennbar sind (siehe 7.4.9.5);
- d) für jede Ausfallart nach c) eine geschätzte Ausfallrate;
- e) alle Einschränkungen in Bezug auf die Umgebung des Elements, die beachtet werden sollten, um die Gültigkeit der geschätzten Ausfallraten auf Grund zufälliger Hardwareausfälle aufrechtzuerhalten;
- f) jede Grenze in Bezug auf die Lebensdauer des Elements, die nicht überschritten werden sollte, um die Gültigkeit der geschätzten Ausfallraten auf Grund zufälliger Hardwareausfälle aufrechtzuerhalten;
- g) alle Anforderungen zu wiederkehrenden Wiederholungsprüfungen und/oder zu Instandhaltungen;
- h) für jede Ausfallart nach c), die durch interne Diagnosemaßnahmen des Elements erkannt wird, den nach Anhang C bestimmten Diagnosedeckungsgrad (siehe Anmerkung 2);
- i) für jede Ausfallart nach c), die durch interne Diagnosemaßnahmen des Elements erkannt wird, das Diagnose-Testintervall (siehe Anmerkung 2);

ANMERKUNG 2 Der Diagnosedeckungsgrad und das Diagnose-Testintervall sind erforderlich, um es zu ermöglichen, dass in dem Hardware-Sicherheitsintegritätsmodell des sicherheitsbezogenen E/E/PE-Systems (siehe 7.4.5.2) für die Durchführung der Diagnosetests in dem Element Kredit in Anspruch genommen wird.

- j) die Ausfallrate der Diagnosetests in Bezug auf zufällige Hardwareausfälle;
- k) jede zusätzliche Information (zum Beispiel Reparaturzeiten), die notwendig ist, um die Ableitung einer mittleren Zeit bis zur Wiederherstellung (MTTR) zu ermöglichen, die auf die Erkennung eines Fehlers durch die Diagnose folgt;
- l) jegliche Information, die notwendig ist, um die Herleitung des nach Anhang C bestimmten Anteils sicherer Ausfälle (SFF) des wie im sicherheitsbezogenen E/E/PE-System angewendeten Elements zu ermöglichen, einschließlich der Klassifizierung als Typ A oder Typ B gemäß 7.4.3;
- m) die Hardware-Fehlertoleranz des Elements.

ANMERKUNG 3 Die Punkte l) und m) sind notwendig, um den höchsten Sicherheits-Integritätslevel, der gemäß den Einschränkungen auf Grund der Architektur (siehe 7.4.4) für die Sicherheitsfunktion beansprucht werden kann, zu bestimmen.

7.4.9.5 Die geschätzten Ausfallraten für Elemente auf Grund zufälliger Hardwareausfälle (siehe 7.4.9.4 a) und b)) können festgelegt werden entweder durch:

- a) eine Ausfallarten- und Auswirkungsanalyse (FMEA) des Entwurfs unter Verwendung von Elementausfalldaten aus einer anerkannten industriellen Quelle;
oder
- b) durch Erfahrung aus vorheriger Verwendung des Elements in einer ähnlichen Umgebung (siehe 7.4.9.6).

ANMERKUNG 1 Alle verwendeten Ausfallratendaten sollten ein Konfidenzniveau von mindestens 70 % haben. Die statistische Bestimmung des Konfidenzniveaus ist in Hinweis [9] der Literaturhinweise definiert. Siehe Hinweis [10] zu einem gleichwertigen Ausdruck, dem Signifikanzniveau.

ANMERKUNG 2 Wenn anwendungsspezifische Ausfalldaten verfügbar sind, sind diese zu bevorzugen. Wenn dies nicht der Fall ist, kann es sein, dass allgemeine Daten zu verwenden sind.

ANMERKUNG 3 Obwohl für die meisten probabilistischen Abschätzungsmethoden eine konstante Ausfallrate angenommen wird, trifft diese nur unter der Voraussetzung zu, dass die Gebrauchsdauer von Elementen nicht überschritten wird. Nach Ablauf ihrer Gebrauchsdauer (d. h. wenn die Ausfallwahrscheinlichkeit mit der Zeit bedeutend ansteigt) sind die Ergebnisse der meisten probabilistischen Berechnungsmethoden daher wenig aussagekräftig. Daher sollte jede probabilistische Abschätzung eine Festlegung der Gebrauchsdauer der Elemente enthalten. Die Gebrauchsdauer hängt stark vom Element selbst und seinen Betriebsbedingungen ab – im Besonderen von der Temperatur (zum Beispiel können Elektrolytkondensatoren sehr empfindlich sein). Die Erfahrung hat gezeigt, dass die Gebrauchsdauer oft innerhalb eines Bereiches von 8 bis 12 Jahren liegt. Sie kann jedoch bedeutend geringer werden, wenn Elemente nahe an ihren Spezifikationsgrenzen betrieben werden. Elemente mit längeren Gebrauchsdauern neigen dazu, beträchtlich teurer zu sein.

7.4.9.6 Lieferanten müssen für jedes konforme Objekt, dass sie liefern und für das sie Übereinstimmung mit IEC 61508 in Anspruch nehmen, ein Sicherheitshandbuch für konforme Objekte gemäß Anhang D zur Verfügung stellen.

7.4.9.7 Der Lieferant muss für die gesamten Informationen in jedem Sicherheitshandbuch für konforme Objekte eine Begründung angeben.

ANMERKUNG 1 Es ist wesentlich, dass die beanspruchte sicherheitsbezogene Leistungsfähigkeit eines Elements durch einen ausreichenden Nachweis unterstützt wird. Nicht unterstützte Ansprüche helfen nicht die Korrektheit und Integrität der Sicherheitsfunktion, zu der das Element beiträgt, nachzuweisen.

ANMERKUNG 2 Es können kommerzielle oder gesetzliche Beschränkungen in Bezug auf die Verfügbarkeit des Nachweises vorhanden sein. Diese Beschränkungen liegen außerhalb des Anwendungsbereichs dieser Norm. Wenn solche Beschränkungen der Beurteilung der funktionalen Sicherheit einen angemessenen Zugriff auf den Nachweis verweigern, ist das Element für die Verwendung in sicherheitsbezogenen E/E/PE-Systemen nicht geeignet.

7.4.10 Anforderungen für betriebsbewährte Elemente

ANMERKUNG Siehe 7.4.2.2. c) für Einzelheiten unter welchen Bedingungen die Anforderungen dieses Unterabschnitts zutreffen.

7.4.10.1 Ein Element darf nur als betriebsbewährt betrachtet werden, wenn es eine klar beschränkte und festgelegte Funktionalität hat und wenn ein angemessener dokumentarischer Nachweis vorliegt, um zu zeigen, dass die Wahrscheinlichkeit aller gefahrbringenden systematischen Fehler gering genug ist, um die erforderlichen Sicherheits-Integritätslevel der Sicherheitsfunktionen, die das Element verwenden, zu erreichen. Der Nachweis muss sich auf Analyse der Betriebserfahrungen aus einer konkreten Konfiguration des Elements zusammen mit einer Eignungsanalyse und Tests gründen.

ANMERKUNG Eignungsanalyse und Tests konzentrieren sich auf die Demonstration der Leistungsfähigkeit des Elements in der vorgesehenen Anwendung. Die Ergebnisse vorhandener Analyse und Tests sollten berücksichtigt werden. Dieses schließt funktionales Verhalten, Genauigkeit, Verhalten im Falle eines Fehlers, Reaktionszeit, Verhalten bei Überlast, Gebrauchstauglichkeit (z. B. Vermeidung von menschlichem Irrtum) und Instandhaltbarkeit ein.

7.4.10.2 Der nach 7.4.10.1 erforderliche dokumentarische Nachweis muss zeigen, dass:

- a) die vorherigen Verwendungsbedingungen (siehe Anmerkung 1) des speziellen Elements die gleichen sind oder ausreichend nah zu denen liegen, denen das Element im sicherheitsbezogenen E/E/PE-System unterliegen wird;

ANMERKUNG 1 Die Verwendungsbedingungen (Betriebsprofil) schließen alle Faktoren ein, die systematische Fehler in der Hardware und der Software des Elements auslösen können. Beispiele sind Umgebung, Verwendungsart, ausgeführte Funktionen, Konfiguration, Schnittstellen zu anderen Systemen, Betriebssystem, Übersetzer, menschliche Faktoren. Genaue Bedingungen für die Ähnlichkeit von Betriebsprofilen können aus Hinweis [11] in den Literaturhinweisen entnommen werden.

- b) die Rate gefahrbringender Ausfälle in vorherigem Betrieb erreicht worden ist.

ANMERKUNG 2 Siehe IEC 61508-7, Anhang D für Anleitung zur Demonstration von Raten gefahrbringender Ausfälle aus vorherigem Betrieb.

ANMERKUNG 3 Die Zusammenstellung des Nachweises für Betriebsbewährung erfordert ein effektives System für die Erfassung von Ausfällen. Als konservativer Ansatz sollte angenommen werden, dass Anwender fehlerhafte Elemente nur während der Garantiezeit zurückgeben.

7.4.10.3 Wenn irgendein Unterschied zwischen den vorherigen Verwendungsbedingungen und jenen, die im sicherheitsbezogenen E/E/PE-System vorliegen werden, besteht, muss eine Einflussanalyse zu den Unterschieden durchgeführt werden, die eine angemessene Kombination von analytischen Methoden und Tests verwendet, um zu zeigen, dass die Wahrscheinlichkeit aller gefahrbringenden systematischen Fehler gering genug ist, um den(die) erforderlichen Sicherheits-Integritätslevel der Sicherheitsfunktion(en), die das Element verwendet(en), zu erreichen.

7.4.10.4 Es muss eine sicherheitsbezogene Rechtfertigung der Betriebsbewährung unter Verwendung der vorhandenen Informationen aus 7.4.10.2 dokumentiert werden, dass das Element die erforderliche Sicherheitsfunktion mit der erforderlichen systematischen Sicherheitsintegrität unterstützt. Diese muss einschließen:

- a) die Eignungsanalyse und Tests des Elements für die vorgesehene Anwendung;
- b) die Demonstration der Gleichwertigkeit zwischen dem vorgesehenen Betrieb und der vorherigen Betriebserfahrung, einschließlich der Einflussanalyse zu den Unterschieden;
- c) den statistischen Nachweis.

7.4.10.5 Die folgenden Faktoren müssen bei der Entscheidung in Betracht gezogen werden, ob die obigen Anforderungen (7.4.10.1 bis 7.4.10.4) sowohl in Bezug auf den Geltungsbereich, als auch auf den Detaillierungsgrad der verfügbaren Informationen erfüllt worden sind oder nicht (siehe auch 4.1 der IEC 61508-1):

- a) die Komplexität des Elements;
- b) die für das Element erforderliche systematische Eignung;
- c) die Neuheit des Entwurfs.

7.4.10.6 Es muss ein zufrieden stellender Nachweis vorliegen, dass vorhandene Elementefunktionen, die nicht in die Demonstration der Betriebsbewährung einbezogen sind, die Sicherheitsintegrität der verwendeten Elementefunktionen nicht nachteilig beeinflussen können.

ANMERKUNG Diese Anforderung kann durch die Sicherstellung erfüllt werden, dass die Funktionen physikalisch oder elektrisch unbrauchbar gemacht werden oder dass die Software für die Ausführung dieser Funktionen von der betrieblichen Konfiguration ausgeschlossen wird, oder durch andere Formen von Argumenten und Nachweisen.

7.4.10.7 Jede zukünftige Modifikation eines betriebsbewährten Elements muss mit den Anforderungen von 7.8 und IEC 61508-3 übereinstimmen.

7.4.11 Zusätzliche Anforderungen für Datenkommunikation

7.4.11.1 Wenn Datenkommunikation bei der Ausführung einer Sicherheitsfunktion verwendet wird, muss das Ausfallmaß (wie zum Beispiel die Wahrscheinlichkeit eines unerkannten Ausfalls) des Kommunikationsprozesses abgeschätzt werden. Dabei müssen Übertragungsfehler, Wiederholungen, Verlust, Einfügungen, falsche Abfolge, Verfälschung, Verzögerung und Masquerade berücksichtigt werden. Dieses Ausfallmaß muss bei der Abschätzung des Ausfallmaßes der Sicherheitsfunktion infolge zufälliger Ausfälle berücksichtigt werden (siehe 7.4.5).

ANMERKUNG Der Ausdruck Masquerade bedeutet, dass die wahren Inhalte einer Nachricht nicht korrekt identifiziert werden, zum Beispiel eine Nachricht von einem nichtsicheren Element wird fälschlicher als eine Nachricht von einem sicheren Element identifiziert.

7.4.11.2 Die notwendigen Methoden und Maßnahmen, um das erforderliche Ausfallmaß (wie zum Beispiel die Wahrscheinlichkeit eines unerkannten Ausfalls) des Kommunikationsprozesses sicherzustellen (siehe 7.4.11.1), müssen gemäß den Anforderungen dieser Norm und IEC 61508-3 implementiert werden. Dies erlaubt zwei mögliche Lösungsansätze:

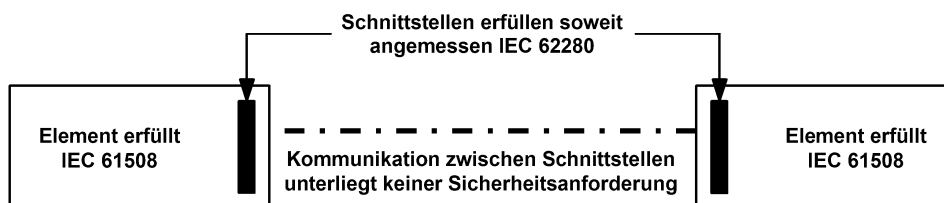
- der gesamte Kommunikationskanal muss gemäß IEC 61508 entworfen, implementiert und validiert sein (ein so genannter „weißer Kanal“, siehe Bild 7 a)); oder

- Teile des Kommunikationskanals sind nicht gemäß IEC 61508 entworfen oder validiert (ein so genannter „schwarzer Kanal“, siehe Bild 7 b)). In diesem Fall müssen die Maßnahmen, die notwendig sind, um die Leistungsfähigkeit bei Ausfall des Kommunikationsprozesses sicherzustellen, in den sicherheitsbezogenen E/E/PE-Elementen implementiert werden, die mit dem Kommunikationskanal in Übereinstimmung mit IEC 62280, soweit angemessen, eine Schnittstelle bilden.

ANMERKUNG Hinweis [12] in den Literaturhinweisen enthält Einzelheiten zu Kommunikationsprofilen für funktionale Sicherheit.



a) Weißer Kanal



b) Schwarzer Kanal

Bild 7 – Architekturen für Datenkommunikation

7.5 Integration des E/E/PE-Systems

ANMERKUNG Diese Phase entspricht Kasten 10.4 in Bild 2.

7.5.1 Ziel

Das Ziel der Anforderungen dieses Unterabschnittes ist die Integration und der Test des sicherheitsbezogenen E/E/PE-Systems.

7.5.2 Anforderungen

7.5.2.1 Das sicherheitsbezogene E/E/PE-System muss nach dem festgelegten Entwurf des E/E/PE-Systems integriert und gemäß den spezifizierten Integrationstests des E/E/PE-Systems (siehe 7.4.2.11) getestet werden.

7.5.2.2 Im Rahmen der Integration aller Module in das sicherheitsbezogene E/E/PE-System muss das sicherheitsbezogene E/E/PE-System wie spezifiziert getestet werden (siehe 7.4). Diese Tests müssen zeigen, dass alle Module korrekt miteinander wirken, um ihre beabsichtigte Funktion auszuführen und so entworfen sind, dass sie keine unbeabsichtigten Funktionen ausführen.

ANMERKUNG 1 Dies bedeutet nicht das Testen aller Eingabekombinationen. Das Testen aller Äquivalenzklassen (siehe B.5.2 der IEC 61508-7) kann ausreichend sein. Statische Analyse (siehe B.6.4 der IEC 61508-7), dynamische Analyse

(siehe B.6.5 der IEC 61508-7) oder Ausfallanalyse (siehe B.6.6 der IEC 61508-7) können die Anzahl der Testfälle auf ein akzeptables Maß reduzieren. Die Anforderungen sind einfacher zu erfüllen, wenn das sicherheitsbezogene E/E/PE-System unter Anwendung eines strukturierten Entwurfs (siehe B.3.2 der IEC 61508-7) oder semi-formaler Methoden (siehe B.2.3 der IEC 61508-7) entwickelt wird.

ANMERKUNG 2 Wenn die Entwicklung nach formalen Methoden erfolgt (siehe B.2.2 der IEC 61508-7) oder formale Beweise oder Assertion-Programmierung verwendet werden (siehe C.5.13 und C.3.3 der IEC 61508-7), können solche Prüfungen vom Umfang her reduziert werden.

ANMERKUNG 3 Ebenso können statistische Nachweise verwendet werden (siehe B.5.3 der IEC 61508-7).

7.5.2.3 Die Integration sicherheitsbezogener Software in das sicherheitsbezogene E/E/PE-System muss in Übereinstimmung mit 7.5 der IEC 61508-3 erfolgen.

7.5.2.4 Es muss eine angemessene Dokumentation der Integrationstests des sicherheitsbezogenen E/E/PE-Systems erstellt werden, welche die Testergebnisse enthält und aussagt, ob die Ziele und Kriterien, die während der Entwurfs- und Entwicklungsphase festgelegt wurden, erreicht bzw. eingehalten worden sind. Falls es einen Ausfall gibt, müssen die Gründe für den Ausfall und seine Korrektur dokumentiert werden.

7.5.2.5 Während der Integration und der Tests müssen alle Modifikationen oder Änderungen an dem sicherheitsbezogenen E/E/PE-System Gegenstand einer Einflussanalyse sein, die alle betroffenen Teilsysteme und Elemente und die notwendigen Reverifikationstätigkeiten identifizieren muss.

7.5.2.6 Zu den Integrationstests des E/E/PE-Systems müssen die folgenden Informationen dokumentiert werden:

- a) die Version der verwendeten Testspezifikation;
- b) die Kriterien für Akzeptanz der Integrationstests;
- c) die Version des getesteten sicherheitsbezogenen E/E/PE-Systems;
- d) die verwendeten Werkzeuge und Betriebsmittel mit Kalibrierungsdaten;
- e) die Ergebnisse jedes Tests;
- f) jeden Widerspruch zwischen erwarteten und tatsächlichen Ergebnissen;
- h) die ausgeführte Analyse und die getroffenen Entscheidungen, ob die Prüfung fortgesetzt oder eine Änderungsanforderung eingeleitet wird, im Falle, dass Widersprüche auftreten.

7.5.2.7 Zur Vermeidung von Fehlern während der Integration des E/E/PE-Systems muss eine angemessene Gruppe von Verfahren und Maßnahmen gemäß Tabelle B.3 verwendet werden.

7.6 Betriebs- und Instandhaltungsverfahren des E/E/PE-Systems

ANMERKUNG Diese Phase entspricht Kasten 10.5 in Bild 2.

7.6.1 Ziel

Das Ziel der Anforderungen dieses Unterabschnittes ist es, Verfahren zu entwickeln, um sicherzustellen, dass die erforderliche funktionale Sicherheit des sicherheitsbezogenen E/E/PE-Systems während des Betriebs und der Instandhaltung aufrechterhalten wird.

7.6.2 Anforderungen

7.6.2.1 Es müssen Betriebs- und Instandhaltungsverfahren des E/E/PE-Systems aufgestellt werden, die Folgendes festlegen müssen:

- a) die routinemäßigen Handlungen, die ausgeführt werden müssen, um die entworfene funktionale Sicherheit des sicherheitsbezogenen E/E/PE-Systems aufrechtzuerhalten, einschließlich des routinemäßigen Ersatzes von Elementen mit einer vorbestimmten Gebrauchsdauer, zum Beispiel Kühlventilatoren und Batterien usw.;

- b) die Handlungen und Einschränkungen, die notwendig sind (zum Beispiel während der Installation, des Einschaltens, des normalen Betriebs, der Routineprüfungen, vorhersehbarer Störungen, bei Fehlern oder Ausfällen und während des Abschaltens), um einen unsicheren Zustand zu verhindern und/oder die Folgen eines Schadensereignisses zu reduzieren;
- c) die Dokumentation, die zu Systemausfällen und Anforderungsraten des sicherheitsbezogenen E/E/PE-Systems geführt werden muss;
- d) die Dokumentation, die zu Ergebnissen von Audits und Tests des sicherheitsbezogenen E/E/PE-Systems geführt werden muss;
- e) die Instandhaltungsverfahren, die durchgeführt werden müssen, wenn Fehler oder Ausfälle in dem sicherheitsbezogenen E/E/PE-System auftreten, einschließlich:
 - Verfahren für Fehlerdiagnose und Reparatur;
 - Verfahren für die Revalidierung;
 - Anforderungen an die Instandhaltungsaufzeichnungen;
- f) die Verfahren für die Aufzeichnung der Ausführung der Instandhaltung müssen festgelegt werden, insbesondere:
 - Verfahren zur Aufzeichnung von Ausfällen;
 - Verfahren zur Analyse von Ausfällen;
- g) die für Instandhaltung und Revalidierung notwendigen Werkzeuge und Verfahren für die Instandhaltung der Werkzeuge und der Ausrüstung.

ANMERKUNG 1 Es kann sowohl aus sicherheitstechnischen, als auch aus betriebswirtschaftlichen Gründen vorteilhaft sein, die Betriebs- und Instandhaltungsverfahren des E/E/PE-Systems mit den Verfahren für den Gesamtbetrieb und die gesamte Instandhaltung der EUC zusammenzufassen.

ANMERKUNG 2 Die Betriebs- und Instandhaltungsverfahren des E/E/PE-Systems sollten die Softwaremodifikationsverfahren einschließen (siehe IEC 61508-3, 7.8).

7.6.2.2 Die Betriebs- und Instandhaltungsverfahren des sicherheitsbezogenen E/E/PE-Systems müssen fortlaufend durch Eingaben, wie zum Beispiel den Ergebnissen von Audits der funktionalen Sicherheit (1) und Prüfungen zu dem sicherheitsbezogenen E/E/PE-System (2), auf den letzten Stand gebracht werden.

7.6.2.3 Die Routine-Instandhaltungstätigkeiten, die erforderlich sind, um die funktionale Sicherheit des sicherheitsbezogenen E/E/PE-Systems (wie entworfen) aufrechtzuerhalten, müssen durch eine systematische Methode festgelegt werden. Diese Methode muss nicht erkannte Ausfälle aller sicherheitsbezogenen Elemente (von Sensoren bis zu Stellgliedern) feststellen, die eine Verringerung der erreichten Sicherheitsintegrität verursachen würden. Angemessene Methoden schließen ein:

- Untersuchung von Fehlerbäumen;
- Ausfallarten- und Auswirkungsanalyse (FMEA);
- zuverlässigkeitsbezogene Instandhaltung.

ANMERKUNG 1 Eine Betrachtung menschlicher Faktoren ist ein Schlüsselement bei der Bestimmung der erforderlichen Handlungen und der angemessenen Schnittstelle(n) mit dem sicherheitsbezogenen E/E/PE-System.

ANMERKUNG 2 Die Wiederholungsprüfungen werden mit der Häufigkeit ausgeführt, die zur Erreichung des Ausfallgrenzwertes notwendig ist.

ANMERKUNG 3 Die Häufigkeit der Wiederholungsprüfungen, das Diagnose-Testintervall und die Zeit für die nachfolgende Reparatur hängen von mehreren Faktoren ab (siehe Anhang B der IEC 61508-6). Diese schließen ein:

- den Ausfallgrenzwert, der mit dem Sicherheits-Integritätslevel verbunden ist;
- die Architektur;
- den Diagnosedeckungsgrad der Diagnosetests; und
- die erwartete Anforderungsrate.

ANMERKUNG 4 Die Häufigkeit der Wiederholungsprüfungen und das Diagnose-Testintervall haben wahrscheinlich eine entscheidende Wirkung bei der Erreichung der Sicherheitsintegrität der Hardware. Einer der Hauptgründe für die Durchführung von Hardware-Zuverlässigkeitsanalysen (siehe 7.4.5.2) ist sicherzustellen, dass die Häufigkeiten der zwei Arten von Prüfungen in Bezug auf den Zielwert der Sicherheitsintegrität der Hardware angemessen sind.

7.6.2.4 Die Betriebs- und Instandhaltungsverfahren des E/E/PE-Systems müssen in Bezug auf ihren Einfluss, den sie auf die EUC haben können, beurteilt werden.

7.6.2.5 Zur Vermeidung von Fehlern und Ausfällen während der Betriebs- und Instandhaltungsverfahren des E/E/PE-Systems muss eine angemessene Gruppe von Verfahren und Maßnahmen gemäß Tabelle B.4 verwendet werden.

7.7 Validierung der Sicherheit des E/E/PE-Systems

ANMERKUNG Diese Phase entspricht Kasten 10.6 in Bild 2.

7.7.1 Ziel

Das Ziel der Anforderungen dieses Unterabschnittes ist es, zu validieren, dass das sicherheitsbezogene E/E/PE-System in jeder Hinsicht den Anforderungen zur Sicherheit im Sinne der erforderlichen Sicherheitsfunktionen und der Sicherheitsintegrität entspricht (siehe 7.2 und IEC 61508-1, 7.10).

7.7.2 Anforderungen

7.7.2.1 Die Validierung der Sicherheit des E/E/PE-Systems muss in Übereinstimmung mit einem vorbereiteten Plan ausgeführt werden (siehe auch 7.7 der IEC 61508-3).

ANMERKUNG 1 Die Validierung der Sicherheit des E/E/PE-Systems wird im Sicherheitslebenszyklus des E/E/PE-Systems so gezeigt, dass sie vor der Installation ausgeführt wird. In einigen Fällen aber kann die Validierung der Sicherheit des E/E/PE-Systems nicht vor dem Ende der Installation ausgeführt werden (zum Beispiel, wenn die Entwicklung der Anwendungssoftware nicht vor der Installation abgeschlossen wurde).

ANMERKUNG 2 Die Validierung eines sicherheitsbezogenen programmierbaren elektronischen Systems beinhaltet die Validierung sowohl von Hardware, als auch von Software. Die Anforderungen für die Validierung von Software sind in der IEC 61508-3 enthalten.

7.7.2.2 Alle Prüfmesseinrichtungen, die für die Validierung verwendeten werden, müssen gegen eine Norm, die, falls vorhanden, auf eine nationale Norm rückführbar ist oder nach einem weithin anerkannten Verfahren kalibriert werden. Die gesamten Prüfeinrichtungen müssen in Bezug auf korrekte Funktion verifiziert werden.

7.7.2.3 Die angemessene Implementierung jeder Sicherheitsfunktion, die in den Entwurfsanforderungen des E/E/PE-Systems (siehe IEC 61508-1, 7.10) spezifiziert ist, die Entwurfsanforderungen des E/E/PE-Systems (siehe 7.2) und alle Betriebs- und Instandhaltungsverfahren des E/E/PE-Systems muss durch Test und/oder Analyse validiert werden. Wenn eine angemessene Unabhängigkeit oder Entkopplung zwischen einzelnen Elementen oder Teilsystemen nicht analytisch aufgezeigt werden kann, müssen die zugehörigen Kombinationen funktionalen Verhaltens getestet werden.

ANMERKUNG Da die Anzahl notwendiger Testkombinationen sehr groß werden kann, könnte eine Restrukturierung des Systems aus diesem Anlass erforderlich sein.

7.7.2.4 Es muss eine angemessene Dokumentation der Tests zur Validierung der Sicherheit des E/E/PE-Systems erstellt werden, die für jede Sicherheitsfunktion Folgendes darlegen muss:

- a) die Version des verwendeten Plans zur Validierung der Sicherheit des E/E/PE-Systems;
- b) die geprüfte (oder analysierte) Sicherheitsfunktion zusammen mit dem spezifischen Bezug zu der während der Planung der Validierung der Sicherheit des E/E/PE-Systems festgelegten Anforderung;
- c) die verwendeten Werkzeuge und Einrichtungen zusammen mit Kalibrierungsdaten;

- d) die Ergebnisse jedes Tests;
- e) Widersprüche zwischen den erwarteten und tatsächlichen Ergebnissen.

ANMERKUNG Es ist keine getrennte Dokumentation für jede Sicherheitsfunktion erforderlich, aber die Informationen von a) bis e) müssen auf jede Sicherheitsfunktion zutreffen und wo sie sich für die Sicherheitsfunktionen unterscheiden, muss die Beziehung dargelegt werden.

7.7.2.5 Wenn Widersprüche auftreten (d. h. die tatsächlichen Ergebnisse weichen von den erwarteten Ergebnissen um mehr als die festgelegten Toleranzen ab), müssen die Ergebnisse der Tests zur Validierung der Sicherheit des E/E/PE-Systems dokumentiert werden, einschließlich:

- a) der durchgeführten Analyse; und
- b) der getroffenen Entscheidung, ob die Prüfung fortgesetzt oder eine Änderungsanforderung gestellt wird und eine Rückkehr zu einem früheren Teil des Validierungstests erfolgt.

7.7.2.6 Der Lieferant oder Entwickler muss die Ergebnisse der Tests zur Validierung der Sicherheit des E/E/PE-Systems dem Entwickler der EUC und des EUC-Leit- oder Steuerungssystems zur Verfügung stellen, um ihnen zu ermöglichen, die Anforderungen für die Gesamtvalidierung der Sicherheit nach IEC 61508-1 zu erfüllen.

7.7.2.7 Zur Vermeidung von Fehlern während der Validierung der Sicherheit eines E/E/PE-Systems muss eine angemessene Gruppe von Verfahren und Maßnahmen gemäß Tabelle B.5 verwendet werden.

7.8 Modifikation des E/E/PE-Systems

7.8.1 Ziel

Das Ziel der Anforderungen dieses Unterabschnittes ist es, Korrekturen, Verbesserungen oder Anpassungen an dem sicherheitsbezogenen E/E/PE-System auszuführen und dabei sicherzustellen, dass die erforderliche Sicherheitsintegrität erreicht wird und aufrechterhalten bleibt.

7.8.2 Anforderungen

7.8.2.1 Für jede Tätigkeit zur Modifikation des E/E/PE-Systems muss eine angemessene Dokumentation erfolgen und fortgeführt werden. Die Dokumentation muss beinhalten:

- a) die genaue Spezifikation der Modifikation oder Änderung,
- b) eine Analyse der Auswirkung der Modifikationstätigkeit auf das gesamte System, einschließlich Hardware, Software (siehe IEC 61508-3) und Bedienung, sowie auf die Umgebung und mögliche Wechselwirkungen;
- c) alle Genehmigungen für die Änderungen;
- d) den Fortschritt der Änderungen;
- e) Testfälle für Teilsysteme und Elemente einschließlich der Revalidierungsdaten;
- f) Historie des Konfigurationsmanagements des E/E/PE-Systems;
- g) Abweichung vom Normalbetrieb und normalen Bedingungen;
- h) notwendige Änderungen von Systemverfahren;
- i) notwendige Änderungen der Dokumentation.

7.8.2.2 Hersteller oder Systemlieferanten, die Konformität mit dieser Norm oder Teilen dieser Norm beanspruchen, müssen ein System führen, um Änderungen als Ergebnis von erkannten Störungen in Hard- oder Software einleiten zu können und Anwender über die Notwendigkeit von Modifikationen zu informieren, falls die Störungen die Sicherheit beeinflussen.

7.8.2.3 Die Modifikation muss mindestens mit der gleichen Sachkenntnis, mit automatisierten Werkzeugen (siehe 7.4.4.2 der IEC 61508-3) und mit einer Planung und einem Management, wie in der ursprünglichen Entwicklung der sicherheitsbezogenen E/E/PE-Systeme, ausgeführt werden.

7.8.2.4 Nach der Modifikation müssen die sicherheitsbezogenen E/E/PE-Systeme erneut verifiziert und validiert werden.

ANMERKUNG Siehe auch 7.16.2.6 der IEC 61508-1.

7.9 Verifikation des E/E/PE-Systems

7.9.1 Ziel

Das Ziel der Anforderungen dieses Unterabschnittes ist es, die Ergebnisse einer gegebenen Phase zu testen und zu bewerten, um Korrektheit und Konsistenz hinsichtlich der Produkte und Normen sicherzustellen, welche die Eingabe zu dieser Phase bilden.

ANMERKUNG Zur Erleichterung sind alle Verifikationstätigkeiten unter 7.9 zusammengefasst worden, sie werden jedoch tatsächlich über mehrere Phasen verteilt ausgeführt.

7.9.2 Anforderungen

7.9.2.1 Die Verifikation der sicherheitsbezogenen E/E/PE-Systeme muss gleichzeitig mit der Entwicklung (siehe 7.4) für jede Phase des Sicherheitslebenszyklus des E/E/PE-Systems geplant und dokumentiert werden.

7.9.2.2 Die Planung der Verifikation des E/E/PE-Systems muss sich auf alle Kriterien, Verfahren und Werkzeuge beziehen, die in der Verifikation für diese Phase zu verwenden sind.

7.9.2.3 Die Planung der Verifikation des E/E/PE-Systems muss die Tätigkeiten festlegen, die auszuführen sind, um Korrektheit und Konsistenz hinsichtlich der Produkte und Normen sicherzustellen, welche die Eingabe zu dieser Phase bilden.

7.9.2.4 Die Planung der Verifikation des E/E/PE-Systems muss Folgendes betrachten:

- a) die Auswahl der Verifikationsstrategien und Verifikationsverfahren;
- b) die Auswahl und Verwendung von Testeinrichtungen;
- c) die Auswahl und Dokumentation von Verifikationstätigkeiten;
- d) die Bewertung der durch die Verifikationseinrichtungen unmittelbar und durch Tests gewonnenen Verifikationsergebnisse.

7.9.2.5 In jeder Entwurfs- und Entwicklungsphase muss gezeigt werden, dass die funktionalen Anforderungen und die Anforderungen zur Sicherheitsintegrität erreicht worden sind.

7.9.2.6 Das Ergebnis jeder Verifikationstätigkeit muss dokumentiert werden und entweder aussagen, dass die sicherheitsbezogenen E/E/PE-Systeme die Verifikation bestanden haben, oder die Gründe für die Ausfälle angeben. Folgendes muss betrachtet werden:

- a) Punkte, die mit einer oder mehreren relevanten Anforderungen des Sicherheitslebenszyklus des E/E/PE-Systems (siehe 7.2) nicht übereinstimmen;
- b) Punkte, die mit einer oder mehreren relevanten Normen für den Entwurf (siehe 7.4) nicht übereinstimmen;
- c) Punkte, die mit einer oder mehreren relevanten Anforderungen zum Management der Sicherheit (siehe Abschnitt 6) nicht übereinstimmen.

7.9.2.7 Zur Verifikation der Entwurfsanforderungen des E/E/PE-Systems muss, nachdem die Entwurfsanforderungen des E/E/PE-Systems festgelegt worden sind (siehe 7.2), und bevor die nächste Phase (Entwurf und Entwicklung) beginnt, die Verifikation:

- a) entscheiden, ob die Entwurfsanforderungen des E/E/PE-Systems angemessen sind, um die Spezifikation der Sicherheitsanforderungen des E/E/PE-Systems (siehe IEC 61508-1, 7.10) für Sicherheit, Funktionalität und andere während der Planung der Sicherheit festgelegte Anforderungen zu erfüllen; und
- b) auf Inkompatibilitäten überprüfen zwischen
 - den Sicherheitsanforderungen des E/E/PE-Systems (siehe IEC 61508-1, 7.10);
 - den Entwurfsanforderungen des E/E/PE-Systems (siehe 7.2);
 - den Tests des E/E/PE-Systems (siehe 7.4); und
 - der Dokumentation für den Anwender und der gesamten anderen Systemdokumentation.

7.9.2.8 Zur Verifikation von Entwurf und Entwicklung des E/E/PE-Systems muss, nachdem Entwurf und Entwicklung des E/E/PE-Systems (siehe 7.4) fertig gestellt worden sind und bevor die nächste Phase (Integration) beginnt, die Verifikation:

- a) entscheiden, ob die Tests des E/E/PE-Systems angemessen für den Entwurf und die Entwicklung des E/E/PE-Systems sind,
- b) Konsistenz und Vollständigkeit (hinunter bis auf und einschließlich Modulniveau) von Entwurf und Entwicklung des E/E/PE-Systems hinsichtlich der Sicherheitsanforderungen des E/E/PE-Systems (siehe IEC 61508-1, 7.10) feststellen, und
- c) auf Inkompatibilitäten überprüfen zwischen:
 - den Sicherheitsanforderungen des E/E/PE-Systems (siehe IEC 61508-1, 7.10);
 - den Entwurfsanforderungen des E/E/PE-Systems (siehe 7.2);
 - dem Entwurf und der Entwicklung des E/E/PE-Systems (siehe 7.4); und
 - den Tests des E/E/PE-Systems (siehe 7.4).

ANMERKUNG 1 Tabelle B.5 empfiehlt zur Validierung der Sicherheit Ausfallanalyse und Testverfahren, die auch zur Verifikation anwendbar sind.

ANMERKUNG 2 Die Verifikation, dass der Diagnosedeckungsgrad erreicht worden ist, erfolgt unter Berücksichtigung der Tabelle A.1, welche die Fehler und Ausfälle angibt, die erkannt werden müssen.

7.9.2.9 Zur Verifikation der Integration des E/E/PE-Systems muss die Integration des sicherheitsbezogenen E/E/PE-Systems verifiziert werden, um zu begründen, dass die Anforderungen von 7.5 erreicht worden sind.

7.9.2.10 Testfälle und ihre Ergebnisse müssen dokumentiert werden.

8 Beurteilung der funktionalen Sicherheit

Die Anforderungen zur Beurteilung der funktionalen Sicherheit sind in Abschnitt 8 der IEC 61508-1 ausführlich beschrieben.

Anhang A (normativ)

Verfahren und Maßnahmen für sicherheitsbezogene E/E/PE-Systeme: Beherrschung von Ausfällen während des Betriebs

A.1 Allgemeines

Dieser Anhang muss in Verbindung mit 7.4 verwendet werden. Er begrenzt den höchsten Diagnosedeckungsgrad, der für die relevanten Verfahren und Maßnahmen beansprucht werden kann. Für jeden Sicherheits-Integritätslevel empfiehlt er Verfahren und Maßnahmen zur Beherrschung zufälliger Hardwareausfälle, systematischer Ausfälle, umgebungsbedingter Ausfälle und von Ausfällen während des Betriebs. Weitere Informationen über Architekturen und Maßnahmen sind im Anhang B der IEC 61508-6 und Anhang A der IEC 61508-7 enthalten.

Es ist nicht möglich, jede einzelne physikalische Ursache eines Ausfalls von komplexer Hardware aufzuführen. Dies hat zwei Hauptgründe:

- die Beziehung zwischen Ursache/Auswirkung von Fehlern und Ausfällen ist oft schwierig zu bestimmen;
- der Schwerpunkt von Ausfällen ändert sich von zufälligen zu systematischen Ausfällen, wenn komplexe Hardware und Software verwendet wird.

Ausfälle in sicherheitsbezogenen E/E/PE-Systemen können nach dem Zeitpunkt ihrer Entstehung in folgende Klassen aufgeteilt werden:

- Ausfälle verursacht durch Fehler, die **vor oder während der Systeminstallation** entstehen (zum Beispiel Softwarefehler einschließlich Spezifikations- und Programmfehler, Hardwarefehler einschließlich Herstellungsfehler und falsche Auswahl von Elementen); und
- Ausfälle verursacht durch Fehler oder menschliches Versagen, die **nach der Systeminstallation** entstehen (zum Beispiel zufällige Hardwareausfälle oder Ausfälle, die durch unsachgemäßen Gebrauch verursacht sind).

Um solche Ausfälle bei ihrem Auftreten zu vermeiden oder zu beherrschen, ist üblicherweise eine große Anzahl von Maßnahmen notwendig. Die Struktur der Anforderungen in den Anhängen A und B resultiert aus der Aufteilung der Maßnahmen in Maßnahmen zur **Vermeidung von Ausfällen** während der verschiedenen Phasen des Sicherheitslebenszyklus des E/E/PE-Systems (Anhang B) und Maßnahmen zur **Beherrschung von Ausfällen** während des Betriebs (dieser Anhang). Die Maßnahmen zur Beherrschung von Ausfällen sind eingebaute Merkmale der sicherheitsbezogenen E/E/PE-Systeme.

Der Diagnosedeckungsgrad und der Anteil sicherer Ausfälle werden auf Basis der Tabelle A.1 und nach den im Anhang C detaillierten Verfahren bestimmt. Die Tabellen A.2 bis A.14 unterstützen die Anforderungen der Tabelle A.1 durch Empfehlung von Verfahren und Maßnahmen für Diagnosetests und Empfehlung höchster Diagnosedeckungsgrade, die durch ihre Verwendung erreicht werden können. Die Tabellen ersetzen keine der Anforderungen aus Anhang C. Die Tabellen A.2 bis A.14 haben keinen ausschließlichen Charakter. Andere Maßnahmen und Verfahren können unter der Voraussetzung verwendet werden, dass ein Nachweis in Bezug auf den geltend gemachten Diagnosedeckungsgrad erbracht wird. Wird ein hoher Diagnosedeckungsgrad geltend gemacht, sollte mindestens ein Verfahren mit hohem Diagnosedeckungsgrad aus jeder dieser Tabellen angewendet werden.

In ähnlicher Weise empfehlen die Tabellen A.15 bis A.17 für jeden Sicherheits-Integritätslevel Verfahren und Maßnahmen zur Beherrschung systematischer Ausfälle. Tabelle A.15 empfiehlt Gesamtmaßnahmen zur Beherrschung systematischer Ausfälle (siehe auch IEC 61508-3), Tabelle A.16 empfiehlt Maßnahmen zur Beherrschung umgebungsbedingter Ausfälle und Tabelle A.17 empfiehlt Maßnahmen zur Beherrschung von Ausfällen während des Betriebs. Die meisten dieser beherrschenden Maßnahmen können gemäß Tabelle A.18 abgestuft werden.